packt

The Cybersecurity Executive's First Year Playbook



From Onboarding to Strategic Impact

Renana Friedlich | Yuri Diogenes

The Cybersecurity Executive's First Year Playbook

From Onboarding to Strategic Impact

Renana Friedlich
Yuri Diogenes

‹packt›

The Cybersecurity Executive's First Year Playbook

Copyright © 2026 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.
Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.
Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Portfolio Director: Vijin Boricha
Senior Portfolio Manager: Niranjan Naikwadi
Program Manager: Ankita Thakur
Content Engineer: Shubhra Mayuri
Technical Editor: Nithik Cheruvakkodan
Copy Editor: Tracy Brown
Indexer: Pratik Shirodkar
Production Designer: Ajay Patule
Growth Lead: Ankita Thakur

First published: October 2026

Production reference: 1291026

Published by Packt Publishing Ltd.
Grosvenor House
11 St Paul's Square
Birmingham
B3 1RB, UK.

ISBN 978-1-80667-933-1
www.packtpub.com

To the next generation of security executives taking on greater responsibility, navigating uncertainty, and committed to doing the right thing.

– Renana Friedlich & Yuri Diogenes

Foreword

I've known Renana for years, both as a friend and as someone I've had the privilege of advising, learning from, and watching evolve as a leader. Because of that, I had a unique perspective reading this manuscript. I wasn't just evaluating the book. I was also paying attention to whether the person reflected in these pages was the same person I've come to know over the years.

It absolutely is.

On the surface, this book by Renana Friedlich and Yuri Diogenes is a guide for cybersecurity executives navigating their first year in a senior leadership role. It offers practical frameworks, playbooks, templates, and real-world guidance across everything from stakeholder management and board communication to risk, governance, hiring, and incident response. But what makes the book resonate well beyond cybersecurity is that, at its core, it is really about leadership.

The Renana who appears in these pages is the same person I know: curious rather than judgmental, deeply thoughtful about people, focused on building trust, and honest about the realities of leadership. She writes openly about mistakes, uncertainty, burnout, difficult decisions, and lessons learned the hard way. She doesn't present herself as someone who always had the answers. Instead, she shares how her perspective evolved through experience, mentorship, and reflection.

I was impressed by the balance that the authors strike between practical execution and personal insight. Readers will find frameworks and guidance they can put into practice immediately, but they will also find something much harder to capture: an honest account of what it actually feels like to step into a leadership role where expectations are high, information is incomplete, and the stakes are real.

Throughout the manuscript, the recurring themes aren't really about technology. They are about trust, influence, resilience, communication, and the responsibility leaders have to develop the people around them. Those lessons apply whether you're a first-time CISO, an experienced executive, or a leader operating in an entirely different field.

The result is a book that is both practical and deeply human. It reflects not only Renana's expertise, but also her character, and I believe that is what will stay with readers long after they finish the final chapter.

Maggie Myers

Principal, Korn Ferry

What Industry Leaders Are Saying

Cybersecurity is no longer a technology issue. It is a business leadership imperative. In *The Cybersecurity Executive's First Year Playbook*, Renana and Yuri capture that reality with remarkable clarity. This is far more than a cybersecurity handbook. It is a practical guide for leaders who must build trust, align security with business strategy, navigate risk, and lead through complexity. Drawing on years of real-world experience, they offer actionable insights that help security executives move beyond protecting systems to enabling business success. Any current or aspiring security leader will find tremendous value in these pages.

Rich Steinmeier

CEO, LPL Financial

The first few days of any executive are pivotal. They build the trust and drive the outcomes that define their tenure. Stepping in as a security exec rarely gives you time to figure it out as you go. Renana and Yuri have built a compelling framework that turns those first months into lasting strategic impact.

Assaf Keren

CISO, Meta

In an era where AI is radically redefining both innovation and enterprise risk, the first year of a modern CISO's tenure has never been more critical. It is the defining window to establish executive credibility, shape security culture, and set the organizational tone for resilience. In *The Cybersecurity Executive's First Year Playbook*, Renana and Yuri have done a fantastic job capturing both the broad strategic strokes and the subtle nuances required to succeed today. Grounded in a fresh, authentic practitioner perspective, this is an essential roadmap for any security leader looking to make an immediate and lasting business impact.

Michael Piacente

Managing Partner, Hitch Partners

I've spent my career backing cybersecurity startups and sitting in rooms where security leaders succeed or fail—and the difference is rarely technical. It's the ability to translate risk into business language, win budget, and earn the board's trust. This book teaches exactly that, from someone who has done it at the highest levels of Fortune 500 financial organizations.

Sid Trivedi

Partner at Foundation Capital

Contributors

About the authors

Renana Friedlich is an enterprise technology and cybersecurity executive who serves as Executive Vice President, CISO and CIO at LPL Financial. An award-winning leader with more than two decades of experience, Renana is known for turning strategy into execution and driving innovation across cybersecurity, AI, and enterprise technology. Before joining LPL, she held senior leadership roles at PayPal, EY, and the IDF, where she helped protect some of the world's largest organizations against cyber threats. Renana actively engages in shaping the future of cybersecurity. She serves on advisory boards for universities, technology companies, startups, and venture capital firms and is a sought-after speaker at leading conferences, where she shares her perspectives on building trust and enabling growth in highly regulated environments. Renana holds multiple security certifications, including the CISSP, CISM, and a CISO certification from the Technion – Israel Institute of Technology.

To my family—especially my husband, Arye; our mini CISO, Leah; and our baby CISO, Danielle—thank you for accepting the mornings, evenings, weekends, and family hours I needed to dedicate to this book. Your support allowed me to come this far and allows me to continue dreaming about what lies ahead. I hope this book inspires you to chase your own dreams, whatever they may be.

To my mentors and sponsors Assaf, Sri, Rich, Greg, Cherie, Papanii, William, Patrick, James, Danielle, Mandana, Tal, Shay, and Oran—thank you for believing in me, offering candid guidance, opening doors, and sometimes pushing me before I felt ready. You helped shape the leader I am today.

To Stan, Ron, Michael, Kaushal, Dan, Ed, Guy, Tuffy, Kelly, Mark, Johnny, Avi, Joe, Jocelyn, Ryan, along with the many others I have had the privilege of leading and working alongside: thank you for your trust, partnership, and everything you have taught me. Much of what I know about leadership was learned with—and from—you.

To Yuri, thank you for arriving at the right moment, challenging me to write my first book, and walking beside me as we turned that challenge into a reality.

Yuri Diogenes is a cybersecurity executive, author, and educator with more than 30 years of experience in the technology industry. He holds a PhD in Cybersecurity Leadership, a Master of Science in Cybersecurity Intelligence and Forensics Investigation, and an MBA.

Yuri is a Professor at the University of Texas at Dallas and EC-Council University. He spent more than two decades at Microsoft, holding various technical and leadership positions, most recently serving as Principal PM Manager for Microsoft Defender for Cloud.

An accomplished author, Yuri has published more than 30 books, primarily focused on cybersecurity, information security, and Microsoft technologies. He also holds numerous industry-recognized certifications, including CISSP, CEH, CHFI, ECSA, CND, CompTIA SecAI+, Security+, CySA+, Network+, CASP+, and MITRE ATT&CK certifications in Cyber Threat Intelligence, Threat Hunting, and Detection Engineering.

You can follow Yuri on X: @yuridiogenes

To my mother, who passed away in September 2025, and will forever be with me. Thank you for all your efforts to raise me alone.

To Renana, thanks for taking this challenge and driving the project with resilience and precision. While this was your first book, your years of experience in the field of cybersecurity helped to shape this book the way it is. Thank you for your dedication and tenacity.

About the reviewers

Jason Witty is the EVP, Chief Information Security Officer (CISO) for Fidelity Investments. He leads a global team of nearly 1,500 people dedicated to maintaining the safety and trust of their customers, workforce, data, and systems. He is an award-winning CIO/CISO, co-editor of *Cybersecurity Risk Management: Enhancing Leadership and Expertise*, and a certified Information Systems Security Management Professional (ISSMP) with more than 30 years of experience in technology and information risk management. Jason has provided extensive industry leadership, currently serving as the Vice-Chair of the National Technology Security Coalition (NTSC). He previously served as the Chair of the FS-ISAC from 2014 to 2019 and the Sector Chief for Financial Services in FBI Chicago's InfraGard program. He has a bachelor's degree in electrical engineering technology from Old Dominion University.

Tracy Brown Hamilton is a writer, editor, and journalist with more than thirty years of experience in technical, trade, and educational publishing. She has edited hundreds of books on subjects ranging from technology to education, security to healthcare. She lives in the Netherlands with her husband and three children.

Table of Contents

Preface xxv

Free benefits with your book xxx

Chapter 0: Introduction 1

The challenges of your first year 1

Strategic alignment and business integration • 2

Security program management • 2

External pressures • 3

What makes this book unique 3

How to use this book 4

The road ahead 4

Part 1: Assessing and Setting Direction 5

Chapter 1: Laying the Foundational Bricks: The Initial Assessment 7

Understanding the business context 8

General knowledge • 9

Revenue • 9

Operational dependencies • 10

Regulatory and compliance landscape • 10

Conducting a listening tour 11

Owning your calendar • 12

Asking general questions • 14

Meeting your manager • 16

Meeting your directs • 17

Meeting technology leaders • 18

Software development • 18

Architecture • 19

Infrastructure • 20

Meeting internal stakeholders • 21

Business leaders • 21
Legal • 21
Human resources • 22
Physical security • 23
Risk and internal audit • 23
Finance and procurement • 24
Third-party risk management • 24
Meeting external stakeholders • 25
Consulting firms • 25
External audit • 25
Vendors • 26
Identifying the existing security posture 27
Security metrics • 27
Asset inventory • 28
Tool and control coverage • 28
Threat exposure management • 28
Security incidents • 29
Policies and governance • 29
Assessments and audit reports • 29
Initial risk landscape analysis • 30
Evaluating the organizational culture 31
Assessing leadership alignment • 31
Identifying risk appetite and ownership • 32
Reviewing cross-functional collaboration • 32
Documentation and information validation 33
Avoiding common mistakes • 33
Using documentation templates • 34
Checking for legal liability • 35
Validating your observations • 35
Notes from the field with Renana 36
Summary 37
Chapter checklist 37
Additional resources 37

Chapter 2: Forging Alliances: Building Key Relationships 39

Assessing and empowering your team 40
Introducing the Team Assessment Tool • 40
Evaluating skills and role alignment • 42
Identifying champions • 43
Moving beyond first impressions • 44
Empowering through development and recognition • 46
Counseling/mentoring/sponsorship framework • 46
Amplifying success through recognition • 49
Collaborating with IT and product leaders 50
Understanding competing priorities • 50
Aligning around shared business outcomes • 50
Introducing the Security Scorecard • 52
Managing stakeholder relationships 55
Building a partnership mindset • 56
Creating the stakeholder map • 56
Determining cadences • 58
Making time to connect • 60
Engaging with C-suite and the board 61
10-minute security update framework • 62
Building long-term trust • 64
Notes from the field with Renana 64
Case study: collaboration with stakeholders • 64
Summary 65
Chapter checklist 65
Additional resources 66

Chapter 3: Crafting Your Vision: Developing the Security Plan 67

Moving from assessment to planning 68
Recognizing the shift from tactical to strategic thinking • 68
Avoiding common pitfalls in defining the plan • 69
Defining security philosophy 70
Establishing guiding principles for security decision-making • 70
Balancing risk tolerance, innovation, and compliance pressures • 72

Aligning security with business objectives • 72
Setting your security vision, strategy, and initiatives 73
Reflecting on the vision • 74
Creating the vision statement • 75
Translating vision into long-term strategic pillars • 76
Documenting the initiatives • 76
Selecting meaningful metrics to track progress • 77
Key performance indicators • 78
Key risk indicators • 78
Presenting and cascading the security plan 78
Choosing the visual format • 79
The Cascade Pyramid • 80
The Security Plan Flowchart • 81
The Alignment Matrix • 81
Creating a one-page security plan overview • 82
Cascading the plan • 83
Security teams • 83
Cross-functional partners • 84
Executives and the board • 84
Maintaining strategic agility 85
Leveraging emerging risks and technologies to stay ahead • 85
Building a review rhythm • 86
Notes from the field with Renana 86
Case study: blank pages to shared vision • 86
Summary 87
Chapter checklist 88
Additional resources 88

Chapter 4: Charting the Course: Designing the Security Roadmap 89

Establishing priorities for security initiatives 90
Avoiding common prioritization mistakes • 90
Building the prioritization matrix • 91
Identifying prioritization factors • 91
Applying prioritization factors • 93
Visualizing priorities • 95

The Prioritization Quadrant Model • 95
The Sun Diagram Model • 96
Optimizing the security technology stack 97
Evaluating current tools • 98
Evaluating internally built, best-in-breed, and platform solutions • 99
Tool mapping • 100
Designing the future state • 101
Security simplification case studies • 102
Case study 1: platform to platform • 102
Case study 2: best-in-breed to platform and back • 103
Managing technical debt and legacy risks 104
Planning for phased implementation – security roadmap 106
Sequencing dependencies across initiatives • 106
Identify foundational prerequisites • 107
Look for hidden "enabler" projects • 108
Evaluate risk-based urgency • 108
Visualizing the roadmap • 109
Gantt chart timeline • 109
Swimlane timeline • 110
Measuring the roadmap's progress • 111
Reviewing roadmap performance • 112
Notes from the field with Renana 113
Case study: many voices to one roadmap • 113
Summary 115
Chapter checklist 115
Additional resources 116

Part 2: Building the Program 117

Chapter 5: Fueling the Program: Budgeting, Legal, and People Management 119

Making a credible security budget request 120
Building credibility with finance • 120
Laying the groundwork: earning the right to ask • 121
Deciding whether and how to ask • 122

Risk: understanding the problem you are solving • 122
Initiatives: clarifying what is possible • 122
Budget: anchoring the ask in context • 123
Timing: deciding when to act • 123
Leveraging the budget request template • 125
Option 1: minimum viable investment ("Safe to Drive") • 126
Option 2: recommended investment ("Right Fit") • 126
Option 3: accelerated investment ("Luxury") • 127
Navigating the ask with confidence • 127
Using procurement levers and contractual protections 128
Core procurement levers security leaders should know • 129
Additional contractual protections to be aware of • 130
Partnering effectively with procurement • 131
Navigating privacy incidents with legal 133
Preparing for privacy incidents • 133
Recognizing when a security incident becomes a privacy incident • 134
Shifting responsibilities from technical response • 135
Establishing attorney-client privilege • 137
Common pitfalls that undermine privilege • 138
Case study: when the forensic report was not protected • 139
Knowing when to escalate further • 139
Assessing materiality • 140
Considering when and how to notify executive leadership and the board • 141
Case study: when materiality is reassessed after the fact • 142
Making the call without owning the risk alone • 142
Building a high-performing team 143
Hiring with intention • 144
Setting expectations with recruitment • 144
Staying personally engaged in the interview process • 146
Using references as final signals • 148
Investing in your talent • 149
Using training strategically • 150
Coaching at scale • 151
Making appreciation visible • 151
Notes from the field with Renana 152

Case study: expanding the security-only lens • 152
Summary **153**
Chapter checklist **154**
Additional resources **154**

Chapter 6: Operationalizing Defense: Core Security Functions 155

Building the operational backbone of a security program **156**
Defining your objectives and key results • 157
Integration across business units • 158
Building incident response excellence **158**
Maturing incident response capabilities • 160
Evolving your role during incidents (reactive) • 160
Establishing incident response cadence (proactive) • 160
Assessing the current IR plan • 163
Leverage industry standards • 163
Proactive vulnerability and exposure management **168**
Defining the limitations of traditional vulnerability management • 169
Moving from vulnerabilities to exposure with CTEM • 170
Applying the CTEM framework • 170
Scoping: establish executive alignment • 172
Scoping: identify crown jewel assets • 172
Discovery: identify assets and exposures • 172
Prioritization: rank exposures using threat context • 173
Validation: confirm defensive effectiveness • 173
Mobilization: from insight to action • 173
Integrating threat intelligence into decision-making **174**
Tactical, operational, and strategic TI • 175
Building an intelligence-led defense • 176
Maturing the SOC: people, processes, and technology **180**
Leveraging the MITRE ATT&CK framework • 181
Maturing your SOC from reactive to predictive • 182
Security architecture as a strategic enabler **183**
Summary **186**
Additional resources **187**

Chapter 7: Protecting the Crown Jewels: Identity, Access, and Data Security 189

What are the "crown jewels"? 190
The need to protect identity and data • 191
Identity as the new security perimeter 193
Human and non-human identities • 195
Business risk of identity sprawl and privilege creep • 197
Understanding and classifying critical data 200
You can't protect what you don't know exists • 200
Data classification models for executives • 203
Ownership and accountability for data • 204
Data protection strategies across the data lifecycle 205
Data stages • 206
Encryption and key management • 208
Backup and recovery • 209
Managing third-party and supply chain risk 210
Fourth-party risk • 213
Identity and access risks in the supply chain • 213
Summary 216
Additional resources 217

Chapter 8: Navigating the Landscape: Governance, Risk, and Compliance (GRC) 219

GRC as a leadership function 220
Developing security policies and standards • 222
Policy development checklist • 226
Considerations regarding risk 226
Risk appetite and risk tolerance • 227
The risk register as a system of accountability • 228
Third-party and contractual risk • 229
Self-identified risks • 230
Roles and responsibilities • 230
Measuring what matters most • 232
Compliance as a baseline 232

Governance committees • 236
Summary **239**
Additional resources **239**

Part 3: Sustaining and Influencing **241**

Chapter 9: Speaking the Language: Mastering Executive Communication and Board Reporting **243**

Translating security risk into business impact **244**
Building your reporting framework **247**
Choosing consistency over ad hoc structure • 248
Selecting reporting elements for executive updates • 249
The threat landscape • 249
Industry or peer security incidents • 252
The risk posture • 253
The maturity assessment • 256
The compliance posture • 259
The roadmap • 261
The metrics • 263
Preparing for executive and board sessions **264**
Understanding executive and board reporting cadence • 264
Aligning before the session • 265
Drafting the narrative • 265
Reviewing and aligning • 266
Practicing your storytelling • 266
Case study: preparing for a first audit and risk committee update • 267
Finding the focus • 267
Aligning the message • 267
Conclusion • 268
Showing up for the meetings **268**
Leading the conversation • 268
Managing time and focus • 269
Reading the room • 269
Handling questions and dialogue • 270
Closing with the message to remember • 271

Notes from the field with Renana **272**
Case study: developing executive presence • 272
Summary **273**
Chapter checklist **273**
Additional resources **274**

Chapter 10: Championing Change: Cultivating a Security-First Culture **275**

Scaling security beyond the security team **276**
Establishing a security champions program • 277
Introducing or uplifting the program • 277
Sustaining engagement and developing future talent • 278
Implementing a BISO model • 279
Introducing or uplifting the BISO model • 280
Sustaining strategic business partnerships • 281
Designing security education programs **282**
Establishing continuous security awareness • 283
Defining the core components of awareness • 284
Delivering through diverse communication channels • 285
Delivering meaningful security training • 287
Distinguishing security awareness from security training • 287
Structuring training for different employee populations • 288
Reinforcing learning through testing • 289
Using phishing simulations as a learning tool • 289
Using tabletop exercises to improve decision-making • 290
Conducting live exercises to validate readiness • 291
Using gamification as part of testing • 292
Managing exercise documentation and legal privilege • 292
Building a security education calendar • 293
Influencing C-suite and board security culture **295**
Responding to emerging threats through proactive communication • 295
Establishing ongoing engagement • 296
Notes from the field with Renana **298**
Case study: making security everyone's business • 298
Summary **299**

Chapter checklist **300**
Additional resources **300**

Chapter 11: Proving Your Impact: Measuring Success and Demonstrating Value 301

Defining meaningful security metrics that align with business objectives **302**
Operational metrics vs. executive metrics • 305
Automating metrics and dashboards • 306
Aligning metrics with their owners • 307
Demonstrating the return on investment (ROI) of security initiatives **308**
Quantifying risk reduction • 311
Demonstrating value through business enablement • 312
Connecting maturity to metrics **313**
Communicating security outcomes to technical and non-technical audiences **315**
Translating technical achievements into business outcomes • 315
Summary **316**
Additional resources **317**

Chapter 12: The Resilient Leader: Sustaining Leadership and Managing Burnout 319

Recognizing the impact of security leadership on your well-being **320**
Recognizing the early warning signs of burnout • 321
Using a structured check-in • 322
Distinguishing temporary pressure from chronic overload • 322
Protecting your capacity to lead **323**
Managing your energy • 324
Preserving decision quality • 325
Protecting your calendar • 327
Setting boundaries and coverage • 328
Maintaining perspective beyond the role **329**
Building a personal support system • 330
Continuing to learn • 331
Maintaining career resilience in times of change • 332
Building resilience into the operating model **333**
Delegating as a resilience control • 334

Making room for recovery in the operating model • 335
Sustaining team capacity • 336
Notes from the field with Renana 337
Case study: when the blueprint had to change • 337
Summary 338
Sustained leadership checklist 338
Additional resources 339

Chapter 13: Conclusion: Beyond the First Year – A Journey of Continuous Evolution 341

Wrapping up your first year 341
Reflecting on your progress • 342
Documenting your thoughts • 343
Recalibrating expectations and priorities • 344
Preparing for your second year 344
Chapter checklist 346
Additional resources 346

Chapter 14: Unlock Your Exclusive Benefits 347

Unlock this Book's Free Benefits in 3 Easy Steps 348

Appendix: Security Executive Onboarding Questionnaire 351

Using this appendix 351
Understanding the business 352
Understanding governance and key stakeholders 352
Understanding the organization and talent 353
Understanding financials and vendors 354
Understanding risk, controls, and compliance 354
Understanding architecture and infrastructure 355
Understanding resilience, business continuity, and crisis management 357
Conducting security program deep dives 358
Establishing the security program baseline • 358
Ransomware readiness • 358
Security strategy and risk assessment • 359
Vulnerability and patch management • 359

Penetration testing and offensive security • 359
Monitoring, detection, and security operations • 359
Cloud security • 360
Incident response and recovery • 361
Threat intelligence • 361
Identity and access management • 361
Customer identity and authentication • 362
Governance, risk, and control • 362
Network security • 362
Endpoint security • 362
Application security • 363
Third-party risk management • 363
Insider threat and data protection • 363
External engagement and partnerships • 363
Business change and security enablement • 363
Artificial intelligence and machine learning governance • 364
Getting oriented to the organization 364

Other Books You May Enjoy 366

Index 369

Preface

You may be preparing for your first cybersecurity executive role, or you may have just stepped into it. In either case, the questions come quickly: Where should you focus first? Which relationships matter most? How do you turn what you learn into a credible plan, make difficult trade-offs, and demonstrate progress? These decisions can be challenging even for accomplished security professionals, especially when access to experienced mentorship is limited.

We wrote this as the book we needed when stepping into leadership roles. It brings together lessons from our different paths across government, consulting, academia, and large global organizations, and translates them into practical guidance you can use when preparing for an important conversation, working through a difficult decision, or challenging your own assumptions.

This is not a book you need to read once and set aside. Return to it throughout your first year, using the questions, frameworks, checklists, templates, and case studies when the need arises. Start with the chapter most relevant to the challenge in front of you, and adapt the guidance to your organization's structure, culture, maturity, risk tolerance, and regulatory obligations.

Who this book is for

This book is primarily for experienced cybersecurity professionals aspiring to executive leadership and for newly appointed executives navigating their first role. Deputy CISOs, heads of security, senior leaders taking on expanded responsibilities, and experienced executives joining a new organization can also use it as a practical reference. Readers need a foundational understanding of cybersecurity, but not expertise in every domain.

What this book covers

Chapter 1, *Laying the Foundational Bricks: The Initial Assessment*, provides a structured approach to understanding the business, conducting a listening tour, assessing security posture and culture, and validating initial observations.

Chapter 2, *Forging Alliances: Building Key Relationships*, explores how to assess and empower your team, partner with technology and business leaders, build a network of counselors, mentors, and sponsors, and engage key stakeholders, the C-suite, and the board.

Chapter 3, *Crafting Your Vision: Developing the Security Plan*, guides you in defining and communicating a business-aligned security philosophy, vision, strategic pillars, initiatives, and metrics while keeping the plan adaptive.

Chapter 4, *Charting the Course: Designing the Security Roadmap*, shows how to prioritize initiatives, rationalize the technology stack, address technical debt, sequence dependencies, and monitor roadmap execution.

Chapter 5, *Fueling the Program: Budgeting, Legal, and People Management*, covers budget credibility, procurement and contract protections, partnership with Legal during privacy incidents, and building a high-performing team.

Chapter 6, *Operationalizing Defense: Core Security Functions*, focuses on integrating incident response, exposure management, threat intelligence, security operations, and security architecture through clear cadences, standards, and outcome-driven measures.

Chapter 7, *Protecting the Crown Jewels: Identity, Access, and Data Security*, examines how to protect critical assets through identity and access management, data classification and lifecycle protection, and third-party and supply-chain risk management.

Chapter 8, *Navigating the Landscape: Governance, Risk, and Compliance (GRC)*, explains how governance supports leadership through practical policies, clear risk ownership, accountable risk registers, and audit and regulatory readiness, while positioning compliance as the baseline.

Chapter 9, *Speaking the Language: Mastering Executive Communication and Board Reporting*, shows how to translate security risk into business impact, build a consistent reporting framework, and prepare for and lead executive and board discussions.

Chapter 10, *Championing Change: Cultivating a Security-First Culture*, shows how to extend security ownership through Security Champions and BISOs, build an education program across awareness, training, testing, and annual planning, and engage senior leaders in shaping security culture.

Chapter 11, *Proving Your Impact: Measuring Success and Demonstrating Value*, guides you in selecting operational and executive metrics, demonstrating ROI and business enablement, connecting maturity to measurement, and communicating outcomes to different audiences.

Chapter 12, *The Resilient Leader: Sustaining Leadership and Managing Burnout*, examines sustained leadership pressure and offers practical guidance for managing decision fatigue, strengthening personal and team resilience, learning deliberately, and building a sustainable leadership model.

Chapter 13, *Conclusion: Beyond the First Year – A Journey of Continuous Evolution*, guides you in documenting first-year progress, explaining why greater maturity can reveal more risk, and preparing stakeholders and the program for year two.

Appendix: Security Executive Onboarding Questionnaire, provides you with a comprehensive set of questions and information requests to help you deepen your understanding of the organization. It covers business priorities, governance, stakeholders, talent, financials, risk, technical security capabilities, and operational resilience, serving as a practical reference for initial assessments and targeted deep dives.

To get the most out of this book

- Bring a foundational understanding of cybersecurity and experience working with technology, risk, and business stakeholders. You do not need experience across every security domain or a specific certification, framework, or technical platform.
- Use the book at the moments that matter: before a stakeholder meeting, budget discussion, incident, board session, or planning cycle. Return to the questions, checklists, templates, and exercises as needed, and adapt them to your role and organization.
- **Download the companion resources:** The companion resources referenced throughout this book, including templates, checklists, frameworks, and exercises, are available through the links provided at the end of each chapter.

Download the color images

Your purchase includes a color, DRM-free PDF copy of this book, ideal for viewing color images, screenshots, and diagrams. Refer to the *Free benefits with your book section* at the end of the *Preface* to unlock your PDF copy.

Conventions used

There are a number of text conventions used throughout this book.

Bold: Indicates a new term, an important word, or words that you see on the screen. For instance, words in menus or dialog boxes appear in the text like this. For example: "**Security Scorecards** help translate cybersecurity risk into measurable operational outcomes and reinforce accountability across technology teams."

> **Note**
>
> Warnings or important notes appear like this.

> **Tip**
>
> Tips and tricks appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book or have any general feedback, please email us at `customercare@packt.com` and mention the book's title in the subject of your message.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you reported this to us. Please visit `http://www.packt.com/submit-errata`, click **Submit Errata**, and fill in the form.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `http://authors.packt.com/`.

Share your thoughts

Once you've read *The Cybersecurity Executive's First Year Playbook*, we'd love to hear your thoughts! Scan the QR code below to go straight to the Amazon review page for this book and share your feedback.



https://packt.link/r/1806679337

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Free benefits with your book

This book comes with free benefits to support your learning. Activate them now for instant access (see the "*How to Unlock*" section for instructions).

Here's a quick overview of what you can instantly unlock with your purchase:







How to Unlock

Scan the QR code (or go to `packtpub.com/unlock`). Search for this book by name, confirm the edition, and then follow the steps on the page.





Note: Keep your invoice handy. Purchases made directly from Packt don't require one.

0

Introduction

After a lengthy interview process, you've finally landed the job. You've worked so hard to get to this point, whether this is your first time serving as an in-house practitioner after spending years as a consultant, climbing up the corporate ladder into a mid-level leadership position, or even being appointed as a first-time **Chief Information Security Officer (CISO)**.

The experience that earned you the role still matters, but you will need to quickly shift your perspective and apply new lenses to challenges you may have faced before. Decisions that once seemed primarily technical must now account for how the business operates and what its leaders value.

As a cybersecurity executive, you are responsible for protecting your organization's most valuable assets—its data and reputation. The stakes are high and the pressure to perform is immense. You need to serve as a subject matter expert, a business strategist, a diplomat, and a people leader all at once. How you position yourself in the first year is going to be critical for your success.

The challenges of your first year

Navigating your first year as a cybersecurity leader is a demanding experience. During your first year, you are expected to learn the business and its security environment while building credibility within an unfamiliar culture. At the same time, the program you inherited continues to operate or a new one needs to be built from the ground up. Decisions need to be made, incidents may arise, and the organization may look to you for direction even before you have completed your onboarding.

Strategic alignment and business integration

As an executive, your influence extends well beyond the decisions made within the security team. Technical accuracy remains important, but it will not be enough to build support or change behavior. Consider the following:

- **Translate Risk to Business Impact:** Your audience has changed. It is no longer enough to speak in technical jargon; you need to explain how a risk could affect the organization's operations, financial position, customers, or reputation. This translation helps leaders make informed decisions rather than simply asking them to trust the security team's judgment.
- **Gaining Executive Buy-In:** Support from the C-suite and board is built through consistent communication and credible follow-through. Leaders need to understand your direction, the trade-offs involved, and why a security investment matters to the business.
- **Building a Security Culture:** Security cannot operate solely within the security department. Over time, you will need to embed security into everyday business decisions and create shared ownership across the organization. This includes moving beyond traditional annual training to more relevant education, role-based engagement, and visible leadership support.

Security program management

While you are building alignment, you are also taking responsibility for a program shaped by decisions made before you arrived. Its team structure, budget, technology, and priorities may not reflect the direction you ultimately want to pursue. Before making significant changes, you need to understand why those decisions were made and which constraints remain relevant:

- **Managing Budget and Resources:** Your initial assessment may reveal more gaps than the current budget can address. You will need to determine which investments matter most and build a compelling case by connecting them to business priorities and risk reduction.
- **Navigating Team Dynamics:** Every team has existing strengths, capability gaps, and established ways of working. Understanding the people behind the program is essential before changing roles, adding talent, or addressing performance concerns.
- **Evaluating Technology and Vendors:** You may inherit a fragmented collection of security tools and vendor relationships. Beyond learning how those tools operate, you

will need to determine whether they support the security vision, where capabilities overlap, and where consolidation could reduce complexity.

- **Managing Competing Priorities:** Security priorities can shift quickly, and your team may already be managing alert fatigue or an overwhelming workload. You will need to prioritize deliberately and communicate the trade-offs so that leaders understand what will move forward, what will wait, and why.

External pressures

Even as you strengthen the program, the environment around it continues to change. New threats emerge, regulatory expectations evolve, and business decisions can introduce risks that were not part of your original plan. Your strategy must provide direction without becoming so rigid that it cannot respond to changing conditions:

- **Responding to the Evolving Threat Landscape:** New technologies and attack methods will continue to change the organization's exposure. You will need to evaluate whether the program's priorities still reflect the threats most relevant to the business rather than react equally to every new development.
- **Preparing for Regulatory and Legal Scrutiny:** Security executives operate under increasing regulatory attention and, in some circumstances, personal accountability. You will need to understand current obligations while working closely with Legal, Compliance, and Risk to prepare for emerging expectations.

These demands do not arrive in a predictable order. They overlap throughout the year and often require you to make progress in one area before another feels complete. That is why a traditional 90-day plan is only the beginning—and why the remainder of the first year deserves its own playbook.

What makes this book unique

Many leadership books focus on the first 90 days. That period matters, but it represents only the beginning of a security executive's transition. Drawing on more than 50 years of combined experience, we wrote this book to address what comes next: turning what you learn into a clear direction and leading the program through the remainder of the first year.

- **A Complete First-Year Journey:** The opening months help you establish context, build relationships, and understand the program you inherited. The rest of the year requires you to turn those insights into a strategy, secure organizational support, strengthen operations, and demonstrate progress. This book follows that broader journey beyond the initial assessment.

- **Security-Specific, Practical Guidance:** General executive guidance does not always account for the realities of leading a cybersecurity program. Throughout the book, we connect leadership decisions to situations security executives regularly face—from prioritizing investments and responding to incidents to communicating with the board. The frameworks, questions, and examples are intended to give you a practical starting point, not a formula you must follow exactly.
- **The Human Side of Security Leadership:** Technology and controls are only part of the role. Progress also depends on the relationships you build, the confidence you create with senior leaders, and your ability to develop a team that can carry the work forward. The book also addresses the personal demands of the role.

Our goal is simple: Provide you with a structured place to begin while leaving room for executive judgment. Your organization's culture, maturity, and priorities will shape how you apply the guidance. Use the book as a playbook you can return to throughout the year, adapting its lessons to the realities in front of you.

How to use this book

This book is organized around the general progression of a security executive's first year, but it does not prescribe a single reading path. You can read it from cover to cover, move directly to the chapters most relevant to your current situation, or return to different sections as new challenges arise throughout the year.

As authors, we come from different professional backgrounds and bring different areas of experience to the book. That difference is reflected intentionally in the chapters. Some operate more like field guides, offering practical actions, and templates you can use immediately. Others are more educational, providing the context needed to understand a topic. Security leadership requires both: sometimes you need a tool you can use on Monday morning, while other situations require a deeper understanding before you act.

At the end of each chapter, you will find templates that help put the guidance into practice. Treat them as starting points rather than finished solutions and adapt them to your needs.

The road ahead

We hope this book will serve you well during your first year on the job. By applying the principles and strategies outlined in these pages, you will be equipped to not only survive, but to thrive, transforming your role from a tactical function into a strategic driver of business success.

Part 1

Assessing and Setting Direction

This part covers the components of onboarding in a new cybersecurity leadership role. You'll learn how to understand the business and its security posture, conduct a focused listening tour, and establish the relationships needed to build a successful program. You'll then translate those insights into a clear security vision and a prioritized roadmap. By the end of this part, you'll have established your north star and a practical plan for executing against it.

This part of the book includes the following chapters:

- *Chapter 1, Laying the Foundational Bricks: The Initial Assessment*
- *Chapter 2, Forging Alliances: Building Key Relationships*
- *Chapter 3, Crafting Your Vision: Developing the Security Plan*
- *Chapter 4, Charting the Course: Designing the Security Roadmap*

1

Laying the Foundational Bricks: The Initial Assessment

The first few months in a new security leadership role shape how the organization will perceive you for years to come. You are not just stepping into a job; you are stepping into an ecosystem of people, processes, and technology. The success of your tenure will depend on how effectively you spend these initial weeks and whom you spend them with. Early interactions establish credibility, influence how teams share information, and determine how quickly you can begin driving change.

Most new leaders quickly realize how much there is to absorb. You are expected to understand the business model, meet dozens of stakeholders, review security reports, respond to ongoing issues, and begin forming opinions about priorities while building trust with a new team (or building one). Without a structured approach, it is easy to become overwhelmed by competing priorities.

The first stage of the role is primarily observational. Before defining strategy or launching major initiatives, strong leaders take time to understand how the organization operates, how decisions are made, and where the real risks lie.

This chapter focuses on that early stage and provides a structured way to gather the information you will need before shaping your strategy. By the end of this chapter, you will have a clear picture of the challenges and opportunities, enabling you to start building an understanding of how you want to approach the road ahead. You will be able to identify the stakeholders who shape cybersecurity decisions in your organization and understand how the business generates revenue and where security risks matter most. You will also learn how you can evaluate the current health of your organization's security program as well as recognize the cultural signals that influence security adoption.

We are going to cover the following key topics:

- Understanding the business context
- Conducting a listening tour
- Identifying existing security posture
- Evaluating the organizational culture
- Documentation and information validation

This period is not about immediate action or radical change. It is about laying foundational bricks through nonjudgmental information gathering. You should only attempt to make changes if you see threats to the organization that need to be addressed immediately.

> **Note**
>
> **Download the PDF version of this book**
>
> Your purchase includes a DRM-free PDF copy of this book, the code bundle, and a range of exclusive benefits. To unlock everything, follow the *Free benefits with your book* section in the *Preface*.

Understanding the business context

For those stepping up in their career journey, one of the most important lessons is that cybersecurity does not exist in a vacuum. After spending many years honing technical skills, moving into a leadership role requires a fundamental shift in perspective. Earlier in your career, your focus was likely on solving specific security problems such as remediating vulnerabilities, investigating incidents, or deploying new technologies.

As a leader, your responsibility changes. The question is no longer *"How do we fix this?"* but rather *"Which problems matter most to the business, and where should we focus our limited time and resources?"*

This shift—from technical execution to business prioritization—is one of the most important transitions in a security leader's career. The most effective security leaders make this transition early. They evolve beyond thinking only like security experts by adding an additional layer of business leadership responsible for risk, priorities, and trade-offs.

A security executive who cannot articulate how their work supports the company's revenue streams, customer relationships, and strategic goals will struggle to achieve their full potential. In this section, you will build that context by walking through a few core business dimensions. Together, these perspectives will help you connect cybersecurity decisions to business outcomes. This will be essential as you begin defining priorities and shaping your strategy.

General knowledge

Security should serve as an enabling force for most major business initiatives. The following are several basic questions you should ask (and attempt to answer) prior to your start date or during your first few weeks in your new role:

- What are the products or services your company offers?
- Who are the customers?
- Are there different customer segments?
- Is the company launching a new product, expanding into a new market, or undergoing a digital transformation?
- How many business lines are there? What are their growth strategies? Who is the leader of each business? How does each business line earn revenue?
- What are the major goals for the next 1–3 years?
- What are the **key performance indicators (KPIs)** the C-suite cares about the most?

While some of the questions above may seem trivial, a deep understanding of the answers to them will make you stand out from other technology executives early in your tenure in terms of business context. With this understanding, you can frame security risks in terms executives care about and ensure they focus their efforts on the areas that matter most.

Tip

In the past, gathering this type of business context often required hours or days of reviewing earnings calls, analyst reports, press releases, and industry articles. Today, **artificial intelligence (AI)** tools can help you quickly summarize publicly available information and accelerate your preparation before conversations with stakeholders.

Revenue

Security cannot protect all business processes equally and needs to prioritize the most critical revenue streams. For example, for a company that relies on e-commerce, an attack impacting availability such as **distributed denial-of-service (DDoS)** could have a direct correlation to revenue. For a **software as a service (SaaS)** company, a data breach that erodes customer trust could have similar consequences.

Every organization generates revenue differently, and those differences directly influence security priorities. Understanding how the company makes money helps you identify which systems, services, and customer interactions are most critical to protect. The following

questions will help you map security risks to the organization's most important revenue streams:

- How is revenue generated?
- Is it based on direct product sales, subscription models, advertising, a different model, or a combination of the models suggested here?
- What are the most critical revenue generation streams?
- Which revenue-generating activities would be most impacted by a security incident?

Once you understand the revenue model, you can translate technical risks into business consequences and focus your program on protecting what truly matters.

Operational dependencies

Every organization depends on a set of systems, services, and partners that keep the business running. As a security leader, identifying these operational dependencies helps you understand where a disruption would have the greatest impact. The goal is not to protect everything equally, but to recognize which assets and relationships are most critical to business continuity. The following are some questions you can consider:

- What are the crown jewels (i.e., the critical systems, servers, and databases) that the business cannot operate without?
- Are there on-premises data centers? Where are they located?
- How much of the critical infrastructure is hosted in the cloud? Which providers? Which other third-party vendors or external partners are essential to core operations?
- Are there documented business resiliency plans? Are they regularly exercised?

Once you understand these dependencies, you can better anticipate where security failures could cause the most disruption and align your efforts accordingly.

Regulatory and compliance landscape

It is also critically important that you understand what legal obligations and industry-standard requirements the business is subject to. Examples could include regulations from the **U.S. Securities and Exchange Commission (SEC)**, **New York State Department of Financial Services (NYDFS)**, **General Data Protection Regulation (GDPR)**, or **California Consumer Privacy Act (CCPA)**. These requirements shape many security decisions, and overlooking them can expose the organization to compliance gaps, reporting issues, or regulatory penalties. The following questions help you determine the compliance landscape for your organization:

- Which regulations are we subject to in each country we operate in?

- How do they impact business operations?
- How are regulatory changes monitored and incorporated into our security and compliance programs? Is there a dedicated Regulatory Relations team that helps manage the exam/inspection process?

Understanding these requirements gives you a clearer view of the constraints and responsibilities shaping the security program. With that foundation in place, you can move into the next stage of the process: speaking with stakeholders across the organization.

Conducting a listening tour

Once you have developed an initial understanding of the business, the next step is gathering perspectives from across the organization. This is where the listening tour becomes one of the most important activities in your first weeks as a security leader. These conversations help you understand how security is perceived across the company, uncover risks that may not appear in reports, and begin building relationships with the people who will influence the success of your program.

The listening tour is part of the broader early-stage assessment process. In practice, most leaders move through three overlapping steps during their first weeks: *learning how the business operates*, *speaking with stakeholders to gather context*, and *reviewing documentation and metrics to validate what they hear*. The listening tour sits in the middle of this process, allowing you to test early assumptions and identify areas that deserve deeper analysis.

Tip

The specific approach you should take as well as the exact questions will vary based on your role and industry. Use this section as a guide and adjust as needed to your environment.

One final piece of advice before we begin: the definition of what "good" looks like varies widely across organizations. Early in a new role, it can be tempting to evaluate everything against an ideal state. A more practical approach is using models, such as **Capability Maturity Model Integration (CMMI)**, to rate each area on a scale from one to five and compare that with where it needs to be for the organization to operate effectively (*Chapter 11* discusses how to assess program maturity and use a consistent maturity scale).

> **Tip**
>
> Remember that not every capability needs to be a five. With limited time, budget, and people, leaders often learn where "good enough" is appropriate and where improvement matters most.

For example, during a listening tour, a leader may discover gaps across several areas of the program, such as AI security, threat intelligence, and emerging technologies such as quantum computing. Using the maturity scale, they rate each area against where it realistically needs to be for the organization. Instead of trying to elevate every domain at once, the leader focuses first on the capabilities that support the systems most critical to the business. This approach builds credibility and allows the program to mature in a way that aligns with business priorities.

With this mindset in place, the next step is ensuring you create the time and structure needed to have these conversations effectively.

Owning your calendar

Before diving into the details of the listening tour, such as who you will meet with, the questions you will ask, and how to document what you learn, you need to have a solid plan in mind. You are ready to start, and many will ask (if they have not already) for your time. To be as effective as possible, you will need to be strategic in how you manage your time and which meetings you prioritize.

Much like a new president in the US receives a brief period of goodwill, most executives have a 90–100-day grace period to learn, assess, and conduct their initial assessment. At the end of this period, you should have a clearer understanding of the organization and the program. You should also have identified the program's key strengths, the areas that may require attention, and the expectations leaders across the business have for security.

In certain instances, however, such as a recent security incident or in heavily regulated industries, you may find yourself having to make decisions faster within the first 30 days. The plan presented here offers a balanced, hybrid approach between the traditional 100-day framework and a more agile 30-day version.

While there are multiple ways to approach your first few weeks, we suggest starting with the *Listening Tour Calendar Plan* outlined in *Table 1.1* and tailoring it to your specific needs. The schedule assumes you are either a direct report to the **chief information security officer (CISO)** or you are the CISO. The schedule in *Table 1.1* illustrates one way to structure the first weeks of your listening tour, but the exact order may vary depending on your role and the organization.

	Week 0	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7
Manager	X	X						
Directs		X						
Technology leaders		X	X	X				
Internal stakeholders				X	X			
External stakeholders					X	X		
Policy and report review			X	X	X	X		
Documentation	X	X	X	X	X	X	X	X
Validation							X	X

Table 1.1 – Sample listening tour calendar

The rationale behind this sequence is to begin with the people who can provide the most immediate context. Conversations with your manager and direct team help clarify expectations and current priorities. Meetings with technical leaders often reveal how security integrates with development and operations, while discussions with business stakeholders provide insight into risk tolerance and regulatory considerations.

For example, a leader joining a financial services company might start with their manager and security leadership team, then meet with infrastructure and engineering leaders to understand operational realities, before speaking with partners in legal, compliance, and risk. By the time those conversations occur, the leader is able to ask more informed questions and identify patterns across teams.

If you take the 30–45-day approach to perform your initial assessment, you will not be able to meet all internal and external stakeholders or review every policy or report. Accept that you are going to have incomplete information and may only see part of the big picture. For example, you may not yet understand most dependencies between systems, all ongoing security initiatives, or the historical reasons behind certain technology or risk decisions. Prioritize the conversations that will give you the most context early on and continue refining your assessment during the 45–100-day window.

Tip

Do not limit your listening tour to formal meetings. Look for opportunities to connect with colleagues over coffee, breakfast, or lunch during your first few months. Informal settings can lead to more candid conversations and surface context that may not come up in a scheduled meeting. Combining formal and informal interactions can give you a more comprehensive view of the organization.

Asking general questions

As you begin these conversations, lead with questions rather than conclusions. You may quickly identify decisions or practices you would have handled differently, but you likely do not yet understand the history or constraints behind them. Asking why something was done a certain way without offering a solution helps you uncover that context and build trust with the people who lived through those decisions.

Tip

A useful rule of thumb during onboarding is to use ten times as many question marks as periods, and ten times as many periods as exclamation points. If you can avoid exclamation points altogether, even better. The point is not the exact ratio, but the mindset: spend more time asking and learning than declaring what needs to change.

We have created a list of predefined questions you may want to include in most conversations. Starting with a consistent set of questions helps you compare perspectives across teams, identify patterns, and spot areas where expectations may not align. It also makes it easier to document what you learn and revisit those insights later when shaping your priorities. In addition to these common questions, you should prepare a few tailored questions for each stakeholder based on their role. For example, engineering leaders, legal partners, or business executives may each provide a different perspective on the program.

Note

The questions in this chapter are intentionally focused on the areas we believe are most important during your initial conversations. They are not intended to cover everything you may eventually want to understand. For readers looking for a more comprehensive starting point, *Appendix: Security Executive Onboarding Questionnaire* includes an expanded onboarding questionnaire covering business, governance, finance, risk, technology, and security topics. Use it as a reference and tailor it to your role, organization, and priorities.

Sample questions may include the following:

- What are the strengths of the organization (people, process, technology)?
- What are opportunities for improvement of the security program?
    - Were these discussed previously?
    - If so, was any progress made?
- What is the "definition of done"?
    - How do you know if the task was complete?
    - Do you agree with the definition?
    - If not, why not? What is missing for the initiative to be completed?
- What is the number one risk that keeps you up at night? Why?
- What does good cybersecurity look like to you?
- What is working well? What isn't?
- What are the KPIs the stakeholders care about the most? Why?
- How can security enable innovation in your department?

As these conversations reveal areas that require more depth, consider scheduling dedicated deep dive sessions with the relevant teams during your first 60 days. These sessions may run for several hours and should focus on the areas most important to your initial assessment rather than attempting to cover every security domain. They give the team an opportunity to walk you through how the capability operates today, while giving you time to understand the dependencies, gaps, and decisions that may require further attention.

Finish each meeting by asking for additional names of people you should meet with across the organization and add them to the *Listening Tour Calendar* shared earlier in this chapter.

Tip

When company policy permits, approved AI tools can help you transcribe meetings, summarize discussions, and organize key takeaways. Confirm which tools are approved for these conversations and what information may be recorded or entered.

Meeting your manager

Prior to your start date, ask your direct manager for a quick meeting to help you jump-start your learning journey. Keep in mind that not all managers will agree to meet, especially not until you complete your background checks. If they decline, keep the questions from the following table for your first meeting.

Regardless of when you meet, don't forget to go over key learnings from the interview process. This is an opportunity to validate your understanding and ask follow-up questions as needed. *Table 1.2* presents some sample questions to ask your manager:

Proposed Question	**Rationale**
Can you walk me through the organizational chart?	Gain further clarity over roles and responsibilities if you haven't done so already.
What presentations, commitments, or regular meetings should I be aware of in the coming weeks and months?	Reduce the element of surprise and gain clarity on what is important in the coming weeks/months.
Who are the key people I should meet with, internally and externally?	Don't limit yourself just to information security; your strongest allies may be sitting in another function without you knowing it.
How do you prefer to be kept informed about cybersecurity matters?	Establish communication protocols; never assume they are the same as your previous position (even if it was within the organization).
What quick wins would you like to see?	Identify immediate, high-impact improvements that will allow you to build credibility and demonstrate your impact.

Table 1.2 – Sample questions for your manager

Tip

If you joined the company as a CISO, your upper management may not be able to answer all these questions from the table. Consider skipping these questions with them and instead ask your directs for the details.

Meeting your directs

While it is tempting to only start with your immediate directs as a new leader, you should make a conscious effort to meet with team members at all levels, including frontline staff, to gain unfiltered insights. This helps to build trust and uncovers pain points that may be obscured in formal reporting.

The initial meetings with the team should be about listening and empathy. The team may be apprehensive about new leadership, so you should make every effort to explain that this is part of your learning journey with the organization.

In addition to the questions listed earlier in *Table 1.2*, you should also dive deeper to understand the security of the organization better. We will discuss supporting documentation later in this chapter. Key questions you should ask the team members include the ones from the following table:

Proposed Question	**Rationale**
What are the biggest security challenges and pain points you face today?	This helps to identify inefficiencies and frustrations.
What do you consider to be our crown jewels?	This helps identify the most valuable and sensitive assets that should be prioritized.
What are the technical and soft skills of the team, and where are the expertise gaps?	A thorough understanding of team capabilities is essential for resource allocation.
What worked and what didn't under the previous leadership?	This historical perspective helps you understand what is already in place.

Table 1.3 – Sample questions for direct reports

Tip

Through the discovery process, you may identify prior risks that were not registered by the company. It is your responsibility to document them in the risk register—failing to do so could result in personal liability consequences for you as well as the company's upper management.

Meeting technology leaders

Regardless of where security sits within the organization or your own professional background, your partners across the technology department are crucial to the success of your program. You may have spent much of your career in technology, or you may be entering the role from security, risk, consulting, or another function. Either way, do not assume you understand how technology operates in this organization. Leaders across software development, architecture, and infrastructure can provide critical context about the environment and how security integrates into their respective areas.

The questions outlined in this section are drawn from years of responding to security (and non-security) incidents, outages, and breakdowns. In retrospect, many could have been avoided if we had had a deeper understanding of the organization beyond security.

Through these early conversations, you build a foundational understanding of each domain and its connection to security. Later chapters will guide you in diving deeper into specific areas. While it may feel tempting to skip or postpone these conversations, taking the time to build these relationships early will set you apart as a more effective and well-rounded leader.

Tip

Most companies have more than one environment, such as corporate, production, development, and **quality assurance** (**QA**), and the answers may vary based on the environment. You likely will not be able to cover all environments in your early conversation. We recommend coming back to these questions in follow-up meetings as you get fully up to speed.

Software development

The way security integrates into development directly impacts the resilience of the company's products. By gaining a deeper understanding of the process, you'll be able to identify

shortcomings and potentially risky areas that need to be prioritized as part of the security roadmap. Here are some security questions to consider for software development:

- What product development methodologies do you follow, such as Agile, Scrum, and Waterfall?
- Has the organization adopted specification coding or other AI-assisted code development practices?
- How are security requirements incorporated into the **software development lifecycle (SDLC)** today?
- What mechanisms are in place to identify and remediate vulnerabilities during coding, testing, and release?
- What governance exists to ensure new products and features meet security standards before release?
    - When was the governance model introduced?
    - Are there any products or features that were released prior? If so, how do you get them to comply with the current standards?
- What metrics are used to measure the maturity of secure development practices?

Note

Pay close attention to the difference between products and features—you should inquire about both. Although teams sometimes use the terms interchangeably, they represent different levels of the system. For example, a company might offer a customer portal as a product, while capabilities such as login, document upload, and notifications are features within it. Understanding this distinction helps clarify how security work maps to the software being delivered and addresses a common scenario where security gaps will be addressed as a "feature," not a bug, by software development teams.

Architecture

Architecture sets the foundation for security. If security is not factored into early design decisions, the company is both introducing risks to the environment and facing longer, more costly remediation efforts. Consider the following architecture questions:

- How is security embedded in architecture decisions from the start for new products?
    - What is the philosophy for existing products?

- What frameworks or standards guide architectural decisions? How well are those adhered to?
- How do you evaluate trade-offs between scalability, performance, cost, and security when designing systems?
- What are historical architectural gaps that could expose the organization?
    - Is there a risk issue with action plans documented for each?
- What governance processes exist to review and approve new technologies before adoption?

Infrastructure

Infrastructure plays a massive role in day-to-day operations and has a direct impact on security outcomes. Close coordination is required from your early days, as many of the policies and requirements will be implemented by the infrastructure teams. The following are some sample questions you might ask:

- What were the top three infrastructure outages related to cybersecurity attacks or misconfigurations?
- What changes did you make following these incidents?
- Who owns **identity and access management (IAM)**, including **Active Directory (AD)** and privileged access?
- What is the current state of config management and vulnerability remediation across environments?
- How are base images updated or rehydrated, for both on-prem and cloud assets?
- What is the company's policy for **bring your own device (BYOD)** and **virtual desktop infrastructure (VDI)**?
- What is our remote access infrastructure architecture? Is it protected with multi-factor authentication?
- Do we allow Remote Desktop Protocol from the Internet?
- Do we enforce conditional access policies on all SaaS applications?
- What is our firewall architecture?
- When did the company conduct the last Business Continuity/Disaster Recovery exercise?
- What was the scope and what were the outcomes?

Meeting internal stakeholders

Now is the time to gain a broader understanding of the company by having conversations with stakeholders outside of IT leaders. While some may not seem as obvious, a well-rounded security executive needs to have at least a basic understanding of each group and ensure they have a point of contact to reach out to when needed.

> **Note**
>
> The list provided here includes some of the common stakeholders, but not all of them. Evaluate what needs to be added or modified based on your specific needs.

Business leaders

Business leaders can help you understand how security affects the areas of the organization they are responsible for. Who you meet with should reflect your role and scope. For a CISO, this may include business heads or executives reporting to the CEO. If you are a CISO direct, focus on the leaders responsible for the business units, products, or functions your team supports. The goal is to understand where security can better support their priorities and where they see risk or friction today. Consider asking:

- What are your top priorities over the next 12 months?
- Where does security currently create friction for your organization?
- Where could security better support or enable your objectives?
- What security or technology risks concern you most?
- Are there major business or technology changes coming that the security team should be aware of?

If your role includes board exposure, consider extending your listening tour to relevant board members or committees to understand their expectations and concerns about cybersecurity. If you do not interact with the board directly, ask your manager what topics are regularly discussed and what concerns have surfaced.

Legal

This is likely one of the most important relationships you need to establish. Most security executives work closely with the legal department on a variety of matters, ranging from security incidents to compliance and contract negotiations. In addition to the questions outlined earlier in this chapter under *Regulatory and compliance landscape*, you should gain an

understanding of the relationship with outside counsel, how to determine if an incident is material/reportable, and the details of any prior incidents that you should be aware of.

- Who serves as our outside legal counsel?
    - What is their fee structure and who pays for their services?
- What protocol do we have in place for attorney-client privilege?
- How do we determine if a cybersecurity incident is material, and how is the decision documented?
- How many material incidents were identified in the last 12–24 months?
    - Were they all reported to upper management and the board? Could you please share the details?
- Are there any contractual obligations the security team must meet?
    - How are new obligations being communicated to the team?
- What protocol do we follow to engage with law enforcement agencies?
- Which legal clauses are included in our contract?
- What is the process in case of deviation from them?
- Would the company indemnify the CISO during a cyber incident both during and after employment?

Human resources

Security engages with **human resources (HR)** regularly throughout the employee lifecycle, from onboarding to offboarding, to mitigate risks such as unauthorized data access or retention of privileges. Insider threats and employee termination are the top two common topics every security executive should understand:

- Which group is responsible for responding to insider threats?
- What is our process for managing them?
    - Do we have documented response and escalation protocols in place? Are there any gaps?
- What role does security play during employee terminations?
    - Is it a manual or automated process?
- Where is access cut off, and how do we verify the process was successfully completed?
- If we allow remote work, are policies in place to prevent the workforce from working from a country other than their work country when not on business travel?
- How are fraudulent IT workers prevented from being hired?

- Do we have the ability to detect over-employment?
- Can you share examples of large-scale/material security incidents that took place over the last 12–24 months?
    - What learnings did we gain from them?

Physical security

Physical security protects people and company assets. Similar to HR, from time to time there will be a need to partner with physical security on areas that fall under multiple entities' responsibility such as insider threat and terminations. Close coordination enables a smooth flow between digital and physical safeguards.

- What process do we follow when we need to acquire a physical asset for forensic investigation, such as a laptop?
- How do we respond to physical intrusions or insider threats?
- During on-site events, what physical security controls are available, such as badges and visitor management?

Risk and internal audit

Risk and internal audit serve different roles, yet both can give you an independent view of the security program. Risk helps you understand how the organization evaluates cyber risk and where ownership resides. Internal audit assesses whether controls and governance are operating as intended. Some security leaders may initially experience these functions as a source of friction. With the right relationship, however, their independent perspective can surface blind spots and strengthen your decisions.

Understanding their upcoming schedule and how it is going to impact ongoing commitments can allow you to streamline your efforts. For example, you may learn that an internal audit or regulatory review is already planned for later in the year. Coordinating early allows you to account for that work in your roadmap.

As the relationship develops, there may be opportunities to adjust the timing or sequence of a review when business priorities change. That flexibility should never influence the independence of the review or its conclusions. The goal is to reduce surprises and coordinate the work more effectively. Use the following questions to understand how risk and internal audit view the security program:

- How is our risk framework structured?

- What are the upcoming assessment and audit areas for cybersecurity in the next 12 months?
    - How did you prioritize these areas?
    - Can security impact the schedule?
- What were common themes identified as part of previous audits?
- Which are the top three areas you believe we should focus on?
- Which firm serves as our external auditor?
    - Do they use the same audit rating as risk and internal audit?

Finance and procurement

While they control budgets, vendor relationships, and financial risk exposure, finance and procurement are often overlooked in an early listening tour by security executives. Building relationships with these teams can significantly benefit the security program. They can help you understand how security investments are funded, what procurement constraints may affect new tools, and how contracts with vendors can be structured to reduce risk. Climbing the corporate ladder requires us to master how we manage our budget. An understanding of basic terms, such as **operating expense (OpEx)** vs. **capital expense (CapEx),** will also allow you to have more meaningful conversations with the business. We will discuss this topic further in *Chapter 5*. Consider the following questions:

- What are my capital and operating expenditures, including tools, vendors, and personnel?
    - Which tools are up for renewal by quarter?
- When does our budget planning cycle begin?
- Do we use a calendar year plan or a separate fiscal year plan?
- What process is used to evaluate and onboard new vendors?
    - How are security risks assessed during procurement?
- What security and privacy clauses are included in contracts?
- How do you track and manage critical vendors that have access to sensitive systems or data?

Third-party risk management

Third-party cyber risk may be managed within cybersecurity, enterprise risk, procurement, or another function, depending on the organization. Early in your listening tour, identify who owns the process and understand how cybersecurity risk is evaluated across the vendor lifecycle. The objective at this stage is not to redesign the program, but to understand how

responsibilities are divided and where the current process may need further attention. Consider asking:

- Who owns third-party cyber risk assessments?
- How do you determine which vendors require a security review?
- How are identified risks tracked, escalated, and accepted?
- How are critical vendors monitored after onboarding?
- Where do you see the biggest gaps in the current process?

Meeting external stakeholders

Some of the most useful insights on security do not come from within the company, and your view would not be complete without gaining an external view on the program. Consulting firms, auditors, and vendors can provide a different point of view to complement the insights you collected so far. We have included them last in the listening tour to reduce potential bias and allow you to ask for their opinion on specific matters.

Consulting firms

Meeting the top 2–5 consulting firms that provide services to your company will allow you to learn about the types of projects they conduct, the frequency, and some of the unwritten impressions they have of your program. Some of the meetings may seem like a sales opportunity to them, so be clear about your intention of information gathering and ask them to share any relevant reports ahead of the meetings. The following questions will help you gather the relevant insights:

- Which projects did you deliver in the last 12 months?
    - What were the top observations among them?
    - Were there any red flags I should be aware of?
- If you needed to rate the maturity of the domain/program, how would you rate it and why?
- How do you compare the overall program against our peers?
    - What low-hanging fruit should I focus on?

External audit

Gaining an early understanding of how your auditor views the program will allow you to evaluate your program and priorities. They may not be fully aligned with the top risks you or the company have identified, and you will need to be ready to defend them. Ask them these questions:

- How do our controls compare with industry peers?

- Do you have any major areas of concern?
- What upcoming regulatory or compliance changes should we be preparing for?

Note

We assume you have prior experience working with external audit and know what to ask, what to say, and, most importantly, what not to say. If you don't, please seek guidance within the company prior to setting up the meeting. In certain instances, you may want to delay this meeting to a later date, once the strategy has been defined.

Vendors

Finally, vendors often hold objective product-usage data that may not be visible internally. Ask them to compare what the organization has licensed with what is deployed and actively used. Consider an organization in which a vendor showed that a product costing more than $1 million annually was significantly underutilized.

That discovery created two possible paths. The organization could expand its use of capabilities it was already paying for, potentially reducing the need for another purchase. Additionally, if any capabilities were no longer needed, it could right-size the contract at renewal and redirect the savings to a higher-priority item. The conversation also helped identify whether configuration changes or additional training could close the adoption gap. When budgets are constrained, underutilization is more than a procurement issue; it is an opportunity to recover value from an existing investment.

You may choose to meet only your top vendors at this point. They can be defined based on annual spend (start with the highest) or impact to the program (such as endpoint protection and **security information and event management (SIEM)**). Consider these questions:

- What services/tools are we paying for?
- What can be done to improve utilization/consumption? Why are we not doing it currently?
- How can we learn about upcoming features? How do we submit feature requests?
- What **service level agreements (SLAs)** are in place? How are they being tracked?
- How often do we conduct a business review? Who attends those meetings?

In conclusion, a listening tour provides you with valuable perspective on how security operates across the organization. As you reflect on your discussions, begin organizing the insights you gathered, such as what appears to be working well, where concerns were raised repeatedly, and where additional clarity may be needed. These patterns will form the foundation of your early priorities.

To complete the picture, you should now examine the program itself. In the next section, we will review how to assess the current security posture using available reports, documentation, and metrics.

Identifying the existing security posture

After completing your listening tour, the next step is to validate what you heard by examining the current state of the security program. Conversations provide valuable perspective, but they often reflect individual experiences. To build a more accurate picture, you need to review the documentation, metrics, and artifacts that describe how the program operates.

The specific metrics, policies, and reports you must review will vary depending on the role, so you may need to add or modify the suggestions below.

Tip

While it is tempting to focus only on the last 30 days or last quarter, make an effort to review the content for the last 12 months. It will allow you to better identify themes and patterns that would otherwise remain hidden for an extended period.

It is also important to recognize that this step does not replace an independent third-party assessment. As part of your first 90 days, consider commissioning an independent cyber program assessment, particularly if a recent one does not already exist. A qualified external firm can provide an objective view of the program, challenge assumptions, and identify gaps that may be difficult to see from inside the organization. This assessment should complement —not replace—your own initial assessment. Comparing the two perspectives can help validate your conclusions and highlight areas that warrant deeper attention.

Security metrics

Security executives rely on metrics to measure the effectiveness of security controls, track progress against goals, and communicate outcomes in a way that resonates with upper management. Metrics help translate technical performance into business-relevant insights. By presenting trends and outcomes through clear data, security leaders can show where investments are paying off and highlight areas of concern.

We have included a list of some of the top metrics to review, but it is by no means complete. Depending on the role you play, you will need to adjust the specifics.

You should also take the time to understand how each metric is constructed (specifically, how the numerator and denominator are defined). Small changes in scope, such as which assets are counted as "in scope" or what qualifies as a "resolved incident," can significantly change the story your metrics tell.

Asset inventory

You cannot protect what you don't know exists. Start by identifying the organization's source of truth for systems, applications, and databases across both on-premises and cloud environments. In most organizations, you will quickly hear that the list is incomplete, so begin with the best version available.

If the organization has a dedicated asset management function, it is a natural starting point. However, it is also valuable to ask engineering, infrastructure, and cloud platform teams the same questions, as each group typically maintains a different view of the environment, and comparing those perspectives often reveals gaps:

- Do you have assets on-premises, in the cloud, or hybrid?
    - Which cloud providers do you use?
- How often is the list being updated?
- What is the process to add new assets to it?
    - Is there a difference between on-premises and cloud?
- How are assets being removed?
- What is the percentage of assets with known end-of-life or unsupported status?

Tool and control coverage

With an understanding of the asset inventory, you should evaluate whether the tools you have invested in are deployed and delivering value. These questions will help:

- What percentage of in-scope assets are protected by each tool? Calculate the metric separately for endpoint, data protection, encryption, and identity tools.
- What tools are used to monitor the security posture of the on-premises and cloud assets?
- Which tools are sending data back to your SIEM?
    - What is the process to validate the effectiveness of the logs? Could you actually use them for correlation?

Threat exposure management

Many large-scale incidents start with a non-remediated vulnerability. We recommend taking a holistic approach by reviewing infrastructure, application, penetration testing (pentesting), vulnerability disclosure, and bug bounty findings using these questions:

- What is the number of findings by category?
- What is the breakdown by severity?

- What is the subset that is Internet-facing?
- How are findings assigned to owners?
- What are the SLA requirements per category? Are they all the same, or do they vary from one category to the other?
- How many findings are remediated within SLA, in a 12-month view? How many were not?
- For current findings, if they weren't remediated, what is the plan to remediate them?

Security incidents

Incidents are unavoidable. Incidents as well as near-incidents tell a story about the health of the response process. Use these questions to gather the necessary information:

- Do we have a documented incident response plan?
- How often do we exercise the plan?
- How does that plan fit with any company crisis response plans?
- Does the plan specify the roles and decision rights of participants during an incident?
- Does the plan specify the triggers and timing associated with reporting of incidents to regulators and law enforcement?
- What tools are used for investigations?
- What is the number of incidents, mean time to detect, and mean time to mitigate by month in the last 12 months?

Policies and governance

Security policies form the foundation of the organization's governance framework. As a new security executive, it is important to understand not only what policies exist but also how they are maintained, communicated, and enforced across the business:

- How many security policies exist, and how are they organized?
- Which industry standards do they align with (such as NIST or ISO 27001)?
- What does the approval process look like?

You should also attempt to cover the company's risk issues and risk register, where identified risks, their scoring (likelihood and impact), and remediation plans are documented. As you go through the initial assessment, you will want to create self-identified issues for any misses.

Assessments and audit reports

Written documentation provides a deeper level of insight beyond high-level conversations. Reports tell a story, highlight patterns, and provide context that may otherwise be missed. For example, an audit report may reveal recurring access control issues across multiple systems, or

a penetration test may highlight architectural weaknesses that teams have learned to work around over time.

If time does not allow for reviewing all materials, ask your team to help prioritize. At a minimum, it is valuable to review one report from each category to understand the structure, yet it is essential to come back and complete the review at a later date prior to setting up your strategy. Here are the questions to help you with your review:

- What penetration test reports were issued in the last 12 months, including red and purple teams?
    - Are there any themes, or were these findings identified in prior reports?
    - How are findings tracked?
    - How are findings validated post remediation?
- What audits and assessments were completed in the last 12 months?
    - What is the typical audit cadence for each topic? How were the audit topics selected?
    - How are findings tracked? Is the same process consistent with pentest findings?
    - What escalation occurs if remediation SLAs are breached?
- When was the last cybersecurity maturity assessment?
    - How often are these assessments conducted?
    - Which domains received the lowest and highest ratings? Why?
    - How are recommendations tracked?

Different areas often follow their own remediation processes, but this can create silos and inconsistencies in how risks are addressed. If a unified approach is not already in place, consider streamlining these processes as part of your strategy, which will be discussed in greater detail in *Chapter 3*. Doing so can reduce duplication, improve accountability, and deliver greater operational efficiency.

Initial risk landscape analysis

The last step as part of your security posture evaluation is to assess the threat environment. What may seem like a catastrophic outcome in one industry will seem negligible in another. For example, during an assessment, a team might discover that the organization does not have **network access control (NAC)** in place. At first glance, this may appear to be a major gap. However, the CISO may already be aware and have chosen to prioritize other risks first, such as improving identity controls, addressing critical vulnerabilities in internet-facing systems, or strengthening monitoring and incident response capabilities. What initially looks like a major

issue can sometimes be a conscious prioritization decision based on the organization's most pressing risks. The following questions will help you obtain a clear understanding:

- What are the current and emerging threats specific to our industry? How are our peers being targeted?
- What threat intelligence sources are leveraged (feeds, law enforcement briefings, **Information Sharing and Analysis Centers (ISACs)**)?
- How actionable is the information? How is it being measured?
- How do geopolitical developments or third-party dependencies (such as suppliers, critical vendors, or cloud service providers) impact business operations?
- Are there specific threat actor groups that have targeted us in the past?

After reviewing the organization's security posture, the next step is to evaluate the culture surrounding security.

Evaluating the organizational culture

Security programs are shaped not only by technology and processes but also by culture. Understanding how leaders and teams perceive security will help you determine how easily new initiatives can be introduced and where additional education or alignment may be required.

Even the most well-designed strategy can struggle if it does not fit the organization's culture. Some organizations naturally integrate security into everyday decision-making, while others view it primarily as a compliance requirement. Recognizing these dynamics early will help you adjust your approach and identify where relationship-building or communication will be most important. In this section, we will explore several aspects of organizational culture that influence the success of a security program:

- Leadership attitudes toward security and how executives prioritize risk
- Collaboration between teams across security, engineering, risk, and business units
- Employee awareness and behavior related to security practices
- Organizational risk tolerance and how decisions are made when trade-offs arise

Assessing leadership alignment

The tone at the top sets the direction for how security is perceived across the organization. Many organizations view security as a compliance checkbox and will only address security needs after a major security event, such as a data breach. In this case, it is going to take more time to educate upper management on the importance of integrating security into day-to-day operations.

The questions below are best directed to executive leadership and key decision makers across the organization, such as your manager, business executives, and other members of the leadership team who influence risk decisions:

- How often is security discussed at upper management meetings and the board?
- What happens when a topic is brought up out of the standard reporting cycle?
- Who makes the final call regarding incident reporting to regulators and the board?

Identifying risk appetite and ownership

Risk management heavily depends on clarity of ownership. Often, security needs are deemed the sole responsibility of the security team. We strongly believe a healthy culture views it as a shared responsibility across the enterprise. Every employee has a role to play in protecting the business, from an intern to the CEO. These questions will help you determine ownership and appetite:

- How do you hold teams accountable for addressing security needs?
- Is there a documented corporate risk appetite?
- What number is a "big" number when it comes to operating losses? Loss of customers? Number of customer records lost?
- How tolerant is the organization of trade-offs between speed-to-market and secure practices?

Reviewing cross-functional collaboration

Effective programs thrive when security teams are viewed as trusted partners to the business and serve as business enablers. This is true across compliance needs as well as the development lifecycle. Consider these questions:

- Is there a "three lines of defense" model? If so, how well do the three lines of defense work together?
- When do development and business teams engage with the security team to identify requirements?
- Does the security organization have the "veto" right to stop a risky step? Was it ever used?

Note

It takes time to create a healthy culture, where most of the questions above are being addressed. Identify the most crucial areas you need to focus on and make them a priority as part of your strategy (to be discussed further in *Chapter 3*).

The next step after gathering information is to effectively document and validate it.

Documentation and information validation

Gathering information is only the first step. Documentation once took nearly as much time as the listening tour itself. When company policy permits, AI can now accelerate transcription, summarization, and organization. Even so, documentation still requires a little bit of art. You need to decide what deserves attention without losing the context behind it. You also need to distinguish a stakeholder's observation from your own interpretation.

Over the years, we have seen several leaders struggle to organize their thoughts and use the information to fuel the next phase of their journey. In this section, we will explore several ways to structure and validate the information you have collected:

- Organizing notes and observations to identify patterns across conversations, reports, and assessments
- Validating key findings to distinguish confirmed issues from assumptions or individual opinions
- Connecting insights across sources to understand how business context, security posture, and culture interact
- Preparing the foundation for strategy development so the next phase of your work is grounded in evidence

Avoiding common mistakes

Most leaders will go through the information gathering phase 6–10 times during their career. Given our shared consulting background, we have gone through the initial assessment process 100+ times and identified these common mistakes that can be easily avoided:

- Using exclamatory language or making statements such as "Why on Earth did you do it that way?" or "Wow. At my last place, we implemented this 15 years ago." Be careful when referring to specific prior employers (that annoys everyone), but be especially careful about expressing displeasure with the current environment, at least until you understand the history.
- Not taking notes at all and relying on your memory: This is going to fail you. In this time of information overload, you consume so much data. What may seem important after one meeting will be gone or mostly forgotten after a full day of meetings.
- Using multiple note-taking methods without organizing them in one place: Whether you type, write by hand on a digital device, or take handwritten notes on paper, keep everything in one company-approved digital location. The format matters less than

being able to find, compare, and use the information later. If you capture notes elsewhere, move or link them to that location before the end of the day.

- Scheduling back-to-back meetings without time for reflection: It can be tempting to condense the listening tour by scheduling as many meetings as possible within a short period. Without time to process each discussion, details begin to blur, and you may later rediscover information that was already shared. Leave five to ten minutes between meetings to capture the key takeaways and prepare for the next conversation.
- Using AI without confirming company policy: AI tools can accelerate note-taking, but listening-tour conversations may contain sensitive business or security information. Before using one, ask: "*Which AI tools are approved for recording or summarizing meeting notes, and what information are we prohibited from entering?*" Do not assume that a tool approved for general use is appropriate for these conversations. Confirm first so convenience does not create unnecessary data exposure risk.

Using documentation templates

Early observations need to be carefully collected into themes. We personally like to keep the structure simple, allowing executives to quickly organize the details, connect the dots, and present to other stakeholders without having to spend weeks pulling a deck together.

- **Wins**: Start by articulating what is working well as part of your domain and give credit to those who were there before your time. Many new leaders skip this phase, which in turn makes their new team less receptive to feedback down the road. If you take the time to document and discuss the existing strengths, both the team you inherited and your superior will appreciate the positive view.
- **Areas of opportunity**: During the listening tour, you will likely identify dozens of items that require at least some change. If you try to list them all in this document, you will lose the attention of your audience quickly, especially if they do not consider themselves cybersecurity experts. Focus on the top 5–10 opportunities that truly move the needle for the program. For the remainder that did not make it to the top, keep them in your "parking lot" list and set up a cadence to review it on a monthly or quarterly basis. This list will become handy as you set up the strategy.
- **Action plan**: Until you have a moment to gather your thoughts and update the strategy for your area, you need to quickly turn the opportunities into actions. What support do you need to execute against the plan in terms of people, budget, or impact to the schedule? How will you bring your team and stakeholders along on the journey?

Note

Security leaders often think about security needs without considering the impact they are going to have on the business. Work with your technology leaders to understand the role they play in executing your plan.

Checking for legal liability

The notes you take, both handwritten and digital, create a paper trail. Without the right legal understanding, you could unintentionally create personal and company liability for security issues. As an example, if you choose to change the calculation of a certain KPI (such as the number of incidents or vulnerabilities that were not mitigated within SLA), your company may now be subjected to additional regulatory reporting.

Note

Prior to putting formal observations in writing, consult with your in-house and/or outside counsel. Follow their guidance on how to document and label the material.

Validating your observations

Before closing this phase, take time to review and pressure-test the observations you have captured. What initially seemed like a clear opportunity or issue may, in fact, be based on incomplete context or a misinterpretation. Catching these early is far better than presenting them in a multi-stakeholder meeting and having someone explain why your conclusion was off track.

For example, you might conclude that a team is ignoring vulnerability remediation timelines after seeing several overdue items in a report. However, a follow-up conversation may reveal that the systems in question are scheduled for retirement or are already part of a larger infrastructure migration. Without validating the context, the issue could easily be misinterpreted.

To strengthen your findings, validate them with a handful of trusted advisors, people who understand both the business and your role. Share your insights, preferably in a live conversation rather than over email or slides alone. A real-time discussion allows you to ask follow-up questions, uncover missing context, and refine your interpretation. Finally, enter these sessions with curiosity, not defensiveness. The goal is to verify that your observations are accurate and relevant.

Notes from the field with Renana

As a consultant, I facilitated a wide range of engagements for Fortune 500 clients. While no two projects were alike, many required going through the listening tour process dozens of times. Since the approach wasn't well documented, I developed the methodology described in this chapter and refined it over the years through hands-on experience—often in the aftermath of some of the most significant security breaches of that time.

When I transitioned from consulting to becoming an in-house practitioner at PayPal, I followed the same playbook. It served me well as a consultant, but this time, things felt different. The stakes were higher, the dynamics more personal, and the feedback loop much shorter.

One of the first lessons I learned was the importance of approaching everything with curiosity and an open mind. It is easy to step into a new environment and start critiquing what you see, pointing out gaps in maturity, or wondering aloud why things were done a certain way. You have to remember that the people you are talking to were often there when those systems, processes, or tools were built. They may take pride in what they created, even if it is not what you would have designed. Taking the time to understand the context before making decisions about people, processes, or technology earns trust and gives you the full picture.

I also learned the value of giving credit wherever possible. A listening tour can sometimes feel like an interrogation, especially for those on the receiving end. A sincere thank-you or acknowledgment of good work costs nothing, yet it can completely change the tone of a conversation and open doors that might otherwise remain closed.

I discovered that the "paper trail" matters more than I thought. Understanding what to document—and what to keep conversational—is an art form every security leader needs to master. If you have not encountered this before, talk to your legal team early. They can help you navigate what should be recorded formally versus what is better left off email or meeting notes.

Finally, I wanted to know it all right away, but the reality is it is going to take time to get fully up to speed. In my opinion, in certain instances it is better to make decisions based on partial information than to be paralyzed by analysis. At PayPal, I knew my perspective was incomplete and had to come to terms with it. I used an asterisk, literally or figuratively, to note that my initial observations were just that: initial, letting my stakeholders know that I reserved the right to revisit and refine my conclusions in a few months. None of them objected to this approach.

Over time, I realized that the listening tour is not just a one-time onboarding exercise. It is a mindset. The most effective leaders never stop asking questions; they treat every new project,

challenge, and relationship as another opportunity to learn. Leadership is not about having all the answers on day one. It is about asking the right questions and evolving your perspective on the go.

Summary

In this chapter, we explored how to develop an informed view of the organization during your first weeks as a security executive. We examined how understanding the business context, conducting a listening tour, reviewing the current security posture, and assessing the organizational culture can shape your initial perspective. We also discussed how to document and validate your observations without treating preliminary conclusions as final.

In *Chapter 2*, we will build on this initial understanding by examining how to develop strong relationships, establish credibility, and earn the trust of key stakeholders across the organization.

Chapter checklist

- Understand the business context. Identify how the organization creates value and where disruption would cause the greatest harm. Use that knowledge to place security decisions in the right business context.
- Conduct a listening tour. Meet with your manager, your team, key business partners, and relevant external stakeholders to understand expectations and uncover potential blind spots.
- Establish an initial view of the security program. Review metrics and existing documentation, noting what is supported by evidence and what still needs to be validated.
- Assess the organizational culture. Observe how security decisions are made, who owns risk, and how effectively teams work together.
- Document and validate your observations. Store your notes in an approved location, reconcile conflicting information, and capture the themes that will inform your next steps.

Additional resources

- Listening Tour Calendar Plan template: `https://bit.ly/CISOBook2`
- Documentation template: `https://bit.ly/CISOBook3`

2

Forging Alliances: Building Key Relationships

One of our favorite relationship quotes is "*If you want to go fast, go alone. If you want to go far, go together.*" In security leadership, this could not be more true. Too often, executives focus on their own domain, overlooking the bigger picture. Success in this role depends heavily on your ability to build meaningful relationships beyond the security team.

The early days with an organization provide a rare opportunity to set the tone for how you are going to be positioned within the company. If used wisely, you will establish yourself as an open, business-oriented leader who can inspire confidence and drive alignment. Ultimately, it is the people who determine whether your strategy succeeds or stalls.

In this chapter, we will explore practical steps for managing relationships at every level of the organization, starting with your immediate team and extending to peers, stakeholders, the C-suite, and the Board of Directors. We will also provide practical frameworks to help you begin developing your own relationship management approach and creating the foundation for long-term impact.

Specifically, we will cover the following topics:

- Assessing and empowering your team
- Collaborating with IT and business leaders
- Identifying key internal and external stakeholders
- Engaging with C-suite and the board

Assessing and empowering your team

While the listening tour described in *Chapter 1* was mostly focused on understanding the current state of the program, the most important aspect of your program is *people*. You can have a bold vision as to how you are going to transform your domain, but without an engaged and capable team driving day-to-day execution, you will not get very far.

Whether you have inherited a team of five or five hundred, your first priority as a new leader is to understand who they are, how they operate, and what motivates them. You need to assess the current state of your team versus your desired state, identify gaps in skills or structure, and determine what actions are required to bridge any gaps.

Introducing the Team Assessment Tool

Teams are formed through shared work toward a vision. Over time, they develop written (and unwritten) norms and a hidden culture code known only to those who have been a part of the team.

This code influences their ethics, how they collaborate, make decisions, and respond to change. Your goal is to quickly understand the context that shaped the team, including leadership styles and priorities that brought them to where they are today.

You weren't there when this culture and context were created, so the stories you hear will only reveal part of the picture. Approach every conversation with curiosity and humility, focusing on patterns rather than isolated events. Understanding why things are the way they are will help you as you begin to craft your vision.

To bring more consistency to this process, we suggest using the *Team Assessment Tool* as part of your conversations with individual team members. This tool is a framework consisting of some questions or considerations and is designed to help you assess employees across the security organization. *Table 2.1* consolidates the questions introduced throughout this section into a framework that can help guide evaluations and growth planning over time.

Area	**Assessment Question**	**Status**	**Notes/ Action**
Skills Alignment	Are they demonstrating expected technical and soft skills?	Exceed/Meet/Developing	

Area	Assessment Question	Status	Notes/ Action
Role Alignment	Are they in the right role?	Current role/Different security role/Other internal role/External transition	
Champion Potential	Do they act as champions?	Demonstrated/Emerging/ Not observed	
Counselor	Do they have a counselor?	Yes/No/Action needed	
Mentor	Do they have a mentor?	Yes/No/Action needed	
Sponsor	Do they have a sponsor?	Yes/No/Action needed	
Recognition	Did they go above and beyond? Were above-and-beyond efforts recognized?	Yes/No/Action needed	
Growth Potential	Were they given stretch assignments?	Yes/No/Not yet ready	

Table 2.1 – Team assessment reflection questions

The process is not intended to place employees into simple "high" or "low" performer categories. Instead, it will help you better understand how individuals align to their current responsibilities, where they may need additional support, and how their strengths can be best applied across the organization.

The *Team Assessment Tool* should be treated as a living document, not a one-time onboarding exercise. As employees grow, priorities shift, and responsibilities evolve, your assessments should evolve as well. At a minimum, revisit the exercise annually as part of the performance review cycle; ideally, recalibrate it quarterly. Additionally, check-ins with counselors, mentors, and sponsors can help determine whether employees are progressing as expected or would benefit from new assignments, additional exposure, or different development opportunities.

Tip

As you apply this framework, follow your organization's HR guidance and leverage any formal talent management tools already in place. The goal is not to replace existing processes, but to broaden the lens through which you evaluate your team. Too often, security leaders assess employees primarily through technical capability. Long-term success also depends on softer skills, such as communication, collaboration, adaptability, and the ability to drive change across the organization.

In the sections that follow, we will look at the areas listed in *Table 2.1* in more detail.

Evaluating skills and role alignment

With the framework established, the first step is to understand whether employees are positioned to succeed in their current roles.

In many consulting firms, employee management models acknowledge that career growth can take different forms. From day one, employees are taught that there are multiple career paths —growing *within* the organization or expanding *beyond* it as an "industry executive." It can take time to accept that not everyone will climb the traditional leadership ladder. Yet over time, many consultants come to appreciate the flexibility and honesty of this model, as it allows individuals to find the path best aligned with their strengths and aspirations.

The same mindset can help security leaders manage and grow their teams more effectively. Not every employee will grow in the same direction, and part of your responsibility is to identify where individuals can contribute most successfully—whether in their current role, a different role within security, or elsewhere in the organization.

When assessing each employee, consider the following questions and answers:

- **Are they demonstrating the technical and soft skills expected at their level?**
    - Yes, exceed
    - Yes, meet
    - No
- **Are they in the right role within the organization?**
    - Good fit for the role
    - Better suited for a different role within security
    - Potential fit for a different team within the organization
    - May be better positioned outside the organization

The answers to these questions help identify current performance in addition to long-term fit and growth potential. Over time, patterns will begin to emerge across the organization, highlighting where additional coaching, role adjustments, restructuring, or hiring may be needed. This exercise can also uncover hidden strengths and identify employees who may be underutilized or individuals who could thrive with different responsibilities or development opportunities. Most importantly, it creates a more objective foundation for talent decisions, reducing the risk of relying solely on first impressions or isolated interactions.

Tip

To deepen your assessment, supplement your observations with additional context. Utilize "deep dive" sessions to help you learn, but also to assess the technical, business, and soft skills of those presenting. Review past performance evaluations to identify recurring trends, consult with HR to better understand career history and development goals, and gather informal feedback from peers and stakeholders who regularly collaborate with the employee.

As you evaluate skills, role alignment, and long-term potential across the organization, patterns will begin to emerge around the individuals who consistently influence others, embrace change, and elevate the teams around them. These individuals could be your *champions*, discussed next.

Identifying champions

Many leaders begin designing the organizational structure in their first 90 days.

As you assess your team, look for individuals who can help bring your vision to life. These team **champions** are not always the most senior employees or the loudest voices in the room. They demonstrate initiative, take ownership, and have earned the respect of their peers. Because others trust them, they can model desired behaviors and help build momentum for change.

The next question in the Team Assessment Tool focuses on identifying champions and individuals with the potential to influence change across the organization:

- **Do they influence others and help advance change?**
    - Demonstrated
    - Emerging
    - Not observed

> **Tip**
>
> Look for evidence in everyday work. Note the employees who take initiative rather than wait for direction, collaborate effectively across teams, demonstrate influence beyond their immediate role, and often embrace change as an opportunity for improvement.

On more than one occasion, I needed to transform the vulnerability management program, which we will discuss in more detail in *Chapter 6*. At first glance, the program appeared stagnant and the team seemed comfortable with the status quo. After spending more time with them, I realized they already possessed the qualities needed to succeed. They had a strong technical background, deep operational knowledge, and credibility within the organization. What they lacked was empowerment and belief that change was possible. The challenge was not capability. Historically, the program operated with limited executive support, and over time the team became accustomed to security updates and remediation efforts being delayed or deprioritized. As the backlog continued to grow, the status quo gradually became normalized.

Instead of making staffing changes, I focused on increasing their visibility, involving them in strategic discussions, and assigning stretch goals. Over time, many of them emerged as champions. Within 12 months, the team reduced critical vulnerabilities out of SLA by 97%. Just as importantly, the program evolved from a reactive operational function into a scalable capability better equipped to manage the growing volume and velocity of modern security threats. The experience reinforced an important lesson for me as a leader: In most cases, teams do not need to be replaced. They need the opportunity to lead, knowing that you have their back.

Once you have identified these individuals, bring them closer by involving them early in discussions about your vision and upcoming initiatives. They can serve as a feedback loop, helping you sense the team's readiness for change and signaling where additional communication or support may be needed. They can also mentor others and help raise the bar for the overall organization. Champions may stand out early, but avoid making permanent judgments about the rest of the team too quickly. People often reveal different strengths, motivations, and potential over time. The next section examines how to look beyond those initial impressions.

Moving beyond first impressions

According to research (see `https://www.forbes.com/sites/serenitygibbons/2018/06/19/you-have-7-seconds-to-make-a-first-impression-heres-how-to-succeed`), the first few seconds of each interaction are critical for making a strong first impression. While these early

observations can provide useful signals, they rarely tell the full story of an employee's potential, adaptability, or long-term impact within the organization.

For instance, someone on the team may not show up to the first meeting as the best version of themselves. They may be dealing with a major incident at work, organizational uncertainty, or personal challenges outside of work, all of which can affect how they engage professionally and personally. Therefore, as you assess your team, avoid making permanent conclusions too quickly. Talent assessment requires observing employees across different situations, interactions, and levels of responsibility over time.

The next questions in the *Team Assessment Tool* focus on validating early observations and creating opportunities for employees to demonstrate growth potential beyond their current responsibilities. Ask this:

- **Have they been evaluated across multiple situations and interactions?**
    - Yes
    - Partially
    - No
- **Have they been given stretch opportunities beyond their current responsibilities?**
    - Yes
    - No
    - No, need to assign stretch opportunities

Observe employees in different environments and circumstances, for example, by attending internal team meetings, cross-functional discussions, and stakeholder interactions to better understand how they communicate, influence others, and respond under pressure. These interactions often reveal qualities not visible in one-on-one settings, such as collaboration, adaptability, and influence.

Additionally, watch for both verbal and nonverbal cues. For example, early in one of my leadership roles, I inherited an employee who consistently received negative feedback from his manager. He was described as difficult to work with, non-collaborative, and resistant to change. Based on the feedback alone, it would have been easy to form a quick conclusion about his fit within the organization.

Shortly afterward, his manager left the company, giving me the opportunity to work with him more directly. To my surprise, the experience was completely different from what I had expected. Not only was he collaborative and thoughtful, but he also brought valuable operational insights, challenged assumptions in productive ways, and consistently proposed creative solutions to complex problems. Over time, he became one of the most trusted voices on the team.

The experience served as a reminder that assessments formed through secondhand opinions or limited interactions are often incomplete.

> **Note**
>
> Strong leaders create enough space and time to evaluate people themselves before making permanent decisions about talent.

What is equally important is that some employees may appear comfortable simply because they have mastered their current responsibilities over many years. While this creates stability, it may also limit growth. Stretch opportunities can help reveal adaptability, initiative, leadership potential, and renewed motivation. Start with smaller challenges and gradually increase complexity as confidence and capability grow.

Identifying potential is only the beginning. Now, your role shifts toward creating an environment that helps individuals continue to develop and succeed.

Empowering through development and recognition

The goal is to create a culture where *everyone* feels empowered to make decisions and has a strong sense of ownership across the entire team, not just a few. Empowered teams do not just execute tasks; they innovate, challenge the status quo, and elevate the overall maturity of the program.

Creating that culture requires deliberate investment in people's growth, recognition, and alignment with the broader mission. When employees understand how their contributions connect to business objectives and feel supported in their development, performance naturally follows.

Counseling/mentoring/sponsorship framework

Throughout your career, different individuals will help shape your growth in different ways. During my time at Ernst & Young, the organization emphasized three important support roles that contributed significantly to employee development: **counselors**, **mentors**, and **sponsors**.

While the same person may fulfill more than one role, each serves a distinct purpose in helping individuals grow professionally. For example, a manager may act as both counselor and mentor. However, few people naturally have all three roles covered. The elements are summarized in *Figure 2.1*:

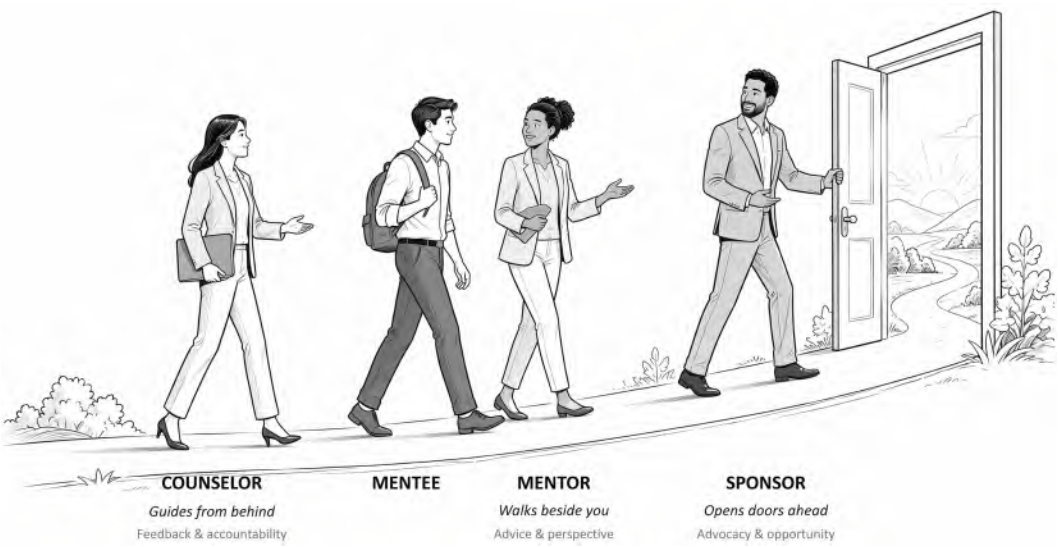


Figure 2.1 – The roles supporting professional growth

A **counselor** is typically a manager or direct supervisor responsible for providing structured feedback, evaluating performance, and helping align individual goals with organizational priorities. Counselors play an important role in day-to-day development by identifying skill gaps, encouraging growth, and helping employees navigate their career progression within the organization. In many ways, a counselor pushes from behind, providing accountability, direction, and support to help individuals continue moving forward.

A **mentor** is an experienced professional who offers guidance, perspective, and a safe space for open discussion. Unlike a counselor, mentors are not responsible for formal evaluations. Instead, they help individuals think through challenges, navigate complex situations, and learn from experiences beyond their immediate role. Mentors often serve as sounding boards, right beside you, sharing lessons from their own careers and providing insight that helps employees develop judgment, confidence, and a broader perspective over time.

A **sponsor** is typically a senior leader who actively advocates for an individual's advancement. Sponsors go beyond providing advice; they use their influence to create opportunities, increase visibility, and recommend individuals for important initiatives or leadership roles. Sponsors pull you upward by opening doors and advocating on your behalf in conversations you may not be part of. Their support can accelerate growth and career progression within or outside the organization.

Using the counselor/mentor/sponsor model, the next questions in the *Team Assessment Tool* focus on whether these structures already exist and where they can be enhanced. If you don't know the answer, engage in a dialog with your staff and peers.

- **Do they have a counselor?**
    - Yes
    - No

Ideally, the answer to this question should consistently be "Yes," as managers typically serve as counselors within the organization. As you evaluate your organizational structure, consider whether employees have the right counselor or if you need to make changes to the structure. As you already know, managers have a direct impact on engagement, development, and retention, while ineffective management often drives employees away.

- **Do they have a mentor?**
    - Yes
    - No
    - No, action needed

Not every employee will naturally build mentorship relationships on their own. As you assess the organization, consider whether individuals, especially high performers and emerging leaders, have access to professionals who can provide guidance beyond day-to-day responsibilities.

- **Do they have a sponsor?**
    - Yes
    - No
    - No, action needed

Sponsorship is often one of the biggest differentiators in long-term career growth. High-performing employees may still struggle to advance if no senior leader is actively advocating for them behind closed doors. As part of your assessment process, identify individuals who would benefit from greater visibility, strategic exposure, or leadership sponsorship.

If time permits, conduct the exercise for all individuals on your team. At a minimum, you should ensure all high-performing individuals have the answer to the mentor or sponsor questions as "Yes." Investing in these support structures compounds over time, helping develop the next generation of leaders within the organization.

Note

A word of caution: mentorship and sponsorship relationships do not always produce the outcome originally intended. In some cases, these relationships may help individuals realize that a different role—or even a different organization—is better aligned with their long-term goals. This happened to me twice with my mentees, and I had to come to terms with a different outcome than intended. While this can be difficult in the short term, supporting employees in their professional growth increases trust, strengthens culture, and reinforces your reputation as a leader who genuinely invests in people.

Amplifying success through recognition

Recognition is one of the most powerful (and underutilized) tools for driving performance and engagement. In a world where attention is often focused on the here and now, the importance of pausing to acknowledge effort and success can easily be overlooked. Intentional recognition reinforces the behaviors you want to see repeated and fosters a culture of accountability, trust, and excellence.

Acknowledging effort and success publicly signals appreciation and creates a sense of belonging. Whether it is a shout-out during a team meeting, a handwritten letter, or an email highlighting someone's impact, these gestures remind people that their work matters.

Empowerment begins when recognition is tied to trust. When you acknowledge someone for taking initiative or solving a problem, you send a clear message: *I trust your judgment*. That validation encourages others to think more creatively, take calculated risks, and find new ways to deliver value. Over time, recognition shifts team culture from dependency to accountability as people stop waiting for direction and start driving outcomes themselves.

The last question in the *Team Assessment Tool* allows you to keep track of recognition.

- **Did they go above and beyond their defined responsibilities, and were they recognized for their efforts?**
    - Yes, and they were recognized
    - Yes, but they were not recognized
    - No

As you establish a strong understanding of your own team, the next step is expanding those relationships beyond the security organization. Security leaders do not succeed in isolation, making strong collaboration with IT and product essential to driving meaningful progress.

Collaborating with IT and product leaders

In most organizations, security operates as part of the technology and/or product groups. While the groups report to the same leader, they are usually measured on different outcomes. In this section, we will explore how to build bridges between the teams through the introduction of shared goals using the *Security Scorecard*, which we introduce later in this section.

Understanding competing priorities

Everyone says cybersecurity is their top priority, right? In practice, the answer often changes when another team needs to stop their work to address the security need. As AI accelerates vulnerability discovery, infrastructure, engineering, and security teams face growing pressure to evaluate and remediate issues more quickly. That pressure makes competing priorities increasingly difficult to ignore.

Consider a common scenario: The security team identifies a critical vulnerability that must be remediated immediately to limit potential unauthorized access. Addressing it means asking the infrastructure team to pause existing work and redirect resources for several days.

If this happens occasionally, IT leaders will usually respond quickly, recognizing the urgency and business risk involved. But as these interruptions become more frequent, frustration begins to build. What was once a quarterly disruption can quickly become a weekly—or even daily—operational challenge. Delivery timelines slip, product releases are delayed, and customer commitments are impacted. Suddenly, security and IT teams find themselves operating with seemingly competing priorities.

So how do we better align security goals with the rest of the organization? It starts with recognizing that both teams are working toward the same broader business outcomes, even if they are measured differently.

Aligning around shared business outcomes

One of the most important lessons for any security executive is understanding that while the security teams are measured by risk reduction, the rest of the IT team is measured by speed, stability, and delivery. This naturally creates tension when operational priorities compete for the same resources.

While both organizations ultimately support the same business objectives, they often evaluate success through very different operational lenses. *Table 2.2* highlights common examples of how IT, product, and security teams may prioritize and measure outcomes differently. Understanding these differences is critical to building empathy and improving communication.

IT/Product teams often focus on	**Security teams often focus on**
Story points and sprint velocity	Vulnerability remediation timelines
Product delivery deadlines	Risk reduction and resiliency
Planned work completion rate (Jira or an equivalent work-tracking tool)	Critical vulnerabilities outside SLA
System uptime and availability	Threat exposure and attack paths
Feature releases and customer commitments	Security control effectiveness
Infrastructure stability	Incident prevention and detection
Deployment speed and operational efficiency	Secure configuration and hardening
Reducing operational friction	Reducing exploitable risks
Platform scalability and performance	Compliance and regulatory requirements
Technical debt impacting delivery	Security debt impacting exposure
Application functionality	Secure-by-design implementation
Mean time to restore service (MTTR)	**Mean time to detect (MTTD)** and **mean time to respond (MTTR)**
Engineering resource allocation	Prioritization of security remediation
Business enablement and innovation	Long-term organizational resilience

Table 2.2 – Different operational perspectives between IT and security teams

Neither perspective is inherently wrong. To bridge this gap, security leaders should understand how their IT and product peers are measured. Once you understand their priorities, timelines, and operational pressures, it becomes easier to position security initiatives in a way that supports broader business objectives rather than always competing against them.

In many cases, improving operational priorities also strengthens security outcomes. For example, investments focused on system uptime and availability often improve organizational resilience and recovery capabilities during **distributed denial-of-service (DDoS)** attacks.

Similarly, efforts to reduce technical debt frequently address **end-of-life (EOL)** systems, unsupported software, and architectural weaknesses that also contribute to security risk.

How these conversations are framed also matters. Security initiatives are far more likely to gain support when teams understand how they align with work already underway rather than viewing them as entirely new obligations imposed by security. Positioning security as an enabler of operational resilience, stability, scalability, and long-term efficiency helps the conversation.

That said, even when you speak the language of the business and align security initiatives to operational priorities, alignment is not always guaranteed. In some organizations, the culture may prioritize speed and delivery almost exclusively, with limited tolerance for conversations about long-term risk. In others, leaders may understand the security concerns intellectually but still underestimate the likelihood or business impact of a major incident until they experience one directly.

As an executive, part of your responsibility is recognizing and documenting these tensions when they exist. Over time, unresolved trade-offs between business priorities and security risk should be formally captured, tracked, and communicated through the organization's governance and risk management processes. We will discuss this topic in greater detail in *Chapter 8*.

To strengthen alignment across teams, organizations often introduce shared metrics and accountability frameworks that make security outcomes more visible throughout the business.

Introducing the Security Scorecard

Security Scorecards help translate cybersecurity risk into measurable operational outcomes and reinforce accountability across technology teams. Instead of discussing security only during incidents or escalations, scorecards create an ongoing mechanism for tracking performance, identifying trends, and increasing visibility across the organization.

Effective *Security Scorecards* are typically structured at two levels:

- An organizational security score representing overall enterprise security health
- Individual leader-level scores measuring the security performance of specific infrastructure, engineering, cloud, or product organizations

This structure allows executives to quickly understand overall risk posture while also creating accountability within the teams responsible for improving it.

The specific metrics included in a *Security Scorecard* will vary based on organizational maturity, regulatory requirements, industry, and risk profile. *Table 2.3* provides examples of commonly used KPIs that can serve as a starting point for building a scorecard framework.

KPI	Rationale
Number of vulnerabilities out of SLA, by severity level	Measures how well the team meets defined remediation timelines.
Number of pentest findings	Reflects the effectiveness of security controls. A higher number may signal systemic issues or areas needing investment as part of the SDLC.
Number of pentest findings outside SLA	Tracks whether identified vulnerabilities from penetration tests are being addressed within agreed timelines. Demonstrates risk prioritization.
Number of accounts without **multi-factor authentication (MFA)**	Highlights identity-related risk and potential attack surface. Drives prioritization of MFA rollout to reduce credential-based compromise.
Security awareness training completion rate	Measures employee engagement with foundational security education. Higher rates correlate with reduced human error and social engineering risks.
Number of architecture/ network exceptions	Tracks deviations from standard security policy (e.g., unpatched systems or unsupported configurations). High counts may indicate process breakdowns.

Table 2.3 – Sample Security Scorecard KPI categories

Each KPI category contributes to both the leader-level score and the overall organizational score. Categories are weighted based on business risk and organizational priorities, allowing leaders to focus attention on the areas with the greatest impact on enterprise security posture.

For example, vulnerability management may carry a higher weight than awareness training because of its direct relationship to exploitable risk. While each KPI is measured individually, the aggregated score provides leaders with a simplified benchmark for determining whether security posture is improving or deteriorating over time.

Figure 2.2 illustrates how different technology organizations may perform across security categories, with the individual KPI ratings ultimately contributing to both leader-level and organization-level aggregated scores.



Figure 2.2 – Sample Security Scorecard structure

Over time, *Security Scorecards* begin changing the nature of operational conversations. Discussions shift away from isolated remediation tasks and toward broader trends, measurable outcomes, and long-term risk reduction. For instance, instead of debating how many patches were applied or awareness sessions were completed, leaders can evaluate whether the organization's overall security posture is improving over time.

Tip

While it may be tempting to use percentages for simplicity, proceed with caution. Percentages can obscure the true risk picture if not calculated carefully. For example, excluding assets with poor coverage from the denominator can make weak performance appear "green." Always ensure that the underlying data and calculations reflect reality, not optics.

Some organizations may take this a step further by formally introducing scorecards into executives' performance evaluations. Prior to taking that step, give teams sufficient time to review the metrics, understand expectations, and improve baseline performance.

Tip

Remember: the goal is not to penalize teams, but to create transparency, alignment, and shared accountability across the organization. Just as important, remember that scorecards alone do not build partnerships. Metrics may create visibility, but long-term collaboration still depends on trust, communication, and strong working relationships across teams.

Managing stakeholder relationships

Strong relationships across the organization are essential to turning security priorities into action. This section focuses on building a partnership mindset and introduces the *Circles of Influence* framework to help you identify key stakeholders, determine the right cadence for engagement, and make time for those relationships.

Building a partnership mindset

Developing a true partnership mindset requires security leaders to broaden their perspective beyond the boundaries of their own function. It is about understanding the goals, pressures, and priorities of the teams you work with and finding ways to align security with their success.

To build collaboration, security should be embedded in the daily work of development, product, and IT teams. This means being present in their discussions, understanding their timelines, and offering solutions that enable progress rather than slow them down. At times, you may have to make difficult trade-offs, balancing risk reduction with business agility.

For example, imagine a product team preparing to launch a major customer-facing feature before a critical business milestone. During testing, the security team identifies several medium-risk pentest findings that should be addressed. Rather than immediately demanding that the release be delayed, a partnership-oriented security leader works with the team to evaluate the actual risk, determine whether compensating controls exist, and prioritize the most critical findings first. In many cases, this approach allows the business to meet its objectives while still reducing risk in a thoughtful manner.

Partnership does not mean compromising security standards or accepting unnecessary risk. It means working together to understand trade-offs, identify practical solutions, and make informed decisions that support both business objectives and security outcomes.

Creating the stakeholder map

Partnerships do not happen by accident. As organizations grow, the number of stakeholders, competing priorities, and communication demands increases significantly. To build influence at scale, security leaders need a deliberate approach for identifying, prioritizing, and managing relationships across the business.

The *Circles of Influence* framework provides a structured way to organize stakeholders based on influence, relevance, and engagement frequency. This is a powerful tool I have been using for the last several years, helping me move from transactional exchanges to deeper relationships.

Figure 2.3 illustrates the four stakeholder tiers and their suggested engagement cadences:

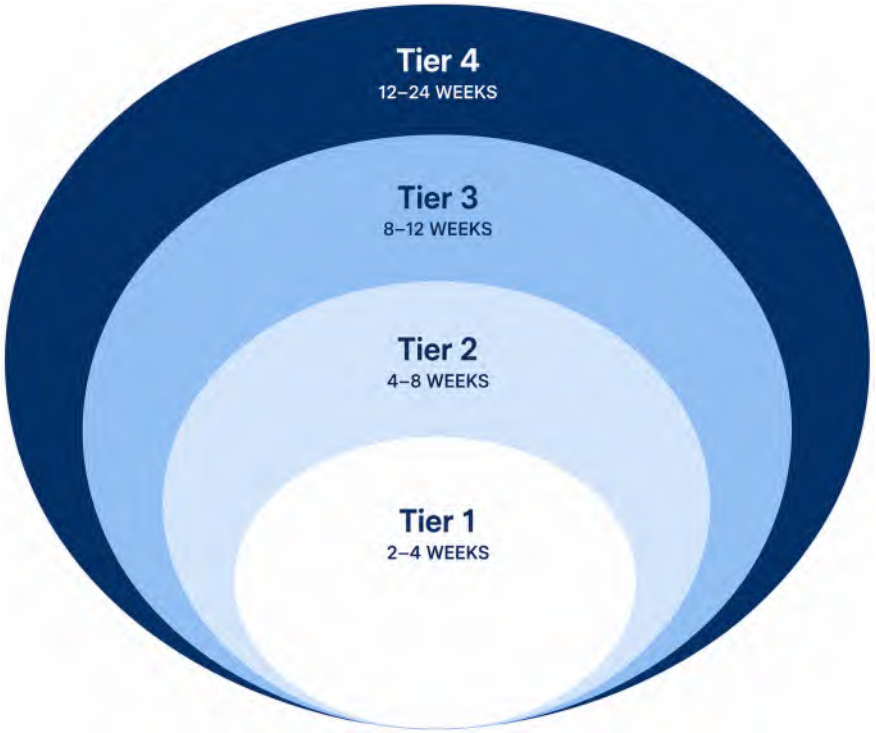


Figure 2.3 – Multi-tier approach for stakeholder engagement

In *Chapter 1*, we suggested a list of stakeholders you should meet as part of your onboarding journey. Now is the time to review the list again and establish cadences for your interactions going forward. It is also an opportunity to identify who else should be added and who should be removed. Start by creating a list of all the stakeholders you currently engage with as part of your job, as well as stakeholders you should engage with but have not had the opportunity to. Be as specific as possible and write down names, not just functions or departments (such as "HR" or "Legal"). Your list should include internal and external contacts.

Here are some important factors to keep in mind:

- This exercise focuses on your work map. You may also want to create a personal map down the road, but for now, focus only on your professional network and colleagues, not your friends.
- All levels matter. The goal of this map is not to prioritize seniority but to help you determine the right level of engagement and frequency of interaction.
- Treat your stakeholder map as a living document, not a one-time activity. Revisit and update it regularly as your role, responsibilities, and organizational dynamics evolve.

Determining cadences

Once your list is complete, reflect on your top professional goals in the role and assign each individual to one of the four tiers. You can follow a simple principle: *the closer the stakeholder is to Tier 1, the more frequently you should interact with them*. Determine placement based on their influence and relevance to your objectives. Are they decision makers, informal influencers, or supporting contributors? This exercise will help you focus your time and energy on where it will have the greatest impact.

Establishing clear communication cadences strengthens alignment, maintains visibility, and prevents relationships from becoming purely transactional or crisis-driven. *Table 2.4* provides sample engagement cadences based on stakeholder priority and relationship type. You are encouraged to adapt it as you see fit.

Tier	Cadence	Rationale
1	2–4 weeks	Core relationships that directly enable you to perform your day-to-day responsibilities. These individuals are essential collaborators or decision makers for your key initiatives.
2	4–8 weeks	Stakeholders who support your goals and can influence Tier 1 relationships; they may be senior leaders or cross-functional partners whose alignment is critical to your success.
3	8–12 weeks	Individuals who benefit from visibility into your team's progress. Regular updates help them understand the broader impact of your work and maintain organizational alignment.

Tier	Cadence	Rationale
4	12–24 weeks	Strategic connections where maintaining the relationship matters more than frequent interaction. Periodic engagement ensures ongoing awareness.

Table 2.4 – Communication cadences by stakeholder tier

While every organization is structured differently, most security executives will find that a relatively small number of stakeholders account for the majority of decisions impacting the security program. *Figure 2.4* is an example stakeholder map for a CISO at a technology company. The placement of each stakeholder reflects both their influence on security outcomes and the frequency with which the security leader should engage them. As business priorities evolve, stakeholders may move between tiers over time.

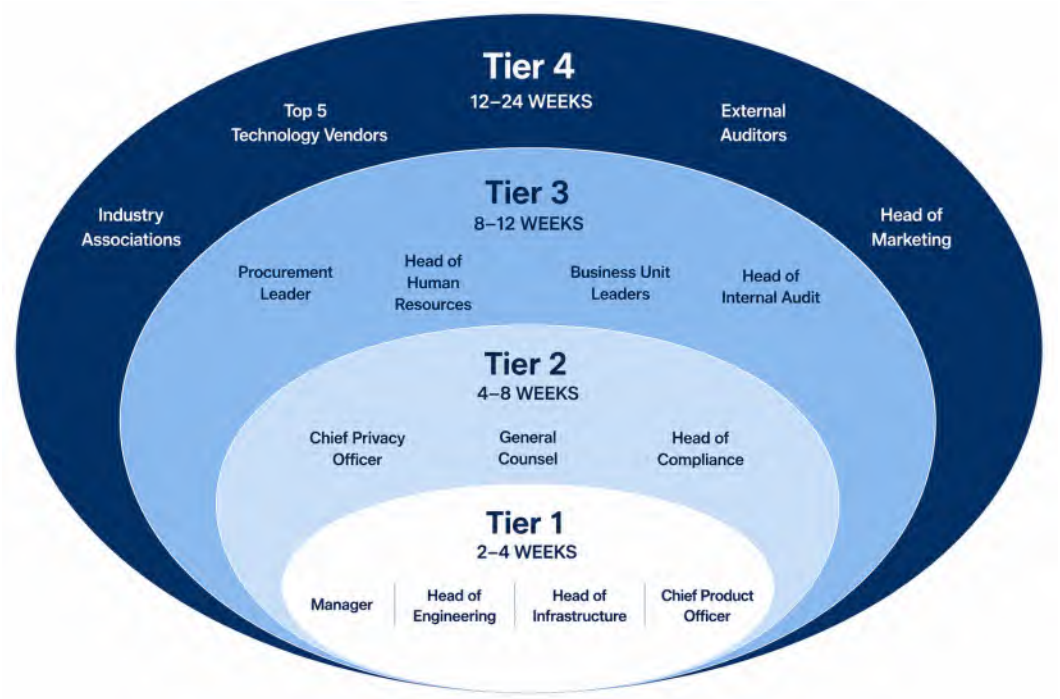


Figure 2.4 – Example stakeholder map for a CISO at a technology company

Notice that stakeholder placement is not determined solely by title. In one organization, the Head of Engineering may be a Tier 1 stakeholder because they influence most security-related decisions. In another organization, that same individual may be Tier 2 because responsibilities

are distributed differently. Focus less on organizational hierarchy and more on influence, decision-making authority, and the organization's current priorities.

Tip

Keep in mind that relationship-building is a long game. If a high-priority stakeholder is not responsive, begin by learning what matters most to them and how your work aligns with their objectives, and look for opportunities to provide value indirectly.

Making time to connect

When you look at your stakeholder map for the first time, it may feel overwhelming. How can you possibly find time to connect with so many people while also managing direct reports and daily responsibilities? The key is to be intentional about how you engage, based on the tier each stakeholder falls into.

Use your relationship map to plan a balanced mix of scheduled one-on-ones, ad hoc touchpoints, and lightweight communications such as emails or texts. Each serves a different purpose and should align with the stakeholder's level of influence. *Table 2.5* provides examples of how different communication methods can be used across stakeholder tiers to maintain relationships without overwhelming your calendar.

Method	Rationale
Scheduled one-on-ones	When most people think about relationship building, they imagine formal 1:1 meetings. This approach should work with Tiers 1 and 2 of your relationship map, along with a select few from Tiers 3 or 4 who have major impact on your priorities. Use the sessions to deepen trust, align on goals, and proactively address issues.
Ad hoc calls	Don't underestimate the power of a spontaneous call. A quick five-minute check-in, perhaps while you are traveling to the office or between meetings, can go a long way in maintaining connection and showing interest. Some of these informal moments often strengthen relationships more than a formal calendar slot.

Method	Rationale
Emails or texts	A short note to share an article, congratulate a win, or comment on a project update is a simple yet effective way to stay visible. It shows you are paying attention and that the relationship matters even when there is no immediate agenda.

Table 2.5 – Sample communication methods

It is easy to fall into the trap of overcommitting yourself to 1:1 meetings. Avoid filling your calendar only to cancel or reschedule later. Reliability builds trust; it is far better to have fewer meetings you consistently honor than to repeatedly move them around. Consistency, more than frequency, is what strengthens credibility and connection. Over time, these consistent interactions help strengthen trust and create relationships that extend beyond operational discussions or moments of crisis. While these principles apply across all stakeholder groups, engaging with senior executives and board members requires an even more intentional approach to communication.

Engaging with C-suite and the board

You already know that building strong relationships with senior executives requires more than technical expertise. They expect something different of you: strategic communication and a deep understanding of the organization's priorities, combined with the ability to translate complex risks into clear business terms.

Not all stakeholders require the same type of relationship. Executive leaders and board members are responsible for shaping organizational strategy, risk appetite, and investment priorities. As a result, they often require a different level of context than operational teams and expect security discussions to focus on business impact rather than technical detail.

Most members of the company's C-suite and board audience do not come from a technical background. They likely do not share the same technical depth or vocabulary as the security organization and may be unfamiliar with many of the acronyms, frameworks, or technologies being discussed. In many cases, they are also less likely to interrupt the conversation to ask clarifying questions.

I learned this lesson personally during a presentation about the bug bounty program. I assumed most of the executives in the room understood what a bug bounty program was and moved directly into metrics, trends, and operational details without explaining the fundamentals. The meeting itself appeared successful; no one challenged the presentation or asked many questions.

Later, my manager shared that several executives had actually left the session confused. They did not fully understand the terminology, the business relevance, or the intended outcome of the discussion. The presentation was delivered, but the message did not land.

That experience fundamentally changed how I approached executive communication. From that point forward, I focused less on demonstrating technical depth and more on ensuring the audience clearly understood the business implications, the decisions required, and the expected outcomes.

Healthy executive communication should feel like a dialog, not a one-sided presentation. Questions, discussion, and even disagreement are often positive signals that the audience is engaged, processing the information, and connecting it to business priorities. Silence, on the other hand, does not always mean alignment or understanding. In many cases, it may indicate confusion, disengagement, or uncertainty about how to participate in the discussion. The following practices can help distinguish you as an effective executive communicator:

- **Having a predictable template that rarely changes**: By keeping the format consistent, you can focus the conversation on the content. If the template changes drastically every time, you will spend a lot of time on education in every conversation instead of focusing on the message and what matters most.
- **Solution-oriented content**: Focus on how you are going to solve the problem and what support you need to be successful. Do not admire the problem, as it will not resonate with them and will take away from your credibility as a leader.
- **Data-driven content that tells a story**: Instead of the typical "doom and gloom" approach, use numbers and facts to support your story.

Similar to the *Circles of Influence* framework we introduced in the previous section, the 10-minute security update framework can help you be better prepared for executive communications.

10-minute security update framework

In many cases, C-suite members and the board share similar concerns regarding the cybersecurity program. Your goal is to proactively be able to answer questions that are top of mind for them without being asked, in under 10 minutes.

At all times, you should be prepared to discuss the current state of the program in a clear and accessible way. This requires more than technical knowledge. It requires understanding your audience, anticipating their concerns, and adjusting the conversation based on the context of the interaction. Over time, with preparation and repetition, these conversations become more natural and impactful.

Last, you are likely not going to be able to fully answer all the questions within 10 minutes. Answer the ones that are most relevant in the context of the conversation. You can always offer to set up a follow-up to continue the dialog.

Table 2.6 provides sample questions you can use to guide a focused and meaningful 10-minute security update conversation. You can adjust these questions based on your role and sector. Over time, these questions become less of a script and more of a mental framework you can quickly adapt to different audiences and situations.

Question	**Rationale**
What are our most significant cybersecurity risks and how are we managing them?	Provide clarity on risk exposure, prioritization, and how controls map to business impact.
How prepared are we to respond to and recover from a major cyber incident?	Offer insight into crisis management, communications, and recovery plans.
Are we compliant with current and emerging cybersecurity regulations?	Inspire confidence that regulatory expectations are being met.
Are we investing the right amount and in the right areas to manage cyber risk effectively? How are we executing against the 3–5-year roadmap? How are we doing compared to our peers?	Show how cybersecurity spend aligns with risk appetite and delivers measurable outcomes.
How does cybersecurity enable our business strategy?	Demonstrate how security supports innovation, digital transformation, and customer trust. Present recent wins.

Table 2.6 – Guiding questions for a 10-minute security update

For example, imagine you run into the CTO shortly after a series of high-profile cyberattacks targeting your industry. That conversation is likely best focused on immediate operational readiness: How prepared are we? Are we seeing similar activity? What actions are we taking to reduce risk over the next several days? In contrast, a conversation with the Chief Compliance

Officer may center more around regulatory exposure, audit readiness, and how the security program is evolving to address emerging compliance requirements.

The goal is not to cover every topic in every interaction, but to make each conversation relevant and valuable to the stakeholder sitting across from you. If time permits, you can always expand into additional areas or schedule a follow-up discussion to continue the dialog.

Building long-term trust

Trust is not earned in a single meeting; it is built through a series of consistent, meaningful interactions. By combining the approaches discussed earlier, such as maintaining regular touchpoints and using the 10-minute security updates, you create ongoing opportunities to reinforce credibility and transparency.

A critical component of maintaining trust is open and honest dialog. It can be tempting to show a dashboard filled with green KPIs because they create a sense of reassurance. But executive trust is not built through perfect-looking metrics; it is built through transparency and consistency over time.

Strong security leaders do not hide challenges, but they also do not create unnecessary panic. The goal is to communicate risk with clarity, explain business impact in practical terms, and demonstrate that the organization has a thoughtful plan to improve over time.

Real trust comes from courageous conversations. When you are willing to share both strengths and weaknesses, successes and failures, and the lessons learned along the way, you demonstrate commitment to progress. This transparency elevates you from a compliance enforcer to a strategic business partner, one who understands that trust is earned through the grind, not perfection.

Notes from the field with Renana

Case study: collaboration with stakeholders

My philosophy today regarding how I approach leadership, communication, and influence is grounded in two formative experiences from my time at EY and my time at PayPal.

During the first year after joining PayPal as Deputy CISO, I was struck by how effortlessly my manager seemed to connect with everyone across the company. People genuinely liked him, and, more importantly, they listened to him. He influenced major decisions without ever appearing rushed or overextended. He also seemed to have time for everyone: regular meetings with key internal partners, quick hallway conversations, and even ongoing dialog with external peers and vendors. I, on the other hand, felt like I was constantly behind. My calendar was overflowing with internal meetings, mostly focused on my immediate team. I was frequently canceling one-on-ones and struggling to find time to connect beyond my direct

reports. Eventually, I asked him how he managed it all, and he introduced me to the *Circles of Influence* model. I had always believed in structure and cadence, but I hadn't realized how intentional time allocation could transform the way I operated as a leader.

During my last two years with EY, I worked closely with a partner at EY's financial services group who was a master communicator. His emails were always precise and polished (long before AI could help with that), he knew what topics would resonate the most with executives, and he knew how to maintain relationships with them even when they were no longer his client. I got to experience it firsthand, and it made a long-lasting impression on me. Even after we stopped working together, he always stayed in touch and reached out every quarter, sending a thoughtful message, sharing an article, or checking on how I was doing. It seemed effortless, and despite the geographical distance between us, we have stayed in touch up to this day.

These two experiences reshaped how I lead. I learned that influence is not about hierarchy but rather consistency, clarity, and genuine connection. By adopting the *Circles of Influence* model and the *10-minute security update framework*, I was able to take my leadership to the next level. Ultimately, this reinforced one of the core lessons from this chapter: relationships are not a side element of leadership; they are the multiplier of technical capability.

Summary

In this chapter, we focused on the power of relationships at every level of the organization. From assessing and mentoring your immediate team to partnering with IT leaders and aligning on shared goals, we explored how to create lasting connections with both internal and external stakeholders. We also examined how to build credibility and trust with the C-suite and board through thoughtful communication and consistent engagement. The frameworks and examples in this chapter are designed to help you accelerate that trust-building process and turn relationships into a force that amplifies your impact.

In *Chapter 3*, we will build on this foundation, moving from relationships into strategy. You will learn how to combine the insights gathered during your onboarding and stakeholder engagement to shape a compelling security plan.

Chapter checklist

- Complete the *Team Assessment Tool*. Evaluate each employee's role alignment, development needs, and access to mentorship or sponsorship.
- Create a *Security Scorecard*. Use shared measures to make performance and ownership visible across technology teams.

- Map your *Circles of Influence*. Assign stakeholders to tiers and establish a communication cadence for each.
- Prepare answers to the 10-minute security update. Practice answering the questions most likely to matter to C-suite and board members in clear business terms.

Additional resources

- Team Assessment Tool template: `https://bit.ly/CISOBook4`
- Circles of Influence template: `https://bit.ly/CISOBook5`

3

Crafting Your Vision: Developing the Security Plan

So far, you have covered two important milestones on your onboarding journey. First, you have developed a deep understanding of the organization through your listening tour and initial assessment. Second, you established relationships, built trust, and gained credibility with the stakeholders who will influence the success of your program. Together, these efforts provide the foundation for the next phase.

When you are roughly 90 to 120 days into your tenure, it is time to shift gears from assessment to building a plan. The final phase of your onboarding is to translate what you have learned so far into a clear, forward-looking plan that aligns security with the company's broader business objectives.

The three building blocks of a comprehensive security plan include your **vision**, **strategy**, and **initiatives**. Each plays a distinct role; your vision defines the "why" or the purpose, the future state you are striving to achieve. Your strategy outlines the "what" or focus areas—the long-term pillars that will get you there. Your initiatives represent the "how" or the path, the specific, actionable steps that turn the strategy into measurable progress. In this chapter, we will explore the following topics:

- Moving from assessment to planning
- Defining the security philosophy
- Setting your vision, strategy, and initiatives
- Presenting and cascading the security plan
- Maintaining strategic agility

Creating these components will require you to balance ambition with realism. While you may be eager to establish an end-to-end vision and ambitious goals, your understanding of the business, its culture, and the factors that shaped the current security program are still evolving. Priorities that appear critical during your first few weeks may later prove less urgent as you gain deeper insight into organizational risks, business objectives, dependencies, and constraints.

By the end of this chapter, you will have a structured approach to define your direction, establish strategic pillars, and identify the initiatives that will inspire others to join you on the journey. The process begins by transitioning from assessment to action, using the insights gathered during your first weeks to develop a plan that aligns security with the organization's broader goals and priorities.

Moving from assessment to planning

The listening tour and initial assessment in earlier chapters provided valuable insight into the organization, its risks, and its priorities. Taking the leap from understanding the current environment to envisioning the future of the program requires a shift in mindset.

Recognizing the shift from tactical to strategic thinking

Whether this is your first executive role or your third, it is important to recognize that expectations have changed. The skills and habits that made you successful in the past are still valuable, but they are no longer enough.

In Marshall Goldsmith's words, "*What got you here won't get you there.*" For example, managers are often rewarded for solving problems, while executives are expected to decide which problems matter most, align resources accordingly, and build support for those decisions across the organization.

Executive leadership also carries unwritten expectations that are rarely explained. Before becoming an executive, identifying a problem and escalating it may have been enough; someone else was responsible for deciding what to do next. As an executive, you cannot stop at the problem. You are expected to recommend a solution and own the trade-off, even when the information is incomplete. You will not get every judgment right, especially during your first few months. Those experiences often become some of your most valuable leadership lessons.

Table 3.1 highlights how focus and expectations shift from mid-level management to executive security leadership:

	Mid-level Management	**Executive Leadership (CISO or direct report)**
Time Horizon	Focused on short-term goals (next quarter to a year)	Plans for long-term outcomes (3–5 years)
Perspective	Operational and tactical: "How do we get this done?"	Strategic and holistic: "Where are we going, and why does it matter?"
Decision-making	Execute decisions, provide input on priorities	Define direction, set priorities
Success Metric	Project delivery	Reduces risk
Leadership Focus	Development of immediate staff	Drives organizational culture

Table 3.1 – Shifting from tactical execution to strategic leadership

The next challenge is applying this executive perspective to the development of your plan.

Avoiding common pitfalls in defining the plan

The pressure to demonstrate value quickly can lead new leaders to make choices that weaken the plan's focus or sustainability. Keep the following common pitfalls in mind as you begin developing your plan:

- **Define what "good enough" means for your organization:** Maturity levels vary based on risk tolerance, industry, and available resources. Consider using a 1 to 5 maturity scale, such as those commonly derived from **National Institute of Standards and Technology (NIST)**-based frameworks, to determine what is acceptable for your environment. In many cases, a level 3 may be enough. Pursuing higher levels without a clear business need can become an expensive investment that is difficult to justify and may divert resources from other areas of the security program (we will discuss maturity models in more detail in *Chapter 11*).

- **Leverage benchmarking to shape your perspective**: Insights from peers, industry reports, and consultants can help you identify emerging trends, avoid blind spots, and align your vision with your sector's expectations. If the risk is at an acceptable level now, you may choose to invest more in other areas.
- **Ensure all security domains are represented**: When leading new or unfamiliar areas, resist the tendency to focus only on what you know best. Spend more time learning about the functions you have not led before to create a balanced and comprehensive strategy.
- **Establish a cadence for reviewing the plan**: While the vision is mostly static, the strategy and especially the initiatives will evolve as the organization and threat landscape change. Define who will be involved in periodic reviews and how feedback will inform future iterations.

A successful plan needs a clear set of principles to guide decisions, especially when competing business objectives, resource constraints, and emerging risks create difficult trade-offs. Those principles form your security philosophy, the foundation upon which the rest of the plan is built.

Defining security philosophy

Your philosophy is the lens through which you view and approach your job. It reflects your beliefs about the purpose of security, how it should operate, and what success looks like. It is shaped by your experiences, mentors, and the environments you have worked in.

This is a rare opportunity to pause and reflect on how your personal security philosophy influences the plan you are shaping. By articulating your philosophy to yourself, you both clarify your own thinking and make it easier for others to understand your decisions.

Establishing guiding principles for security decision-making

There's no single right answer when it comes to which components should be part of your security philosophy. Most leaders find that their approach is a blend of multiple philosophies, each reflecting different aspects of their experience. Your security philosophy will serve as your anchor for decision-making. As an executive, you will routinely face situations where there is no perfect answer, only competing priorities, limited resources, and differing stakeholder perspectives. A clearly defined philosophy provides a consistent framework for making and explaining those decisions.

The following table presents some of the most common principles:

Philosophy	Description
Assume Breach	Operate under the assumption that your network has already been accessed by an unauthorized entity. Focus on limiting impact through detection, response, and resilience.
Defense in Depth	Build multiple layers of security controls. Each layer provides backup protection in case another fails, in an attempt to limit impact so no single point of compromise can lead to a critical incident.
Zero Trust	Every access request, internal or external, needs to be verified, continuously monitored, and contextualized. The goal is to move toward identity and data-centric security.
Secure by Design	Integrate security from the start, embedding it into technology, processes, and culture rather than treating it as an afterthought. This approach emphasizes thoughtful architecture and collaboration with engineering and product teams.
Proactive Security	Reduce threats before they materialize, emphasizing threat intelligence, purple teaming, bug bounties, and continuous improvement to stay ahead of adversaries.
Human First	Recognize that people are at the heart of security. This philosophy focuses on empowerment and education rather than finger pointing.
Exposure Reduction over Alert Reaction	Focus on reducing the organization's attack surface, prioritizing risk based on exploitability, business impact, and attacker behavior, and aligning with **Continuous Threat Exposure Management (CTEM)**.

Table 3.2 – Common security philosophy principles

Tip

Your security philosophy should guide more than strategy documents; it should influence how you communicate, prioritize, and make decisions. As an example, revisit the responses you developed for the *10-minute security update framework* in *Chapter 2*. Review whether the messages reflect the principles and priorities defined in your security philosophy. If not, consider how you would adjust them to better align with the vision you want stakeholders to understand and support.

One area where these principles become particularly important is navigating competing business priorities.

Balancing risk tolerance, innovation, and compliance pressures

Defining your guiding principles is the first step. Living them requires navigating the constant tension between risk, innovation, and compliance. Every organization's balance point is different, shaped by its industry, regulatory obligations, growth ambitions, and culture. As a security leader, your role is to help the company take calculated risks, creating confidence for the business to innovate.

Your philosophy also serves as a consistent basis for making and communicating prioritization decisions. It helps other stakeholders understand the reasoning behind your decisions, especially when trade-offs are required. For example, a leader leaning more on *Secure by Design* may prioritize engineering partnerships and architecture reviews, while someone emphasizing *Assume Breach* may focus more on detection and response.

When you articulate choices through the lens of your philosophy, this builds transparency and trust, allowing stakeholders to see how decisions connect back to an intentional, principles-driven vision.

By this point, you should have a clear understanding of the principles that will guide your decisions and the trade-offs. These principles establish a foundation for defining the future state and the path required to achieve it.

Aligning security with business objectives

Security strategies are most effective when they support the organization's broader objectives. Before defining your vision, take time to understand where the business is headed and what it is trying to achieve over the coming years. Growth initiatives, digital transformation efforts, expansion into new markets, acquisitions, regulatory requirements, and customer expectations can all influence the priorities of the security program.

One of the most common mistakes security leaders make is building a strategy around security problems rather than business goals. Security executives are rarely funded to solve security problems alone. They receive support when they demonstrate how security enables growth, resilience, customer trust, regulatory compliance, and operational efficiency.

Table 3.3 provides examples of how business objectives can influence security priorities. We will return to this concept later in the chapter when exploring ways to visualize the relationship between business objectives, strategic priorities, and security initiatives.

Business Objective	**Security Outcome**
Expand into new markets	Strengthen regulatory compliance and data protection capabilities
Accelerate product delivery	Embed security into development processes and automate testing
Increase customer adoption and trust	Enhance identity security, fraud prevention, and data protection
Improve operational resilience	Strengthen incident response, disaster recovery, and business continuity capabilities

Table 3.3 – Examples of aligning security priorities with business objectives

Understanding these relationships helps ensure the security program is built around business outcomes rather than technical activities alone. With this context in mind, you can begin defining a vision that reflects both the organization's ambitions and the role security will play in enabling them.

Setting your security vision, strategy, and initiatives

Before defining the path forward, it is important to establish the destination. In this section, we will guide you through the process of defining the security vision and translating it into strategy and initiatives that drive meaningful outcomes. The approach outlined here follows a *top-down model*: starting with the organization's broader business vision, translating it into the security vision, cascading it into strategic pillars, and documenting specific initiatives. This approach ensures security is a natural extension of the company's purpose and goals. When your plan is aligned with the organization's business objectives, it becomes a catalyst, positioning security as a business enabler.

In some organizations, leaders may prefer a *bottom-up model*, beginning with tactical initiatives and evolving upward to define strategy and vision. This approach is often used when the organization is responding to an urgent challenge, such as a recent security incident or a major regulatory audit finding. In these situations, immediate actions may be necessary to reduce risk and stabilize the environment.

Regardless of the model you choose, *Figure 3.1* illustrates the relationship between vision, strategy, and initiatives.



Figure 3.1 – Relationship between vision, strategy, and initiatives

While both approaches can work, in most cases we have seen leaders use the top-down approach. A clearly defined vision and strategy help align stakeholders, guide prioritization, and provide context for investment decisions, making it easier to ensure that tactical initiatives support broader organizational goals.

Tip

Before developing your security vision, revisit your notes from the listening tour and initial assessment. Pay close attention to the company's mission, vision, strategic priorities, and core values. This will ensure the security vision is fully aligned with the broader business direction.

Reflecting on the vision

As discussed earlier, the ideal vision answers the question "why." It defines where we want to go and what success looks like in the coming years. In many organizations, a vision serves as the north star for the next three to five years, providing long-term direction while allowing the strategy and initiatives to evolve as business needs change. At its core, a vision statement describes the desired future state, establishes the tone for the security program, and connects people to a common purpose.

To develop the vision, start by answering questions regarding the *future* state of the program. The goal is to paint a clear picture of where you are headed, one that aligns with business objectives and reflects your guiding principles:

- Where is the business likely to be three to five years from now?
- What would a mature cybersecurity plan look like for this organization?
- How would security enable the company's business and competitive advantage?
- What risks would be acceptable, and what risks would be non-negotiable?
- How would customers and regulators describe the company's approach to security?
- What principles should guide security decisions when trade-offs arise?

Tip

While it may be tempting to answer these questions on your own, we strongly recommend engaging with your stakeholders as part of the exercise to gather diverse perspectives.

Creating the vision statement

Once you have answered the foundational questions and gathered stakeholder input, it's time to turn your insights into a clear, concise vision statement.

Think of the vision statement as a short, memorable description of where you want to go and why it matters. Here are a few things to keep in mind while drafting a vision statement:

- **Keep it short and clear**: Aim for 1–3 sentences. The statement should be easy to remember and communicate, even to non-security stakeholders. If it takes more than a paragraph or two to explain, it's too complex!
- **Focus on the future and the impact**: Your vision should describe the desired future state, not the current reality. Highlight the outcomes you want to achieve, such as what the organization will look like, how it will behave, and how security enables business success.
- **Reflect your guiding principles**: The vision statement should include elements from the security philosophies mentioned earlier in this chapter.

Once drafted, test the vision statement with a small group of stakeholders by asking them if it is easy to understand. Iterate until it resonates widely. A vision statement should be aspirational enough to inspire action while remaining grounded in the realities of the organization. If stakeholders cannot see how the vision connects to the company's future, it will be difficult to build momentum around it.

Translating vision into long-term strategic pillars

Once your vision statement is in place, it is time to answer the "what" question. Now you will translate that aspiration into a set of strategic pillars, serving as the foundations of your security strategy. Start by reading your vision and identifying the key themes or ideas that emerge. These often reveal what truly matters, such as resilience, trust, enablement, or agility. For example, if your vision says, "*To build a resilient, human-centered security culture that enables innovation and trust,*" you can extract several key themes, such as resilience, enablement, and trust.

From these themes, define three to five strategic pillars, each representing a major focus area. Each pillar should be big enough to inspire long-term effort but specific enough to drive measurable outcomes. Some of the most common pillars may include Risk (*Building confidence through proactive risk management*), Secure by Design (*Embedding security into every stage of digital transformation*), Human-Centered Security Culture (*Empowering people as a driver of security*), Data Protection (*Safeguarding data to sustain trust*), and Governance and Operational Excellence (*Delivering a 24/7 resilient platform*).

Finally, map each pillar back to your guiding principles and the business outcomes it supports. This step ensures your strategy is not developed in isolation but directly reflects how security enables organizational success. For example, a *Secure by Design* philosophy might align with a pillar focused on digital innovation, while a *Human First* approach might underpin a pillar focused on awareness and culture. Each pillar should tie clearly to one or more business objectives, expressed in terms that resonate with executives, such as accelerating time-to-market, strengthening compliance posture, or increasing customer trust.

Documenting the initiatives

Each strategic pillar is typically composed of several supporting initiatives. These are the actual steps that transform your strategy from concept to execution and represent shorter-term, measurable goals.

Review your strategic pillars and work with your team to outline the concrete steps that will bring them to life. For example, a SaaS company may establish a strategic pillar focused on protecting customer identities and reducing account takeover risk.

Write a one-sentence summary of each initiative. Think of it as a headline others can easily understand (what you are doing and why it matters), for example, "*Upgrade customer authentication to phishing-resistant MFA to reduce account takeover risk.*" Add a clear *definition of done* to create a shared understanding of the condition under which the initiative can be considered complete. Here is an example: "*Phishing-resistant MFA is available to all customers, integrated across all supported authentication flows, and enabled by default for new accounts.*"

Assign one or more metrics to measure progress for each initiative. Without metrics, it becomes difficult to determine whether an initiative is succeeding, where adjustments are needed, or how the work contributes to broader business objectives. See the next section on how to select them. Here are some examples:

- Percentage of active customers enrolled in phishing-resistant MFA
- Percentage of customer accounts protected by phishing-resistant MFA
- Percentage of successful account takeover incidents

Selecting meaningful metrics to track progress

Once your initiatives are defined, the final step is determining how you will measure progress and demonstrate impact. At the initiative level, this is typically done through **key performance indicators (KPIs),** while the overall risk posture is best tracked through **key risk indicators (KRIs)**. Together, these two types of metrics provide a balanced view of execution and residual risk.

Note

In *Chapters 6–8,* we will discuss specific metrics for different aspects of your program. For now, you should select a limited number of KPIs and KRIs that will help the next level of leadership above you understand how your area is performing.

When defining metrics, avoid generic definitions such as *all critical systems*. The more specific and measurable your metric, the more achievable it becomes. Revisit each KPI and KRI with your teams until everyone shares the same understanding of the scope, the data source, and the exact definition of done. This alignment is essential for driving meaningful progress.

Key performance indicators

KPIs measure how effectively your team is delivering against planned work. They assess the progress, quality, and efficiency of your initiatives. KPIs work best when tracking execution and operational improvement. Sample KPIs may include:

- Total number of incidents, broken down by incident type and/or severity
- **Mean time to detect (MTTD)**
- Total number of vulnerabilities, broken down by severity
- Percentage of user awareness training completion
- Phishing simulation click/report rate

Use KPIs when you want to monitor execution and operational progress. These are your indicators of whether initiatives are moving as planned.

Key risk indicators

KRIs measure risk exposure. They highlight conditions that may increase the organization's vulnerability or signal the potential for future incidents. KRIs work best when monitoring risk posture, emerging threats, or systemic weaknesses. Sample KRIs may include:

- Number of privileged accounts
- External-facing systems with vulnerabilities
- Percentage of assets with unknown owners

Use KRIs when you want to understand residual risk (what could still go wrong even if plans are being executed). These metrics help inform leadership about risk tolerance and prioritization.

A cybersecurity program becomes meaningful when people can see their role in achieving it. Communicating the vision, strategy, initiatives, and supporting metrics helps create alignment and build commitment for the road ahead.

Presenting and cascading the security plan

Even a thoughtful security plan can be lost in translation. Executives, board members, and cross-functional partners have limited time and varying familiarity with cybersecurity, so how you present the plan matters as much as the work behind it.

Choosing the visual format

A clear, well-designed visual can bridge the gap between what seems clear to you and what stakeholders understand, helping them grasp direction, priorities, and intended outcomes. In this section, we will examine three ways to visualize the plan: the **Cascade Pyramid**, the **Security Plan Flowchart**, and the **Alignment Matrix**. Each format serves a different purpose and level of detail. *Table 3.4* summarizes the difference between the three formats:

Format	Best Used For	What it Shows
Cascade Pyramid	Providing a simplified view of the security plan	The security vision, strategic pillars, and a high-level selection of supporting initiatives
Security Plan Flowchart	Showing the complete structure of the security plan	The security vision, strategic pillars, and all supporting initiatives organized under each pillar
Alignment Matrix	Demonstrating how security supports broader business priorities	The connection between business objectives, security pillars, and supporting initiatives

Table 3.4 – Comparing security plan visual formats

There is no right or wrong way to present your work. You may want to experiment with the three formats and see which one best resonates with your audience. In certain instances, you may also want to use more than one visual.

Note

Match the level of detail to your audience. For executive conversations, the **Cascade Pyramid** may provide enough context by presenting the vision, pillars, and a simplified view of the initiatives.

When stakeholders need to understand the full structure of the plan, the **Security Plan Flowchart** provides visibility into all supporting initiatives.

When the conversation is focused on business alignment, the **Alignment Matrix** makes the connection between security pillars and business objectives explicit.

In *Chapter 4*, you will take those initiatives one step further by translating them into a prioritized and sequenced roadmap.

The Cascade Pyramid

One of the most effective ways to illustrate how your security strategy supports the broader enterprise mission is through the **Cascade Pyramid**. This visual helps connect high-level business objectives to security activities, making the strategy tangible and relatable across the organization.

Figure 3.2 presents a sample Cascade Pyramid diagram:



Figure 3.2 – Cascade Pyramid

Place the Security Vision at the top, grounded in the organization's broader priorities. Beneath it, show the strategic pillars that translate the vision into focus areas. At the base, include a *small* number of representative initiatives under each pillar.

This structure creates a clear line from the security vision to the strategic pillars and supporting initiatives. It helps employees see how their work contributes to the organization's direction. The Cascade Pyramid works best when presenting the plan to a broad audience, such as during a town hall or executive briefing, where the goal is to communicate the hierarchy quickly rather than to show every detail.

The Security Plan Flowchart

This flowchart offers a detailed, structured view of your security plan. Like the Cascade Pyramid, it includes the security vision and strategic pillars. It also shows the full set of supporting initiatives under each pillar. Unlike the Cascade Pyramid, which emphasizes hierarchy, the flowchart provides more room to show the breadth of plans.

Begin with the Security Vision at the top, connect it to each strategic pillar, and then show the initiatives supporting each pillar. The number of initiatives does not need to be the same across every pillar; the visual should reflect the actual work required. Detailed sequencing, ownership, and timing will be addressed through the roadmap in *Chapter 4*.

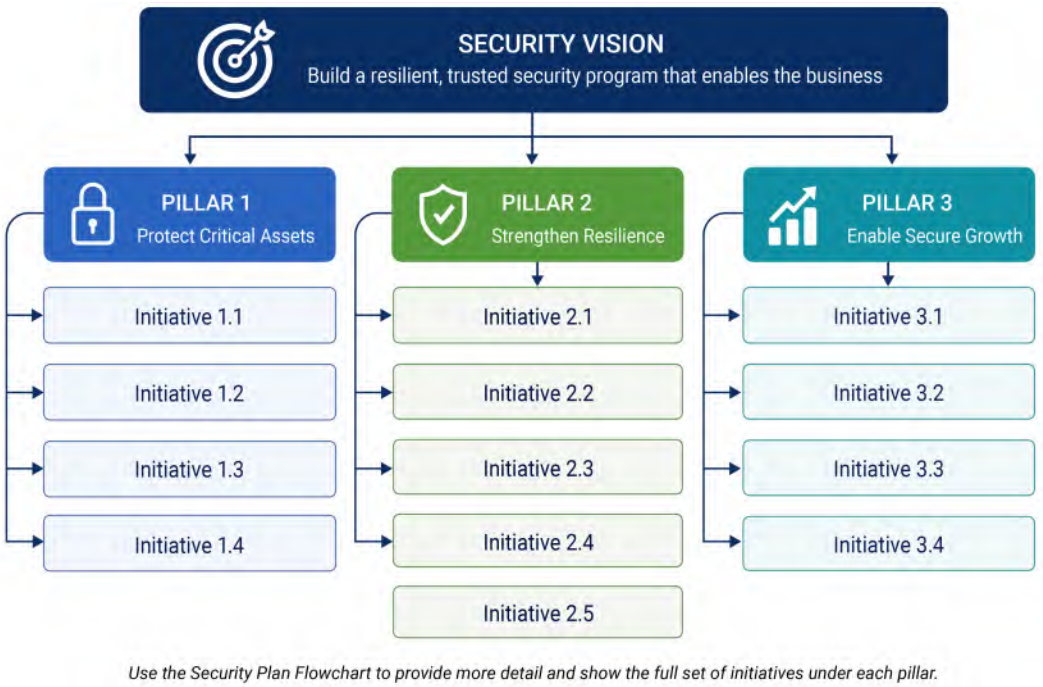


Figure 3.3 – The Security Plan Flowchart

The Alignment Matrix

While the Cascade Pyramid and Security Plan Flowchart begin with the Security Vision, the **Alignment Matrix** begins with the priorities of the business. Use it when stakeholders need to understand why particular security investments or initiatives matter to the organization.

Start with the organization's current objectives and map each one to the strategic pillars and initiatives that support it. For example, a business objective to expand digital services may connect to a pillar focused on secure product development and initiatives involving

application programming interface (API) security or secure design reviews. The matrix makes that connection explicit and can help build support for the work. *Figure 3.4* shows an example:

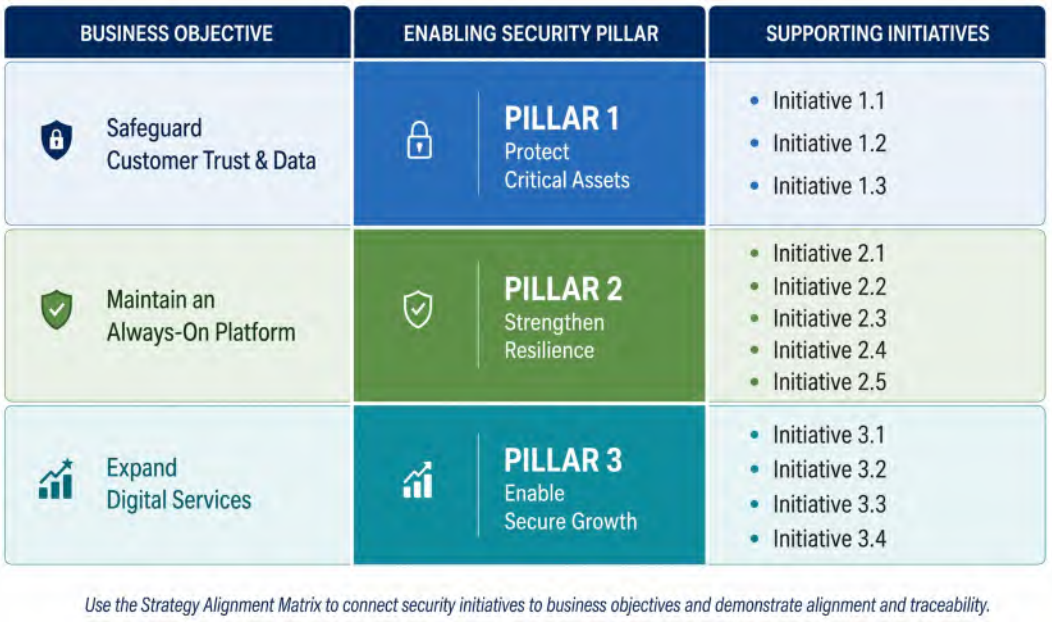


Figure 3.4 – Strategy alignment

This simple format provides direct traceability between what the business cares about and what the security team delivers.

> **Tip**
>
> If some business objectives don't map neatly to a single strategic pillar, that is completely normal. Not every connection will be a perfect match. Focus on creating the strongest logical alignment possible instead.

Once you have selected the visual that best represents your plan, incorporate it into a one-page overview for stakeholders.

Creating a one-page security plan overview

One of the most effective ways to present the work done so far is by summarizing the vision and strategy into a single one-page view. This document will become your business card, providing a clear, executive-ready snapshot that captures the essence of your plan. It can also serve as a leave-behind for stakeholders, as a simple reference point for the plan.

Your one-page security plan overview should include the following components:

- Security vision statement.
- Security strategy, listing your strategic pillars. Include one to two sentences describing each pillar, focusing on its purpose and the business outcome it enables.
- Visual representation, using one of the options listed in the previous section. We recommend removing the initiatives from the view as this page is about communicating direction, not execution.

A sample one-page security plan overview is included in the *Additional resources* section of this chapter and can be used as a starting point when creating your own version.

The one-pager serves as a concise representation of the work completed throughout this chapter. The next step is to actively communicate the plan and connect individual responsibilities to broader objectives.

Cascading the plan

The reality is that most people in the company will not understand your vision, strategy, and initiatives as well as you do. One of the primary responsibilities of executive leadership is creating alignment.

Over the years, we have seen many leaders assume that others can easily "connect the dots," only to discover later that key stakeholders, both within the security and non-security organizations, did not truly understand how the strategic pillars and initiatives fit together. This gap can lead to misalignment and confusion.

We recommend using the stakeholder map and communication cadences you established in *Chapter 2* to guide how you cascade the updated plan across the organization. Let's discuss how you can approach different stakeholders.

Security teams

While members of the security organization are interested in the vision and strategy, many will need clarity on how the strategy translates into their day-to-day work, what they are accountable for, why it matters, and how success will be measured. Use a consistent communication rhythm to build this understanding over time.

Once the plan is finalized, present it at your next town hall to walk the team through the overall direction and reinforce how each pillar connects to their work.

In subsequent town halls, go deeper by focusing on one strategic pillar at a time. Also, invite teams to showcase progress or demonstrate early wins through show-and-tell sessions. At the end of the year, revisit the full plan to celebrate accomplishments, highlight measurable gains,

and introduce updates for the upcoming cycle. Most changes will occur at the initiative level, so emphasize how these updates translate into tangible execution.

Tip

Help teams understand how the broader plan aligns with their work. We will dive further into this as part of *Chapter 4*.

Cross-functional partners

Your cross-functional partners, such as Engineering, IT, Product, Legal, Compliance, Audit, and Risk, play a critical role in bringing the security plan to life. They need to understand what it means for their teams, how collaboration will work, and where their support is essential.

Review the plan with each key partner to align on expected outcomes. Use the one-pager to anchor the conversation and keep the message consistent.

Tip

Strengthen alignment by presenting the plan in both 1:1 settings and broader forums such as town halls or team meetings. This helps employees hear the message directly from you rather than relying on secondhand communication.

Executives and the board

Executive audiences require a different level of detail—focused on outcomes, business alignment, and impact.

Depending on your role, bring the one-page security plan overview to each 1:1 and use it as a standing reference point. Revisit it one to two times per year to show progress and highlight meaningful updates.

Present the plan annually to the board, celebrating achievements, quantifying improvements, and sharing strategic adjustments. In this case, you are likely not going to bring the one-pager with you, just one of the visualizations.

Tip

Focus your conversations on highlighting outcomes and themes and their impacts, not activities. Your update should emphasize the big picture and skip the bits and bytes, unless specifically asked to.

Successfully cascading the plan helps create alignment and shared understanding across the organization. As the business evolves, maintaining that alignment requires periodic review and adjustment.

Maintaining strategic agility

It is easy to fall in love with your plan. After all, you invested time, thought, and team energy to bring it to life. But no matter how carefully designed, your plan is going to change. The business landscape will shift, new technologies will emerge, risks will evolve, and economic or regulatory pressures will change your priorities. What seemed critical six months ago may become irrelevant over time.

The most successful security executives are adaptable. Executive leadership is not about defending a plan that no longer reflects reality. It is about continuously evaluating new information, reassessing assumptions, and adjusting direction while maintaining confidence in the overall vision. Simply put, they treat the plan as a living document. Many security executives re-evaluate their next one-year roadmap quarterly.

It is only through executing the plan that you begin to discover which initiatives truly move the needle, which dependencies are harder than expected, and which opportunities you could not have predicted at the start. Sometimes, you realize that the destination you were aiming for is not quite where you need to go.

Leveraging emerging risks and technologies to stay ahead

A strong vision is anchored in what could be. Being visionary means looking beyond today's challenges and asking: "*What kind of security organization do we need to become to enable the business of tomorrow?*"

To stay ahead, ask yourself and your leadership team the following questions:

- What emerging risks could redefine our priorities?
- What technologies (AI, automation, data platforms, or integrated tooling) could fundamentally change how we operate?
- If we were building a world-class security program from scratch, what capabilities, skills, and operating models would we include?

The questions above are intended to encourage continuous thinking about the future of the security program. As new technologies emerge, risks evolve, and business priorities change, leaders benefit from establishing a consistent process for evaluating whether the strategy remains aligned with the organization's needs.

Building a review rhythm

The final step in maintaining the plan is to establish a structured review rhythm. Review the plan end-to-end annually and revisit it when a material change in the business, risk environment, technology landscape, or regulatory requirements may affect your direction. These reviews help keep the plan aligned with business priorities without waiting for a disruptive event to force change. During each review, focus on two layers:

- **Reaffirming or recalibrating your vision and strategic pillars**: Determine whether they still align with the company's direction, risk posture, and growth strategy. This step ensures you are still solving the right problems.
- **Assessing and refining the initiatives**: Review progress against your definition of done, evaluate KPIs and KRIs, and identify what to accelerate, defer, or retire. Use metrics to drive improvement, not just compliance.

Notes from the field with Renana

Case study: blank pages to shared vision

Back in 2020, each member of the security leadership team was asked to develop a three-year plan for their area. There was no template or structure, just a blank document and a deadline. Each leader created their own version, and unsurprisingly, they all looked very different. Some were too technical, others too high level. I did not know where to start, so I relied on my consulting background to come up with a solution. It was very similar to what we discussed in this chapter, including a vision, strategic pillars, and initiatives.

At times, building the plan felt like another daunting task. We were already busy with much going on, and some questioned whether it was truly necessary. It took weeks of intentional effort to put one together. The reality is that it forced my team and me to see beyond the day-to-day. Even more, it forced us to dream big about what is possible, even if we did not know exactly how we were going to get there. Once the vision and pillars were in place, it felt like the "why," "what," and "how" aligned. It brought clarity and alignment to the team, accelerating prioritization, which also translated into pride of ownership. And yes, we achieved nearly 80% of what we set out to do.

During the process, I made several mistakes. The first was over-planning the small details. We wrote long descriptions of initiatives (3–6 sentences each), including work that was three years away. The process became a writing exercise, and some team members really struggled with it. In retrospect, I would have kept the longer-term initiatives at a higher level and added detail as the work moved closer to execution.

The second lesson was that executive leadership requires comfort with ambiguity. While I wanted certainty and stability, the business continued to evolve. New priorities emerged, resources shifted, and assumptions changed. I learned that the role of a security executive is not to create a perfect plan; it is to provide direction while adapting to changing conditions. My team was frustrated with the change from time to time, and we all had to learn to be more agile in our planning and come to terms with the changes.

The third lesson emerged when the CISO consolidated the work into an enterprise-wide security vision. While the plans aligned internally across security, they didn't clearly connect to business objectives. That made it harder to secure buy-in from product, tech, and executives, as we didn't articulate security's value in their language. It took deliberate effort over several weeks to get everyone on the same page.

The fourth lesson was that communication requires far more repetition and validation than I initially expected. At one point, we introduced the concept of "self-healing" as part of the team's vision. To me, it represented a broader goal of automated remediation of vulnerabilities. Some teams interpreted it as automatically remediating code vulnerabilities; others associated it with infrastructure, and several members of the IT organization viewed it as a blue-green deployment capability. I only discovered these differences after multiple conversations. What seemed clear in my mind had been interpreted in several different ways across the organization. The experience taught me that leaders should continuously reinforce key messages, validate understanding, and create opportunities for discussion. There will be moments when you feel like you are repeating yourself. In such instances, remember that repetition is often part of building alignment, not evidence that the communication has failed.

These lessons changed my view on putting together a cybersecurity plan. It's about creating direction, establishing clarity, and being adaptable. Ultimately, I realized that the plan is not about having all the answers or getting to the destination. It's about intentionally choosing the path, appreciating the journey, and recognizing that the real progress happens along the way.

Summary

In this chapter, we shifted from assessment and relationships to strategic direction. We began by defining a vision that aligns with business objectives, then translated this vision into strategic pillars, and finally into specific initiatives. We also explored how to bring the plan to life using visual frameworks and the one-page security plan overview, making it easier to communicate with stakeholders at every level. Finally, we discussed how to keep the plan adaptive and relevant by establishing review rhythms and leveraging emerging trends.

In the next chapter, we will turn this strategy into a roadmap as the focus shifts to prioritizing investments, evaluating trade-offs, and sequencing initiatives for execution.

Chapter checklist

- Define your security philosophy. Document the principles that will guide decisions and trade-offs across the security program.
- Create a security vision. Align it with the organization's business objectives and describe the direction of the security program.
- Translate the vision into strategic pillars and supporting initiatives. Identify meaningful measures that will show progress and changes in risk.
- Create the one-page security plan overview. Select the visual format and use the overview to communicate the plan to key stakeholders.
- Establish a review rhythm. Revisit the plan annually and whenever material changes in the business, risk environment, technology landscape, or regulatory requirements may affect its direction.

Additional resources

- The Cascade Pyramid: `https://bit.ly/CISOBook6`
- The Security Plan Flowchart: `https://bit.ly/CISOBook7`
- The Alignment Matrix: `https://bit.ly/CISOBook8`
- One-page security plan overview: `https://bit.ly/CISOBook9`

4

Charting the Course: Designing the Security Roadmap

At this point, you are approaching the end of the informal 90-day grace period many executives receive when joining a new organization. You have used that time to listen, build relationships, and define the Security Vision, strategic pillars, and supporting initiatives. As the grace period ends, you need to turn that direction into an achievable sequence grounded in the organization's risk appetite and capacity.

This is where executive judgment becomes visible. New demands will continue to emerge while resources remain limited. A major incident can disrupt your sequencing overnight; a regulatory deadline or shifting business priority can do the same. Throughout your first year, you will repeatedly face a difficult question: "*Given our risk posture and business priorities, what should we do first*?"

A well-designed roadmap defines priorities, sequences work, identifies dependencies, and sets expectations for timelines, milestones, and outcomes.

Creating the roadmap requires balancing ambition with practicality: what must happen now, what can happen next, and what could be deferred without compromising security, resiliency, or regulatory requirements.

In this chapter, we will discuss the following topics:

- Establishing priorities for security initiatives
- Optimizing the security technology stack
- Managing technical debt and legacy risk
- Planning for phased implementation

By the end of this chapter, you will have a repeatable approach for prioritizing your initiatives, a way to communicate your priorities, and a clear roadmap to execute against in the coming months.

Establishing priorities for security initiatives

You have built a solid strategy and defined a list of initiatives. You are almost ready to start execution and transform your domain. But then, reality hits: A critical incident emerges, a new regulatory requirement surfaces, a major business initiative demands support, or an executive asks you to accelerate a different priority. Suddenly, the roadmap that seemed clear only weeks ago is competing with new demands for time, resources, and attention.

In a dynamic environment where priorities shift frequently, it is paramount for you to be doing the right things at the right time. To do that effectively, you need a framework that allows you to quickly make decisions when faced with competing priorities.

This section begins by examining common mistakes that can undermine prioritization. From there, you will establish a consistent way to evaluate initiatives and communicate trade-offs to stakeholders.

Avoiding common prioritization mistakes

Understanding general prioritization mistakes is just as important as selecting the right initiatives. The common pitfalls show up often, especially in fast-paced environments.

First is *saying yes to everything*. This approach may have worked in previous roles where the results were solely dependent on you. It is tempting to accept one more ask, which is likely going to show your value and demonstrate team spirit. Your team may support you initially, especially if they are trying to impress you.

However, if you keep on saying yes without taking anything off their plate, at some point your team is going to break; tasks are not going to be completed on time, and signs of burnout are going to show sooner rather than later. If you are not careful, you may miss key objectives in your plan because your team simply lacks the capacity to execute everything successfully. Before accepting a new request, be explicit about what will need to change in the existing plan.

Rejecting business needs is another problem. At the other extreme, security leaders sometimes protect the roadmap so tightly that they unintentionally communicate "security first, business later." Your role is to protect and enable the business, not dismiss its needs. When a time-sensitive request arises, evaluate the trade-offs and determine which existing priorities may need to shift. After all, the overall outcome of the security program depends on business leaders prioritizing and supporting your initiatives.

Next, we have *missing regulatory requirements*. New regulatory and privacy requirements may emerge during the year, often with fixed deadlines and consequences for noncompliance. Establish a regular cadence with Legal, Compliance, or another designated team to review upcoming changes and determine their effect on the roadmap. Learning about a requirement too late will not relieve the organization of its responsibility to meet it.

Ignoring emerging threats or dismissing a threat that has not yet affected your organization is quite easy. Waiting until it does means you are being reactive without enough time to prepare. The new threat will come up at a bad time, and you will need to explain the logic of why you did not deem it a priority to upper management and the board. Evaluate emerging threats against your environment and document why you decided to accelerate, monitor, or defer the related work.

Overlooking risk assessments and audit findings is another issue. Annual risk assessments and audit findings should directly inform roadmap priorities. This seems trivial, but many solid leaders simply forget about them until they are past due. Track the commitments, owners, and deadlines associated with them so they do not disappear behind newer initiatives. You may also need to demonstrate progress to senior management, the board, auditors, or regulators.

The final pitfall is *failing to document decisions*. In an unknown number of months, a breach is likely to happen. Then, you may be asked to explain why certain initiatives were prioritized while others were deferred. Maintain a record of the information available at the time, the trade-offs considered, and who participated in the decision. The goal is a clear record of how the decision was reached.

Avoiding these pitfalls will help you stay focused on the task at hand, preserve valuable time and resources, and keep your roadmap on track. The next step is establishing a framework that enables you to evaluate competing demands and make prioritization decisions consistently.

Building the prioritization matrix

Before you can determine what to do first, you need a way to compare initiatives consistently. The ideal tool would go beyond gut instinct and remove the influence of whoever is "yelling the loudest" that week. Building a prioritization matrix gives you that framework for evaluating work, aligning expectations, and making transparent decisions.

Identifying prioritization factors

Risk prioritization factors help you evaluate which security initiatives should be addressed first by evaluating how much risk they reduce, how likely that risk is to occur, and how much it matters to the business.

Over the years, we have seen organizations take different approaches. There is no right or wrong answer, as budgets and risk appetites vary greatly from one company to another.

To help you take the guesswork out of how you should prioritize initiatives, we captured some of the most common factors security leaders choose from. You should take the time to develop your own prioritization matrix.

Table 4.1 offers different factors you could choose from or add additional ones based on your own experience:

Category	Factor	Rationale
Threat and Risk Exposure	Likelihood of exploitation	How probable is it that this vulnerability will be exploited?
	Impact severity	It considers the business consequences if exploited (operational, financial, legal, reputational).
	Scope	It considers the number of assets, users, systems, or processes impacted if the risk materializes.
Business Alignment and Value Factors	Business enablement	Does this initiative support strategic business goals?
	Protection of crown jewels	Does it directly protect mission-critical systems, sensitive data, or revenue-generating services?
	Customer/market impact	Does it reduce risk to customers or improve market trust, competitive differentiation, or certification readiness?
	Executive/board visibility	It considers the level of executive attention or scrutiny attached to this risk or initiative.

Category	Factor	Rationale
Feasibility and Execution	Organizational readiness	Is the company capable of executing this now in terms of skills, maturity, and stakeholder ownership?
	Time sensitivity	Is this risk growing rapidly? Is there a deadline or window of opportunity?
	Complexity and dependencies	It considers the number of teams, technologies, or approvals required to execute the initiative.
Risk	Risk reduction value	How much does this initiative reduce or transfer risk when completed?
	Operational efficiency gain	Will it reduce manual processes, redundancy, or technical debt?
Organization-level Acceleration	Strategic enabler	Will this capability enable multiple future initiatives?
	Automation potential	Does it eliminate future repetitive manual effort?

Table 4.1 – Identifying prioritization factors

The factors listed above provide the foundation for your prioritization framework, but identifying them is only the first step. To make informed decisions, you need a consistent way to evaluate initiatives against those factors and compare them objectively. Some leaders rely primarily on experience and judgment, while others prefer a more structured scoring model. In practice, the most effective approach combines both, allowing you to move quickly while maintaining consistency and defensibility in your decision-making.

Applying prioritization factors

Once the factors are defined, you should evaluate each initiative. There are three complementary approaches: qualitative, quantitative, and hybrid. *Table 4.2* compares their strengths, limitations, and when to use them.

	Qualitative	**Quantitative**	**Hybrid**
Description	Relies on experience, judgment, and business context to evaluate initiatives based on factors that may be difficult to quantify; this approach is particularly valuable when data is incomplete, emerging risks exist, or rapid decisions are required	Uses structured scoring to evaluate initiatives against prioritization factors. Each factor is assigned a relative weight based on its importance to the organization, helping leaders compare competing initiatives in a more objective and transparent manner	Combines qualitative judgment with quantitative scoring
Strengths	Fast, flexible, and grounded in real-world context; effective when trust and relationships are strong	Objective, repeatable, and easy to explain; reduces bias and supports alignment	Balances intuition with structure; supports consistency without slowing execution
Limitations	Can be subjective and harder to defend if decisions are challenged	Requires quality data and more effort; can create a false sense of precision if inputs are weak	Requires discipline to avoid overweighting one method
When to use	Early in a role, when data is incomplete, or when fast decisions are required	Complex environments, conflicting stakeholder views, or situations requiring executive justification	Most real-world security programs, especially those balancing speed with rigor

Table 4.2 – Comparing qualitative and quantitative approaches to security prioritization

In practice, most security executives use the hybrid approach, which combines both qualitative and quantitative methods. They start with a qualitative approach to establish an initial view, then strengthen it with quantitative scoring to validate or adjust placement as needed.

Whether you use a qualitative approach, a quantitative approach, or a combination of both, the outcome is the same: a better understanding of which initiatives deserve attention first. The challenge then becomes communicating those priorities and making trade-offs visible to stakeholders. One of the most effective ways to accomplish this is through a visual illustration.

Visualizing priorities

As you are assessing each initiative, the next step is to translate those evaluations into a form that is easy to understand and communicate. While there are many options, our favorite visualizations include the **Prioritization Quadrant Model** and the **Sun Diagram Model**.

Regardless of which of these options you choose (or even if you come up with your own model), the visualization gives you and your stakeholders a shared tool for discussing trade-offs. It also becomes a tool for decision-making to instantly show how they compare to existing commitments.

Tip

Because of the constantly changing threat landscape and shifting business needs, you will often find yourself having to rebalance initiatives. The document will be a living visual that will evolve with you during your role. Do not forget to document your thought process and reasoning for prioritizing one initiative over another; this documentation will help you in case of future questioning about your decision-making by upper management, audit, and regulators.

Let's discuss the visualizations mentioned earlier.

The Prioritization Quadrant Model

The **Prioritization Quadrant Model** (see *Figure 4.1*) shows your **annual** initiatives along two dimensions: *impact* and *effort*. The model groups initiatives into four categories:

- Quick Wins (High Impact/Low Effort)
- Strategic Investments (High Impact/High Effort)
- Opportunistic (Low Impact/Low Effort)
- Avoid/Defer (Low Impact/High Effort)



Figure 4.1 – Prioritization Quadrant Model

Remember that not all initiatives within a quadrant are created equal. Even among quick wins or strategic projects, relative importance may shift based on timing, dependencies, or emerging risks.

Effort should also be viewed from an organizational perspective, not just a cybersecurity one. An initiative that appears to be low effort to the security team may require significant work from engineering, infrastructure, product, or business teams with competing priorities. For example, both enabling data masking and remediating a bug bounty finding may depend on a development team's backlog, as they both require application code changes.

The Sun Diagram Model

Under certain circumstances, you may want to present your **three-year initiatives.** This is particularly common when introducing a new multi-year strategy, communicating a transformation program to executives or the board, planning major platform migrations, or demonstrating how foundational initiatives will enable future capabilities.

The Sun Diagram Model is an elevated roadmap visualization that does just that. It uses two dimensions: *impact* and *time*, helping stakeholders understand not only when initiatives will occur but also how they contribute to the organization's long-term security vision.

Each initiative is represented in a bubble, and the size or color of the initiative represents the level of effort it is going to take to complete.

If you have more than 10 initiatives (you likely do!), it is easier to create a numbered list of initiatives to the right of the diagram and use numbers in the diagram itself. *Figure 4.2* shows an example of the model, including the initiative list.

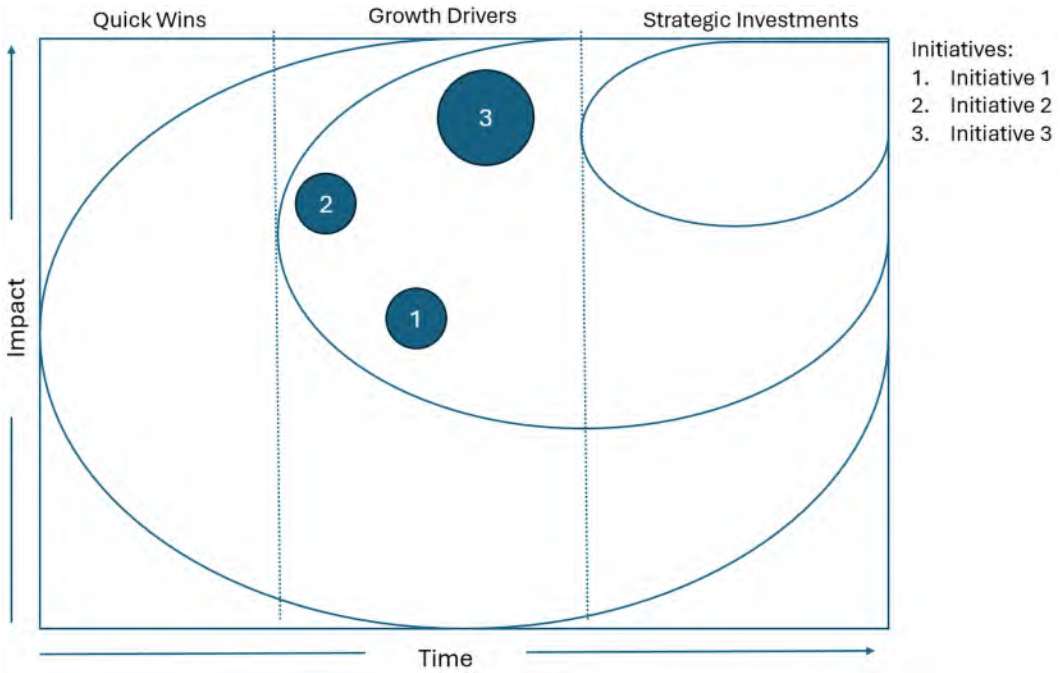


Figure 4.2 – Sun Diagram Model

Prioritization and roadmap planning answer the questions of what to do and when to do it. Next, we should explore whether your technology stack is aligned with those priorities and the future state you are trying to achieve.

Optimizing the security technology stack

As part of the initial assessment described in *Chapter 1*, you collected information about your security tool stack. You now have a clearer understanding of the organization's security needs and can evaluate whether your current tools are delivering the value you expect at a cost you can justify.

This is also an opportunity to build for the future, allowing your stack to evolve alongside the organization and support long-term success. Organizations can evaluate their technology stack in several ways. The right approach depends on the company's culture, the maturity of

the team, and the complexity of the environment. In practice, most organizations will take a hybrid approach, combining the internal team's knowledge of the environment with an external perspective on market trends, peer practices, and technology options.

The following table summarizes the most common approaches:

Approach	Benefits	Considerations
Internal assessment	Leverages the team's firsthand experience, institutional knowledge, and deep understanding of the environment	May be limited by internal assumptions, historical bias, or lack of visibility into broader market trends
Consulting firm assessment	Provides a broader industry perspective, peer benchmarking, and an external view of gaps, overlaps, and opportunities	Some firms may have preferred vendor partnerships, which can influence recommendations
Hybrid assessment	Combines internal context with external perspective, often producing more balanced recommendations and stronger stakeholder buy-in	Requires a clear scope, alignment on decision criteria, and active participation from internal teams

Table 4.3 – Comparing approaches for evaluating the security technology stack

Once you determine how the assessment will be conducted, the next step is understanding what you already have.

Evaluating current tools

Before making decisions about consolidation, replacement, or future investment, you need to know what each tool does, which domain it supports, where it overlaps with others, and whether it is delivering the expected value. This is the foundation for evaluating your current tool landscape.

Evaluating internally built, best-in-breed, and platform solutions

In the early 2000s, organizations commonly maintained dozens of security vendor relationships. Each product was considered "best-in-breed" and typically addressed a narrow use case. A company might use one vendor for antivirus and another for **data loss prevention (DLP)**.

Starting around 2012, many large cybersecurity companies began shifting toward platform-based solutions. Through acquisitions and internal development, they built broader ecosystems intended to address multiple security needs through an integrated platform.

Vendor solutions, however, are only part of the picture. Some organizations develop security capabilities internally when commercial products do not meet their architectural or operational needs. This approach can provide greater control and tighter integration with the environment, but it also makes the organization responsible for ongoing maintenance and support. An internally built capability should therefore be managed as a product, with clear ownership and a funded lifecycle plan.

In practice, most organizations use a combination of these models. Platforms provide the foundation, specialized products address important gaps, and internally developed capabilities support needs that are unique to the organization.

AI security is a good example. Because the field is still evolving quickly, point solutions and homegrown products may provide the fastest way to address an immediate control gap. In other cases, organizations may extend an existing platform or build targeted capabilities internally. As the market matures, some of today's point solutions will likely be absorbed into broader platforms or become less differentiated.

Tip

Emerging domains often start with point solutions before they become platform capabilities. When evaluating tools in areas such as AI security, be clear about whether you are solving an immediate control gap or making a long-term platform decision. This will help you avoid overcommitting to tools that may be replaced, absorbed, or commoditized as the market matures.

As you evaluate your environment, ask yourself what homegrown products you have, which vendors serve as your core platforms, and which are truly best-in-breed point solutions. Understanding this balance will help you simplify your vendor landscape, reduce operational overhead, and make more intentional investment decisions.

Tool mapping

Start by defining your security domains. Choose a domain model that reflects how you actually run your program, not the one that appears the most sophisticated on paper or sounds impressive. Common examples may include:

- **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)**
- **Center for Internet Security (CIS)** controls
- Custom enterprise domains

Once the domains are established, create an inventory of the security capabilities supporting them, including purchased and internally developed solutions. For each tool, capture key attributes such as the solution name, vendor or internal owner, renewal or lifecycle review date, cost, key capabilities, and major gaps or limitations.

Partner closely with procurement to validate renewal dates, pricing, and contract terms, as these details often influence sequencing and decision-making. Pay particular attention to long-term contracts or auto-renewal windows, as they may limit flexibility or create urgency around when a tool can realistically be replaced, consolidated, or renegotiated.

Table 4.4 provides an example aligned to the custom enterprise domain model:

Primary Domain	Tool/ Vendor/ Internal Owner	Secondary Function	Renewal/ Lifecycle Review Date	Cost	Major Gaps
Identity and Access Management					
Endpoint Security					
Network Security					
Application Security					

Table 4.4 – Example security tool mapping using custom enterprise domains

> **Tip**
>
> Some domains may contain multiple tools. This is normal and, in some cases, even necessary. For example, if your organization places a strong emphasis on resilience and continuity of operations, maintaining layered capabilities is intentional and should not be forced into consolidation.

Your final step as part of the current tool evaluation is to validate it with others outside of security. For instance, before making changes to **application security (AppSec)**, you should consult with the development teams. This review increases accuracy and will help guide the following steps. During these conversations, cover the following topics:

- Are the tools mapped to the correct domains?
- Are any domains missing adequate coverage?
- Where do they see redundancies?
- How do tools depend on one another across domains?

Once the mapping has been validated, you should have a clearer picture of your current-state environment. This current-state view becomes the foundation for designing the future state. The goal is not to change everything at once, but to identify the few opportunities that will meaningfully improve security, reduce friction, and align the technology stack with your roadmap.

Designing the future state

Begin by clarifying what matters most to the program right now. Your priorities will shape which tools you optimize, consolidate, or replace. Consider the following questions:

- Are you trying to free up budget, perhaps due to budget cuts or to reinvest elsewhere?
- Do you need a more agile vendor that can quickly deliver a specific feature?
- Are you improving the efficiency of day-to-day operations?
- Are there new regulatory requirements you must meet within a defined timeline?

Based on this analysis, identify the top one to three opportunities per year. Why so few? Because in most cases, meaningful tool changes require planning, implementation, migration, and testing, all of which involve professionals outside of the cybersecurity team. This change is likely going to come on top of all the initiatives we have already discussed, so limiting the scope ensures you focus on what truly moves the needle and delivers the highest return on investment.

At this point, we assume you will follow the vendor selection process already established by your organization, along with the sequencing guidance outlined later.

Designing the future state requires more than identifying the tools you want to keep, replace, or consolidate. It requires judgment, timing, stakeholder alignment, and a clear understanding of the trade-offs involved. We will illustrate this next with the help of some case studies.

Security simplification case studies

Security tool rationalization is not a straightforward process. Organizations often face difficult choices between when to consolidate on platform solutions and when to retain best-in-breed tools.

Note

The case studies discussed in this section illustrate the real-world challenges and trade-offs involved in simplifying a technology stack, including a platform-to-platform replacement and a best-in-breed-to-platform migration followed by a return to the original product. They highlight the importance of verifying that any change reduces risk, improves efficiency, and aligns with long-term strategic goals. The focus is on two more nuanced situations that reveal the operational, technical, and organizational complexities that can arise during transitions.

Case study 1: platform to platform

Consider a new security operations leader who joined the organization and inherited an endpoint protection platform that was not reliably detecting malware. Early on, they relied heavily on assurances from the vendor's sales team that the gaps would be addressed "in the next release." In response, the security team reviewed missed detections, tuned policies, adjusted configurations, and worked directly with vendor support to determine whether the platform's performance could be improved. A year later, the platform was still missing malware and generating inconsistent alerts, forcing analysts to spend more time troubleshooting the tool than investigating and responding to threats.

Coming to terms with the issue

After reviewing the prioritization matrix and broader technology stack, the security operations leader determined that endpoint protection was too foundational a control to remain unreliable. The team had exhausted reasonable tuning options, and the persistent detection gaps posed a material security risk. Replacement was necessary, so the leader prepared a recommendation for stakeholders. Accepting that the solution had failed to meet expectations was not easy. With two years remaining before renewal, replacing the platform early would mean absorbing a substantial financial loss. The replacement was also absent from the

current-year roadmap, and the team was already stretched across other strategic commitments.

Finding a solution

The security operations leader first presented the recommendation to the CISO and technology leaders because the replacement required reprioritizing the roadmap and reallocating technical resources. Finance assessed the financial impact of replacing the platform before renewal, while Legal and Procurement reviewed the contract and potential exit options. Leaders from affected business units evaluated the potential operational disruption. The strongest resistance came from stakeholders in End User Compute whose planned initiatives would need to be delayed to make room for the replacement. Even so, the cost of inaction outweighed the cost of change.

With limited time available, the team shortlisted two vendors based on their malware-detection capabilities, compatibility with the existing environment, migration requirements, commercial terms, and quality of support. The team then conducted a focused, high-intensity **proof of concept (POC)** with both vendors. Domain owners helped validate integrations and dependencies so downstream processes, such as SIEM correlation and incident response playbooks, would continue to function during the migration.

Conclusion

In the end, the organization moved forward with a platform-to-platform replacement. While the work required trade-offs and carried short-term pain, the result was a more resilient endpoint protection strategy, reduced operational friction, and a technology stack better aligned with the company's long-term vision.

Case study 2: best-in-breed to platform and back

A global organization had been relying on a best-in-breed **DLP** product for years. While the tool delivered strong detection and stable operations, its total cost of ownership continued to rise to the point where it was too expensive.

Choosing between options

When the company's broader platform vendor offered a comparable DLP capability at no additional cost, the CISO saw an opportunity: simplify the stack, reduce spending, and reinvest the savings into other high-priority areas of the security program. It sounded like the perfect fit.

To validate this decision, the organization engaged a consulting firm to perform an independent assessment of the security technology stack. The firm brought a broader perspective on industry best practices and helped highlight potential gaps, dependencies, and operational risks. While their input was valuable, the rushed timeline and the team's limited

understanding of the existing DLP renewal schedule meant the assessment could not be completed at the depth needed.

The CISO decided to move forward with the platform solution despite the assessment gaps. However, the transition quickly revealed several operational blind spots. The team underestimated the contract renewal timeline for the existing DLP tool, leaving little room for a pilot. With the clock ticking, the evaluation and migration were rushed, and critical configuration nuances were missed. Gaps between the engineering and operations teams further complicated the rollout, resulting in inconsistent policies between the two tools and missed detections.

Facing unexpected issues

Once deployed, the platform's DLP capabilities failed to perform at the level the team expected. Key features were either immature or unavailable, and the vendor's support organization was slow to prioritize the features the company requested (these capabilities were already offered by the best-in-breed tool out of the box). These deficiencies reintroduced risks the company had addressed years ago and caused significant friction across the business due to the impact on day-to-day operations.

Conclusion

After weeks of struggling with degraded controls, the company ultimately reverted to the original best-in-breed vendor. The anticipated cost savings never materialized, and the team had to find efficiencies elsewhere in the program. This experience reinforced a critical lesson: platform consolidation can unlock value only when evaluation, testing, and operational alignment are given enough time and rigor.

The case studies above highlight that technology decisions are rarely isolated. A tool replacement, consolidation effort, or failed migration can reveal deeper issues in the environment, such as outdated architecture, incomplete integrations, manual workarounds, or controls that no longer perform as expected.

Before finalizing your roadmap, you need to understand where technical debt and legacy risks exist and how they should be prioritized alongside new strategic initiatives.

Managing technical debt and legacy risks

Even if the company was built in the last few years and operates primarily in the cloud, you should assume that there are risks somewhere in the environment. They may not always be visible at first, but over time, shortcuts, outdated assumptions, incomplete migrations, and inconsistent implementations create friction that affects resilience, operations, and security.

Technical debt refers to the accumulated cost of past technology decisions. It is the work that was deferred, deprioritized, or partially completed in order to move faster at the time. Examples may include outdated systems, unsupported software, inconsistent control implementation, manual processes that should have been automated, or systems that aged without being modernized. Like financial debt, technical debt accrues interest in the form of increased maintenance effort, operational instability, slower delivery, and elevated security risk. Put simply, technical debt is the work you put off today that may come back and bite you later.

Legacy risk is closely related, but slightly different. It occurs when older systems, tools, exceptions, or architectural patterns remain in use long after their intended lifespan. These systems may still function, which often creates a false sense of comfort. However, they may lack vendor support, struggle to integrate with modern security capabilities, or rely on outdated assumptions about how the environment operates. Legacy risk often hides in areas that leadership assumes are "fine" because they have not yet failed.

Some legacy risks are obvious, such as unsupported platforms or aging infrastructure. Others are less visible, such as exceptions that were never revisited or controls that work in one environment but not another due to configuration drift. Because these issues may not disrupt normal operations, they often remain hidden until an incident, audit, regulatory review, or major transformation exposes them. You will need to make the risk visible, incorporate the remediation into the roadmap, and build the case for funding. For that reason, technical debt and legacy risk should not be treated as background noise or deferred indefinitely. They are risk categories that should be evaluated and prioritized with the same rigor as other security initiatives. Use the prioritization factors discussed earlier in this chapter to assess impact, likelihood, operational dependency, regulatory exposure, and remediation complexity. Issues selected for near-term remediation should be incorporated into the roadmap, making debt reduction an intentional part of the execution plan.

Realistically, you are unlikely to address every known issue within a single roadmap cycle. Technical debt and legacy risks that cannot be remediated immediately should be formally documented as self-identified issues, assigned to the appropriate owner, and reviewed through an established risk governance cadence. Because remediation often depends on technology or business teams outside cybersecurity, this process makes those dependencies visible and creates a clear record of the decisions made. If an incident later involves one of these conditions, leadership can see that the risk was identified and communicated and that remediation required coordinated action. The goal is to establish shared accountability for risks.

Planning for phased implementation — security roadmap

Effective planning requires more than listing projects on a timeline; it requires sequencing dependencies, identifying foundational prerequisites, and managing risk-based urgency. In this section, we will walk you through how to break initiatives into a roadmap consisting of logical phases, map cross-team dependencies, and visualize them.

If your organization already uses Agile, or a similar delivery framework, the most effective approach is to integrate security into the existing process rather than create a separate one. Security initiatives often depend on engineering, infrastructure, product, and business teams, which means they need to be planned within the same rhythms those teams already use. Creating a parallel security-specific process may feel faster at first, but it often creates confusion, slows adoption, and produces fewer effective outcomes.

Note

For the purpose of this section, we assume you are familiar with your organization's delivery model and will use the roadmap concepts below to strengthen, not replace, the processes already in place.

Sequencing dependencies across initiatives

With the priorities set, you should now determine the order in which initiatives can be executed. Security programs do not fail because leaders choose the wrong initiatives; they fail because initiatives are pursued in the wrong sequence.

Before placing initiatives on the roadmap, evaluate the conditions that could affect timing, sequencing, and execution readiness. Some efforts require foundational capabilities that do not yet exist. Others compete for the same resources, which are not available to support them. They could even introduce new risks if launched too early.

Sequencing the steps minimizes rework by allowing each initiative to build on the work completed before it. The framework that follows provides a structured approach to mapping these dependencies and translating them into a practical roadmap. The steps we will be discussing in the following sections are often carried out by program managers, but program managers are generally not cybersecurity subject matter experts. They will rely heavily on what your team provides them and may not probe for the specific dependency questions security leaders instinctively ask. You can take a more active role during this phase by asking the suggested questions during each phase to validate assumptions, uncover hidden dependencies, and guide the roadmap toward a more realistic execution plan.

Tip

If you have more than five initiatives, you will only be able to take this very detailed approach with your most critical ones (your pet projects). Once your team sees how you operate, they are likely to follow you and take a similar approach at their level.

Identify foundational prerequisites

Many security initiatives rely on an underlying technical or architectural capability. Before sequencing, determine which efforts must happen first. For example, identity stabilization often precedes access governance work, and endpoint agent consolidation typically needs to happen before you can meaningfully improve SIEM use cases. These foundational steps create conditions for subsequent initiatives to succeed. Before sequencing the initiative, validate the following assumptions:

- What technical capabilities must be in place before work on this initiative starts?
- Does any legacy system or tool stop us from moving forward?
- Do teams agree on how the current process works today?
- If we accelerate this initiative or automate this process, what could break?

Tip

Dependencies are not just technical; they also include people, process, and governance. Before you attempt to automate, integrate, or scale, ensure the underlying processes are stable and repeatable.

Look for hidden "enabler" projects

Some initiatives act as force multipliers because they unlock value across multiple domains. These "enablers" reduce friction, accelerate maturity, and simplify downstream work. When sequenced early, they improve the effectiveness of the entire roadmap. Common examples include establishing a reliable asset inventory, normalizing telemetry across tools, building a standardized cloud landing zone, and formalizing data classification. Before sequencing an enabler initiative, validate the following assumptions:

- If we complete this initiative first, what other work becomes easier or faster?
- Is this initiative foundational to multiple strategies or capabilities?
- What happens if we delay this? Does it slow down the entire roadmap?

Note

Enablers are often "unexciting," but they remove hidden bottlenecks. Prioritizing them early allows security initiatives to scale sustainably.

Evaluate risk-based urgency

Not every initiative can wait for perfect sequencing. In some cases, the level of risk, measured using the prioritization factors outlined earlier in this chapter, demands immediate action. When a critical control gap exposes the organization to material business, regulatory, or operational risk, you may need to move quickly, even if foundational work is still underway. In these situations, teams often deploy short-term compensating controls while building toward the long-term solution. The key is to balance urgency with feasibility so that fast action does not introduce instability or create additional technical debt. Before accelerating an initiative, validate the following assumptions:

- What is the risk of waiting six or twelve months, based on the prioritization factors we established?
- Are there feasible short-term mitigations or compensating controls that reduce exposure while long-term work continues?
- Does this initiative reduce a critical, regulator-identified, or board-visible risk?
- If we accelerate this effort, do we have the resources to execute?
- How could this impact stability?

Once dependencies are understood, the roadmap begins to take shape. You now know which initiatives must happen first, which can run in parallel, which should wait, and which may need to accelerate because of risk. With the sequence established, you can now decide how best to present it to different stakeholders.

Visualizing the roadmap

The next step is to translate your plan into a clear, visual roadmap. We like using a timeline view, showing how initiatives build on one another, where resource constraints exist, and when the organization will see meaningful risk reduction.

For many stakeholders, the roadmap is where the security strategy stops being abstract and becomes actionable. The level of detail should change based on your audience. *Table 4.5* summarizes how to tailor your visualization for different audiences.

Audience	What They Need	Diagram
C-suite and board	A single slide showing major results over the next 24–36 months	Sun Diagram (outlined earlier in this chapter)
Direct reports and initiative owners	A detailed view focused on the next 12 months, including dependencies and major milestones	Gantt chart timeline or swimlane timeline

Table 4.5 – Roadmap visualization options by audience and use case

The following subsections take a closer look at each one, beginning with the Gantt chart, a useful format when the audience needs to understand timing, dependencies, and how initiatives overlap across the roadmap.

Gantt chart timeline

A Gantt chart is ideal when your audience needs to understand duration, sequencing, and overlap across multiple initiatives *by domain*. It is useful for project managers, engineering leaders, and operational teams who need to coordinate work. Its strength is that it shows whether the planned work can be delivered within the available timeframe. *Figure 4.3* illustrates how initiatives can be organized by domain and sequenced across the roadmap.

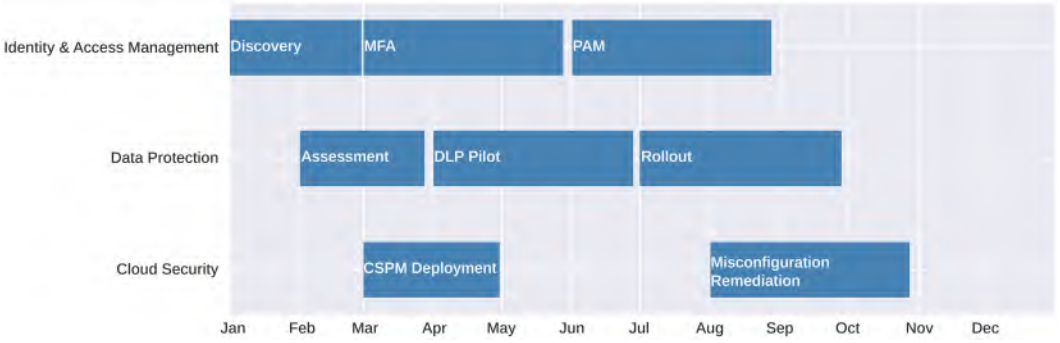


Figure 4.3 – Sample Gantt chart timeline

PAM: privileged access management; CSPM: cloud security posture management

A missed milestone should be represented in a way that makes the issue immediately visible to stakeholders. Best practice is to show both the planned and actual milestone so that variance and the impact on downstream tasks are clear. This dual representation also shows how the milestone affects the overall timeline.

Swimlane timeline

A swimlane timeline works best when you need to show ownership, cross-functional collaboration, and role clarity *by team*. It serves department leaders and program managers who want to illustrate how different teams contribute to the roadmap over time. Swimlanes help resolve accountability gaps and make it easy to see organizational alignment. *Figure 4.4* shows how initiatives can be separated by team while remaining connected through a shared timeline.

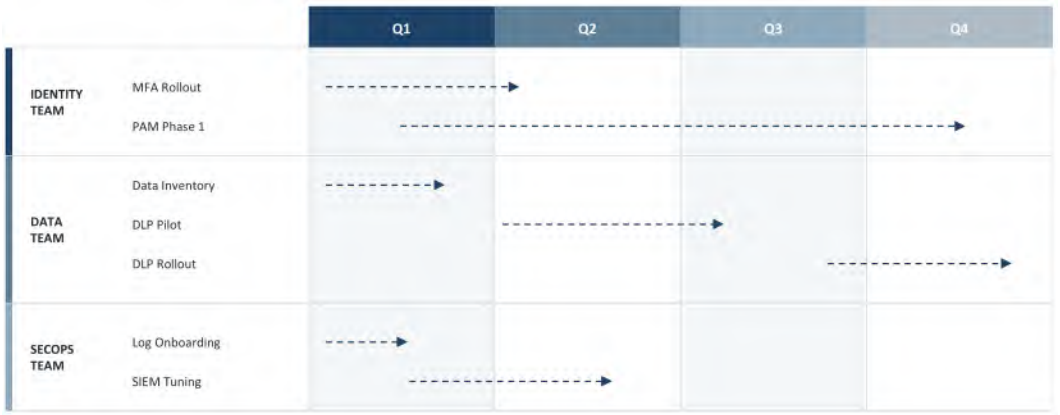


Figure 4.4 – Sample swimlane timeline

Even though swimlanes highlight ownership, they require extra structure to make deadlines visible. Use milestone diamonds with dates, quarterly boundaries, and a "today" marker to show progress. Color-code at-risk items and show dependency arrows so teams can see immediately when slippage in one lane impacts another. This keeps the swimlane simple while making sure that deadlines stay visible.

Measuring the roadmap's progress

A security roadmap is only effective if its progress can be measured. In addition to defining what you are trying to achieve, you should also track how well the work is progressing. This requires an additional layer of measurement beyond strategy.

The strategic metrics introduced in *Chapter 3* define the long-term outcomes that the plan is designed to deliver. To complement these outcomes, execution metrics focus on the operational health and feasibility of delivering the roadmap itself. They measure whether the work is progressing as intended, where friction exists, and how confidently the team can deliver what was committed. Here are a few examples of execution metrics:

- Roadmap execution health
    - Percentage of initiatives completed on time
    - Percentage of initiatives delayed due to dependency or readiness issues
- Dependency and risk tracking
    - Number of blocked initiatives
    - Time lost due to rework or misaligned architecture

Table 4.6 compares strategic and execution metrics:

	Strategic Metrics	**Execution Metrics**
Objective	Define what success means	Track whether we're getting there
Focus	Business outcomes and risk posture	Operational progress and feasibility
Time Horizon	Long-term (12–36 months)	Short- to mid-term (quarterly/phase-based)
Audience	C-suite, board	Program managers, **project management office** (**PMO**), security leadership

	Strategic Metrics	**Execution Metrics**
Format	KPIs, outcome targets, risk impact	Milestones, progress indicators, health scores
Example	Reduction of risk exposure by 40%	80% of Phase 1 roadmap complete

Table 4.6 – Comparing strategic metrics and roadmap execution metrics

Note

In *Chapters 6* and *7*, we will introduce domain-specific metrics that go deeper into each security capability. Together, these layers provide both the destination and the day-to-day signals needed to keep the roadmap on track.

Reviewing roadmap performance

Defining metrics is only valuable if they are reviewed consistently. One of the most effective ways to do this is through a regular cadence that may be referred to as a **Monthly Roadmap Review** or **Security Delivery Review**. In this forum, teams step back from day-to-day execution to assess progress, surface risks early, and course-correct before small issues become major problems.

A **monthly review** usually strikes the right balance. If something falls off track, you learn about it soon enough to take corrective action without waiting until the end of the quarter or year. These sessions are not about status reporting for its own sake; they are about gaining a realistic view of roadmap health.

The biggest risk in these meetings is **over-reliance on self-reporting**. Some leaders may feel pressure to present everything as "green" and on track, only for problems to surface weeks or months later when recovery is far more difficult. Execution metrics are especially powerful here because they shift the conversation from confidence to evidence. The questions introduced earlier in *Sequencing dependencies across initiatives* can also help you test assumptions and explore dependencies while creating space for honest discussion.

I learned why this matters while leading a complex initiative involving many stakeholders and interdependent workstreams. The team held regular project meetings without me and consistently assured me that everything was on track. I wanted to give them room to lead and trust the process, yet something in the updates did not feel right.

Eventually, I insisted on a deeper review. That was when I learned that milestones were already slipping, key dependencies remained unresolved, and stakeholders were working from different assumptions. The status reflected how much activity was occurring rather than whether the initiative was producing the intended outcomes. Team members had also been reluctant to escalate concerns, allowing the reported status to remain more optimistic than the underlying facts supported.

For many new executives, the instinct in this situation is to return to manager mode. That was certainly my instinct. When you discover that work is off track, it can feel faster and safer to attend every meeting, direct individual tasks, and solve the problem yourself. Doing so, however, pulls you away from your executive responsibilities and weakens the accountability of the managers who should own delivery.

As an executive, you cannot remain involved in the details of every large-scale program, yet you are still accountable for the outcome. Your role is to define the outcome and maintain enough visibility to determine whether it remains achievable. The managers responsible for the program should own the execution and be held accountable for delivering it.

My intervention was therefore not about taking over the day-to-day management of the project. I brought the stakeholders together to map what clients would experience and required the plan to be re-baselined around a more realistic view of delivery. Rather than stepping into daily execution, I focused on the downstream client impact. The leadership challenge was finding the right altitude, close enough to recognize when the plan was drifting, while keeping ownership of the work with the managers responsible for delivering it.

Tip

Do not wait for a fixed percentage of the roadmap to fall behind before raising concerns. Escalate when a critical commitment is at risk or recovery would require reprioritizing the roadmap. Bring your manager and affected stakeholders a clear view of the impact and your recommended path forward. There is nothing worse than discovering a misalignment at the end of the year when options to course-correct are limited.

Notes from the field with Renana

Case study: many voices to one roadmap

When a security organization grows quickly, its tools, findings, and expectations often grow even faster. During a significant transformation in 2021, several teams deployed new capabilities, including Data Loss Prevention, Cloud Security Posture Management, and Attack Surface Management. Each tool produced its own findings. Since we had not yet created a unified execution plan, the volume of findings soon outpaced the organization's ability to

respond. The challenge was not a lack of data anymore; it was the absence of a roadmap to direct the work. Every security team was engaging engineering teams independently, asking them to prioritize issues identified by their specific tool. Each group within security believed their work was most urgent. Everyone's intentions were good, but the result felt chaotic. Development teams received multiple, competing requests, and no one had a complete view of the full remediation picture.

The strain began to show. Engineers felt overwhelmed and frustrated as security work felt endless and disconnected from business priorities. Security teams were equally frustrated; they expected action on high-risk findings but encountered resistance instead. This tension revealed that execution needed to both identify what needed to be fixed and sequence that work in a way the business can absorb. The lack of structured prioritization made everyone feel like they were failing, even though they were trying to do their best.

To break the cycle, we stepped back and introduced a unified prioritization model that weighed the severity, business impact, dependencies, and engineering bandwidth. This clarified what needed to be addressed first and gave the security organization one voice when engaging the business.

With prioritization in place, we began building a consolidated remediation roadmap that showed what each team should address and when. Visualizing the plan helped their leaders see how the work fit together. Just as important, we documented known gaps and created risk issues for second- and third-line teams, turning risk into governed accountability.

The roadmap fundamentally changed the dynamic. Cybersecurity stopped speaking with different voices and began operating as one. Engineering teams understood the workload ahead and had a realistic timeline for meeting obligations. Security teams saw progress instead of noise. Momentum replaced friction.

The experience shaped how I now approach roadmap execution. The unified roadmap did more than organize delivery; it gave security teams one voice and allowed priorities to be reassessed as conditions changed. That lesson became even more relevant in 2026 with the emergence of AI-enabled vulnerability discovery capabilities such as Mythos. Mythos changed our assumptions about remediation timelines by accelerating how quickly vulnerabilities could be discovered and validated, including weaknesses in control implementation and unresolved technical debt. Work that once appeared manageable could become urgent much faster.

This is why a roadmap cannot be static. It must provide enough structure to align teams, but enough flexibility to adapt when the threat landscape changes. When new technology changes the likelihood, speed, or impact of exploitation, the security organization needs a mechanism to reassess priorities quickly and communicate those changes with one voice.

Summary

In this chapter, we moved from strategy to execution by turning the security plan into a prioritized roadmap. The key lesson is that leadership is not about doing everything at once; it is about choosing the right things at the right time. A strong roadmap gives security leaders a structured way to make those choices, especially when business needs, regulatory requirements, emerging threats, and operational constraints compete for attention.

We explored how to establish priorities using common risk and business factors, apply qualitative and quantitative decision-making methods, and visualize trade-offs through the prioritization matrix and quadrant model. These tools help leaders compare initiatives consistently, explain why one effort should move ahead of another, and document the reasoning behind those decisions. Just as important, they create a common language for discussing what should happen now, what can wait, and what must be revisited as conditions change.

We also examined how to translate priorities into phased implementation, evaluate the security technology stack, and account for technical debt and legacy risk. Sequencing dependencies, identifying enablers, and visualizing the roadmap help reduce rework and make execution easier for stakeholders to understand.

As you move into the next chapter, the focus shifts from building the roadmap to making it sustainable, determining whether the plan is funded, staffed, governed, and supported by the operating model needed to deliver it.

Chapter checklist

- Build the prioritization matrix. Select the factors that matter to your organization and use them to evaluate competing initiatives consistently.
- Create an executive view of your priorities. Use the Prioritization Quadrant or Sun Diagram to communicate trade-offs and support stakeholder decisions.
- Evaluate current security capabilities. Identify one to three opportunities to improve the environment through purchased or internally developed solutions, while accounting for technical debt and legacy risk.
- Build and visualize the security roadmap. Sequence initiatives around dependencies, organizational capacity, and risk-based urgency.
- Establish a Monthly Roadmap Review. Use execution metrics to assess progress, identify issues early, and adjust the roadmap when conditions change.

Additional resources

- The Prioritization Quadrant Model: `https://bit.ly/CISOBook10`
- The Sun Diagram Model: `https://bit.ly/CISOBook11`
- Gantt chart timeline: `https://bit.ly/CISOBook12`
- Swimlane timeline: `https://bit.ly/CISOBook13`
- The Security Capability Mapping Spreadsheet: `https://bit.ly/CISOBook14`

Part 2

Building the Program

With a clear direction and roadmap in place, this part focuses on the core areas a security executive should manage to generate impact. You'll learn how to secure funding, navigate legal and procurement considerations, and develop the team; strengthen core security functions; protect identities and critical data; and establish effective governance, risk, and compliance practices. By the end of this part, you'll be equipped to make informed decisions, advance the program, and demonstrate tangible progress against the roadmap.

This part of the book includes the following chapters:

- *Chapter 5, Fueling the Program: Budgeting, Legal, and People Management*
- *Chapter 6, Operationalizing Defense: Core Security Functions*
- *Chapter 7, Protecting the Crown Jewels: Identity, Access, and Data Security*
- *Chapter 8, Navigating the Landscape: Governance, Risk, and Compliance (GRC)*

5

Fueling the Program: Budgeting, Legal, and People Management

In *Chapter 4*, you translated your vision into a prioritized roadmap. You clarified what matters most, sequenced the work, and made the trade-offs required to move to execution. The next challenge is enabling that roadmap.

To run an effective security program, funding must be secured, contracts and legal obligations must be understood, and people must be hired, developed, and retained. Even the strongest strategy cannot succeed without funding, business partnerships, and the right people to execute it.

Most of us entered cybersecurity to solve problems, reduce risk, and protect organizations, not to spend our time in budget reviews, contract discussions, legal escalations, or talent planning. Yet this is one of the defining transitions from security manager to security executive. As your scope expands, your success now depends more on enabling others to succeed through sound business decisions.

This chapter focuses on practical tools to enable execution and covers the following topics:

- Making a credible security budget ask
- Using procurement levers and contract protections
- Navigating privacy incidents with legal
- Building a high-performing team

By the end of this chapter, you will have frameworks and guides to shape your approach to budget management, procurement and legal partnership, privacy incident readiness, and talent decisions. This chapter is the starting point. Real fluency develops through repetition:

asking better questions, learning how your partners evaluate decisions, and applying these lenses in live situations where trade-offs, timing, and accountability matter.

Making a credible security budget request

Chapter 4 helped you determine what matters most and how the work should be sequenced. With that foundation in place, the next question is: *can you afford it?* This is where prioritization becomes a financial conversation.

Early in your career, you likely did not spend much time trying to read a balance sheet. Like many security leaders, you focused on technology, hoping the numbers would somehow line up and that no one would ask you too many detailed questions.

This approach is not enough at the executive level. As your scope and influence grow, being able to explain where the funds are spent and the **return on investment (ROI)** out of that expense is critical *before* making any budget request.

You need enough financial fluency to defend your choices and secure the funding your program needs. Executive leadership is often less about having every answer and more about building confidence that you are making thoughtful decisions on behalf of the business.

Having clarity on both priorities and funding sources positions you to make thoughtful trade-offs and advocate for the resources your program requires. Let's walk through the groundwork of making a compelling budget ask.

Building credibility with finance

Start by setting aside time for finance to walk you through your budget in detail. Their "love language" is different than yours and focuses on numbers (not technology!). Only when you can comfortably discuss CapEx versus OpEx, explain how spending shifts over time, or articulate where savings might emerge within your existing budget (even if that is two years out) do you change the dynamic of the conversation.

From their perspective, only then will you demonstrate financial stewardship. That moment matters, as it is often the turning point at which finance begins to view cybersecurity as a partner.

Bring your leadership team into the conversation. They should experience what financial responsibility feels like firsthand. Helping your direct reports understand how budgets work, how trade-offs are made, and how investment decisions ripple across the organization means that you are not carrying the financial narrative alone. Over time, this shared understanding improves decision-making at every level of the team.

Finally, turn this first meeting into a regular cadence (monthly works well for most). Regular check-ins allow you to track spend, anticipate challenges, and course-correct early. They also help you stay prepared.

Tip

Always maintain a short list of prioritized initiatives (projects, tools, or headcount) that sit just below the funding line. When opportunities arise, such as unspent budget at the end of a quarter or year, you will be ready to act decisively and responsibly.

Building this rhythm with finance does more than help you track spend. It helps you evaluate whether your current budget is being used effectively and gives you the credibility to ask for additional funding in certain cases.

Laying the groundwork: earning the right to ask

Before we go any further, a word of caution: it is easy to ask for more funding, but it is hard to keep being taken seriously when you ask repeatedly without demonstrating discipline. Cybersecurity leaders lose credibility when they make an unreasonable ask, fail to show they have fully optimized what they already have, or don't speak the right language.

Before you ask for more funding, you need to clearly understand how your existing budget is being used and where it can be used better. That means knowing which investments are delivering outcomes, which are maintaining the status quo, and which may no longer be needed. For example, you may discover that one tool is no longer needed or that a consulting budget can be redirected toward a higher-priority initiative.

Some executives formalize this discipline by partnering with finance to define a set of *Financial Credibility Metrics* that demonstrate efficient management of the current budget. The specific measures will vary from one organization to another, but their purpose is consistent: to answer finance's questions about the security plan in its own "love language"—numbers. These metrics might include forecast accuracy, the variance between planned and actual spending, savings that have been realized and reinvested, or the balance between employees and contractors. Equally important is knowing whom to ask. Your initial budget discussions should start with your direct leadership chain, finance, and key cross-functional partners who can help shape, pressure-test, and refine your request before it ever reaches an executive forum.

Tip

Remember: Internal audit or the board does not allocate funding, and you should not ask them for it. For example, if Internal Audit identifies a control gap, use that finding to strengthen the business case with your leadership and finance partners.

Be prepared to articulate outcomes in business terms, not in security terms. Funding requests framed around tools, headcount, or technical gaps rarely land with executives. Requests framed around risk reduction, operational resilience, regulatory readiness, and business enablement do.

For example, instead of asking for funding to expand endpoint coverage, explain that the investment reduces the likelihood of business disruption from unmanaged devices and improves the organization's ability to respond quickly during an incident.

Deciding whether and how to ask

The next question is whether you should even ask for more funding. Not every gap warrants immediate action. Requesting additional funding beyond your existing budget should be a deliberate decision. Building on the discipline established earlier, the strongest requests are grounded in evidence, timed thoughtfully, and framed to clarify both urgency and trade-offs.

At a minimum, this evaluation should span four dimensions: risk, initiatives, budget, and timing. Reviewed together, these dimensions form a simple decision framework, helping you determine whether to reallocate, defer, phase, or formally request additional funding.

Risk: understanding the problem you are solving

Every funding conversation should begin with risk. Clear articulation provides the rationale for why action may be needed now rather than later. Follow these steps:

- Start by reviewing your top risks based on your initial assessment. Consider whether the exposure falls within the organization's stated risk tolerance.
- If you have a formal risk assessment, use it as a reference point to validate which risks require immediate attention and which can be addressed through the normal roadmap cycle.

Initiatives: clarifying what is possible

Once the risk is clear, assess your initiatives. This step demonstrates discipline, showing that you have already prioritized and made trade-offs.

Review what you can deliver within your existing budget. These are your "above the line" initiatives: the work that is already funded, staffed, and actively moving forward within your current resource limits. Also identify what cannot be executed without additional funding. These are your "below the line" initiatives: the work that remains important but is deferred because it exceeds your current budget, staffing, or delivery capacity. For each deferred initiative, be clear about which risks remain unaddressed and what the business is implicitly accepting.

Budget: anchoring the ask in context

Budget context helps answer the unspoken executive question: *Is this reasonable? How are we doing compared to the benchmark?* It frames your request within market norms and reduces the perception that the ask is arbitrary.

Collect data points through partnership with finance, such as security budget as a percentage of IT spend, as a percentage of company revenue, and security spend per employee.

Additionally, look at how your current spend compares to external market research. These reports are available mostly at the CISO level and can provide useful guardrails, even if they are not a perfect match. One of our favorites is the annual IANS + Artico enterprise and budget report.

Timing: deciding when to act

Timing often determines the shape of the request. Some investments belong in annual planning while others require off-cycle action. Explicitly addressing this trade-off signals judgment and maturity.

Ask yourself whether this investment can wait until the next planning cycle or whether the current risk level is unacceptable today. In cases where urgency exists but full funding may be difficult to secure, the decision does not have to be binary.

Review recent incidents or trends, and whether interim mitigation steps are possible. You may choose to present the full level of investment you believe is required over time, while requesting a smaller portion upfront. This is often referred to as a "seed investment": an initial amount of funding used to start the work, prove progress, and create a stronger case for future investment. This approach accepts a calculated level of risk in the near term, but it often makes it easier for the organization to act, build confidence through execution, and reassess before committing additional funding.

Table 5.1 summarizes the key questions and inputs to review before deciding how to proceed:

Dimension	Questions to answer	Data Inputs	Rationale
Risk	• What are our top security risks? • Are we within risk tolerance?	• Risk assessments. • Incident data. • Industry benchmarks.	Establishes urgency and anchors the request in evidence.

Dimension	Questions to answer	Data Inputs	Rationale
Initiatives	• What can be delivered within the current budget (above the line)? • What is deferred without additional funding (below the line)? • What risks remain unaddressed? • What measurable risk reduction or business outcomes can be delivered monthly or quarterly?	• Security roadmap. • Prioritization outputs.	Demonstrates discipline and transparency around trade-offs.
Budget	• How does our security spending compare to peers or benchmarks? • What percentage of IT spending and company revenue does our security budget represent? • What is the spend per employee?	• Internal budgets. • External benchmarks.	Provides context and reasonableness for the ask.

Dimension	Questions to answer	Data Inputs	Rationale
Timing	• Can this wait for the next planning cycle? • Is risk currently unacceptable? • Are interim mitigations possible?	• Risk tolerance statements. • Budget calendars. • Incident trends.	Determines whether to act now or plan ahead.

Table 5.1 – Funding request decision framework

The framework helps you determine when a funding request is ready to move forward. From there, the work shifts to framing the investment in a way leadership can compare and act on.

Leveraging the budget request template

If you decide to proceed, we assume this is going to be an out-of-cycle budget request. Many security leaders step into the role after budgets have already been set, so their first major funding request may happen off-cycle. This option requires a different mindset than annual planning as you are asking the organization to reassess priorities and make room for unplanned asks. That means the way you frame the request often matters as much or more than the request itself.

One helpful analogy is buying a car for a family. The safest, most fully loaded model may be attractive, but the final decision depends on budget, actual need, timing, and what other commitments the family already has.

The same is true for a funding request. Leadership may understand the risk and still need to weigh the investment against other business priorities, available funding, and the organization's capacity to absorb change. Your role is to present reasonable options, explain the trade-offs, and help leadership decide how much risk they are willing to reduce now.

Using this analogy, an effective out-of-cycle ask should present three options as shown in *Figure 5.1*.



Figure 5.1 – Budget template

The labels used for these options in *Figure 5.1* are meant to guide your thinking, but should not be included in your actual presentation. When making the request, use naming that will resonate with your audience and represent your outcomes.

For example, if your request is focused on vulnerability management, you might present the options as "Stabilize Critical Exposure," "Improve Remediation Capacity," and "Accelerate Exposure Reduction." This keeps the conversation focused on risk reduction and business impact rather than on internal planning labels.

Option 1: minimum viable investment ("Safe to Drive")

This is the lowest reasonable level of investment that stabilizes the most critical risks. It is not comprehensive or everything you want, but it brings risk down to a more acceptable level including the following:

- Targeted controls delivering short-term risk reduction
- Limited scope or phased implementation
- Reduced organizational disruption

This option demonstrates restraint. It shows you understand constraints and are willing to operate within them if necessary.

The advantage is its focus on non-negotiable work and the likely improvement in compliance posture. The trade-off is its limited scope: it may stabilize the most immediate risks without providing the broader protection or maturity the program really needs.

Option 2: recommended investment ("Right Fit")

This is the option you believe is good for the organization. It addresses the top risks, improves maturity, and delivers meaningful outcomes. It includes the following aspects:

- Addressing core risks identified in your assessment

- Measurable improvement in security maturity
- Clear alignment to risk reduction

This option ties directly back to your roadmap, and it reflects the level of change the organization can reasonably absorb. This option is more likely to deliver meaningful improvement across the security plan. The trade-off is competition for shared resources; if the investment requires funding from the IT budget, it may create tension with technology leaders whose priorities are displaced.

Option 3: accelerated investment ("Luxury")

This is a broader, faster investment designed to transform multiple parts of the security roadmap rather than fund a single capability. It can support new capabilities while also addressing the legacy risks and technical debt identified in Chapter 4, particularly where older systems or architectural constraints would otherwise limit progress. Because several workstreams may move in parallel, this option requires significant capacity and coordination from technology and business teams outside security. It may include:

- Expanded scope or accelerated timelines
- Modernization of legacy systems or reduction of technical debt
- Faster risk reduction across different capabilities

Including this option gives leaders visibility into what more could be achieved (remember your three-year roadmap) without forcing them into it prematurely.

Before finalizing these options, ask yourself a critical question: *How much change can the organization realistically tolerate in the next few months?* This is critical because timing and context matter. For example, if the company is in the middle of a major acquisition, it may not be realistic to expect teams to drop that work to support a major new security initiative. In those cases, a phased or minimum viable option may be the responsible choice even if it is not your preferred one.

This option offers the greatest potential to transform the security program, but it also carries the highest execution risk. Success depends heavily on teams outside security having the capacity and commitment to move at the required pace, which can be especially difficult for a first-time executive still building organizational influence.

Navigating the ask with confidence

Even with a prioritized roadmap and a well-prepared budget request, real-world funding conversations rarely go as expected. Executives will challenge your assumptions, timing may

be off, or funding may not be available. The following tips are designed to help you handle these situations with grace.

- Be prepared to live with a "no" or a "not right now." Timing, priorities, and competing initiatives can all affect the decision. Document the rejection and the rationale; this record can be critical later when a security incident occurs and leadership asks why a risk was not addressed.
- You may be asked if there is a middle option (some may refer to it as option 1.5) in between your baseline and preferred request. Do not feel pressured to answer on the spot. Take the time to evaluate trade-offs and respond at a later time.
- When security asks for more funding, there usually is not a hidden money source waiting to be unlocked. Additional investment often means the broader organization needs to reduce spending elsewhere. Understanding this reality and acknowledging it with your peers helps frame your requests with empathy.
- When making your budget request, consider visually showing how each option helps reduce risk; it can make your case more concrete. In *Chapter 9*, we will introduce the Cyber Heat Map as a key tool for communicating risk with executives.

A strong budget case may secure investment. To make that investment work, you also need to understand how procurement shapes contract terms, accountability, risk transfer, and the flexibility you retain as your program evolves.

Using procurement levers and contractual protections

Much like working with finance, you likely did not envision becoming well-versed in legal contracts. As your role expands, your effectiveness increasingly depends on how well you partner with procurement. While you are not expected to become a contract expert, understanding the most important contractual levers will help you engage thoughtfully, ask the right questions, and recognize when contractual decisions carry meaningful risk implications.

In my opinion, procurement is one of the most underutilized risk-management tools available to cybersecurity leaders. Contracts determine not just what you buy, but how vendors are held accountable, how risk is transferred, and how much flexibility you retain when things don't go as planned.

This section focuses on practical contractual levers security executives should understand, when to use them, and how they support both resilience and credibility.

Core procurement levers security leaders should know

The goal of the levers is to create options and accountability before you need them. For clarity: You should not use every lever in every agreement. Knowing they exist helps you partner more effectively with procurement and avoid being surprised.

Table 5.2 highlights the contractual protections most relevant to security leaders and the situations in which they matter most:

Lever	What It Is	When to Use It	Why It Matters
SLAs	Defined performance expectations and remedies	When a vendor provides a critical or customer-facing service	Creates accountability and leverage when failures introduce operational or security risks
Opt-Out/ Termination Clauses	Contractual rights to exit under defined conditions	When vendor performance is unproven or risk tolerance may change	Preserves flexibility and prevents long-term lock-in to unacceptable risk
Incident Notification and Cooperation Clauses	Requirements for timely notification and investigation support	When vendor incidents could affect regulatory or contractual obligations	Reduces surprises and supports faster, compliant incident response
Security and Audit Rights	Rights to assess vendor security controls	When vendors handle sensitive or regulated data	Provides visibility and leverage when controls fall short

Lever	What It Is	When to Use It	Why It Matters
Data Ownership, Protection, and Retention	Contract terms defining data ownership, permitted use, protection, retention, and secure return or destruction	When vendors process, store, or access sensitive or regulated data	Reduces downstream privacy risk, limits unnecessary retention, and supports regulatory obligations

Table 5.2 – Example of procurement levers

Additional contractual protections to be aware of

Not every contract requires the same level of protection. The levers below can be used selectively, and when applied in the right circumstances, they can improve your negotiating position:

- **Contract Length and Renewal Timing**: The length of a contract can be just as important as its price. Long-term agreements often look attractive, especially when paired with discounts, but they reduce flexibility if a tool or vendor underperforms. This risk is **extremely high** early in your tenure, when you are still validating product fit and operational maturity.

Tip

If concerns arise regarding a product during your initial assessment, resist the temptation to lock into a multi-year deal even if the commercial terms are compelling. You have other options to preserve flexibility while you validate performance. If pricing pressure is the concern, use a price protection clause rather than extending contract length.

- **Price Protections and Renegotiation Triggers**: These clauses serve as an alternative to long-term commitments. They allow you to lock in favorable pricing or cap future increases without sacrificing flexibility. This approach is particularly useful when a vendor offers a discounted multi-year deal, but the product or service has not yet proven itself in your environment. In those situations, protect the price (not the vendor) so you retain the ability to adjust course if performance does not meet expectations.

- **Contract Buyout and Transition Options**: In some situations, preserving a clean exit can be just as important as selecting the right vendor. These provisions create an exit path when circumstances change, allowing early termination or a controlled transition, sometimes with financial support from a new vendor. These provisions are most relevant when you are locked into a long-term agreement. Even when these options are never exercised, having them in the contract can restore leverage and prevent leaders from staying with a poor vendor decision, also known as sunk cost, simply because money has already been spent.
- **Liability Caps and Indemnification**: These provisions determine how financial responsibility is allocated when a vendor failure results in harm. While these provisions do not prevent incidents, they clarify accountability and signal that security failures carry real consequences. For vendors handling sensitive data or providing critical services, aligning liability with risk exposure is an important part of managing third-party risk.
- **Publicity and Reference Rights**: Vendors often place significant value on being associated with well-known customers in marketing materials, case studies, or joint announcements. When used intentionally and approved by legal and communications, these rights can increase vendor visibility and credibility, often resulting in discounted pricing, improved commercial terms, or additional value-added services.

Tip

Publicity rights should never be granted by default. They should reflect a deliberate organizational choice: you may decide not to grant them at all or reserve them for a select group of strategic vendors. When granted, they should be time-bound, with brand, legal, and communications involved in the decision.

Partnering effectively with procurement

Invest time with your procurement partner to understand their style, priorities, and negotiation approach, and then let them do their job. Vendors may attempt to engage you directly on pricing or contract terms, but in a corporate environment, this can break protocol and weaken your negotiating position.

Redirect commercial discussions to procurement. You can serve as an escalation point while working with them behind the scenes to support strong outcomes. This discipline protects your credibility as a security leader and ensures that security requirements are backed by enforceable commercial terms.

Your presence is most valuable when setting expectations, clarifying risk requirements, or escalating issues, not negotiating pricing. Even well-intentioned side conversations can undermine months of procurement strategy and weaken your leverage at exactly the wrong moment.

Security leaders can sometimes unlock better commercial terms by engaging directly with the vendor. Only use this option after discussing your strategy with procurement, considering the time and communication method. In practice, it may look like this:

- **If procurement asks you to engage**, then do so with a clear objective, such as reinforcing strategic importance, validating long-term potential, or clarifying security requirements that justify pricing adjustments.
- **If a vendor is early in the sales cycle**, then your involvement can help set expectations around security maturity, roadmap gaps, or required commitments before pricing hardens.
- **If the vendor is pushing for a multi-year deal and you are not ready for it,** explain to procurement why flexibility matters from a risk perspective and ask for support with alternatives such as price protection or phased commitments.
- **If negotiations are nearing closure**, limit your involvement. Late-stage interventions often disrupt leverage and confuse roles unless explicitly coordinated with procurement.
- **If you engage directly with the vendor**, ensure procurement is aware and aligned on messaging before and after the conversation.

Tip

Lean in to shape expectations early or reinforce priorities and step back when numbers are on the table. Your credibility is highest when procurement knows you are supporting the strategy, not negotiating around it.

Strong procurement partnership helps you manage risk through contracts before problems arise. During privacy incidents, legal partnership becomes just as important.

The next section focuses on how security leaders should engage legal when an incident moves beyond technical response and begins to carry regulatory, contractual, or business implications.

Navigating privacy incidents with legal

A privacy incident occurs when a security event may involve unauthorized access to, exposure of, or misuse of personal, regulated, or customer data. These incidents sit at the intersection of security, legal, and business risk because the response may trigger notification obligations, customer commitments, regulatory scrutiny, or disclosure considerations. Understanding that shift (and knowing when to involve legal) is a critical executive responsibility.

This section provides a high-level view of how privacy incidents typically unfold from a security practitioner's perspective. It explains when legal should become involved and how your role shifts from technical lead to cross-functional partner. The intent is not to prescribe one "right" process, but to help you recognize key inflection points and navigate them with confidence.

Use this section as a starting framework, not a substitute for your company's specific legal guidance. You should review these concepts with your legal and privacy teams to validate how incident escalation, privilege, materiality, and disclosure decisions are handled in your organization.

Tip

Treat this section as a conversation starter with legal, not a checklist to follow blindly. Alignment matters more than precision. The best time to confirm roles, thresholds, and escalation paths is before you need them under pressure.

Preparing for privacy incidents

The implications of many incidents go far beyond technical issues. What begins as an alert in the SOC can quickly trigger contractual obligations, regulatory notifications, or customer conversations. The moment an alert crosses that line and becomes an incident above a certain severity threshold, timing and who is involved become important.

Ideally, expectations around escalation and legal engagement were set during your onboarding period. Once you are 120–180 days into the new role (if not sooner), this should be one of the first areas to pressure-test and confirm your understanding of the overall preparedness for privacy incidents. As part of this, discuss the following areas with the relevant cross-functional partners:

- **Clear ownership for keeping requirements up to date:** Someone outside of security should be explicitly accountable for maintaining the inventory of contractual, regulatory, and customer-specific security obligations. This is about *owning the system*

of record, not interpreting the requirements. Without clear ownership, obligations quietly expire, change, or are forgotten, increasing the risk of failing to meet them.

- **Shared understanding of what those requirements mean:** Knowing that requirements exist is not the same as understanding how they apply during an incident. Security, legal, privacy, and compliance should align and **document** thresholds, timelines, and what constitutes a reportable event. This helps create a shared understanding when speed matters most.
- **Defined escalation paths from security:** Escalation fails if the incident never leaves the SOC. Analysts are trained to respond to technical matters, not contractual exposure or business impact. Clear criteria must exist for elevating incidents when privacy or compliance risks may be present, even if technical indicators appear limited.
- **Materiality readiness**: While materiality is assessed later in the incident lifecycle, preparation starts much earlier. Security, legal, finance, and compliance should agree in advance on who participates in materiality decisions, what criteria will be considered, and how those decisions will be documented.

This preparation work is not about predicting every scenario. It is about ensuring that when a privacy risk emerges, the organization knows who decides, who is consulted, and how fast escalation occurs.

Recognizing when a security incident becomes a privacy incident

Not every security incident with data exposure automatically becomes a privacy incident. The security team needs clear triggers that indicate when legal and privacy should be engaged. These triggers are escalation points, not legal determinations. *Table 5.3* highlights some of the most common conditions that warrant further review:

Privacy Trigger	What to Look For
Regulated or sensitive data	Exposure of regulated data such as **personally identifiable information (PII)**, financial records, or **protected health information (PHI)**, even if only a single record is affected, may trigger certain privacy laws or sector-specific regulations, such as GDPR or CCPA.
Customer-facing systems	Incidents affecting systems that customers interact with directly or rely on for services.

Privacy Trigger	What to Look For
SOX-in-scope systems	Incidents impacting systems that support financial reporting or internal controls (e.g., systems used to generate revenue reports or financial statements under **Sarbanes-Oxley Act (SOX)**).
Cross-border data exposure	Data subject to multiple jurisdictions or international data transfer rules.
Contractual notification clauses	Customer or partner agreements that mandate notification independent of regulatory thresholds.
Timing sensitivity	Incidents occurring during earnings periods, mergers and acquisitions, or major contract negotiations.

Table 5.3 – Common triggers for privacy incident escalation

Tip

When in doubt, consult. Over time, you will build the necessary experience to get more comfortable with this situation and make better judgment calls regarding privacy triggers. Do not attempt to take the responsibility upon yourself as shared decisions reduce personal risk and lead to better outcomes.

Once one of these triggers is present, the response begins to change. Security still drives the facts and technical analysis, while legal, privacy, compliance, and business leaders become essential to the decisions that follow.

Shifting responsibilities from technical response

When a security incident crosses the threshold and becomes a privacy risk, the nature of the response needs to change quickly. What was once a contained technical investigation now carries implications that extend well beyond the security team.

This does not mean security steps back; it means the role changes. The security leader shifts from sole decision-maker to strategic advisor, providing technical context while legal, privacy, and business leaders weigh broader implications. *Table 5.4* highlights what changes once legal and privacy considerations are introduced and how your response adjusts accordingly:

What Changes	Why It Matters	What to Do Differently
The audience expands	Legal, privacy, compliance, communications, and business leaders may need to be involved, increasing coordination complexity	Define escalation paths in advance and include the right cross-functional leaders early.
Disclosure obligations may be triggered	Regulatory notification timelines and contractual commitments may apply, often with strict deadlines	Engage legal and privacy to interpret obligations before committing to disclosures or timelines.
Decision-making moves beyond security	Materiality, disclosure, and external communications should not be owned by the security executive alone	Explicitly share decision authority across security, legal, privacy, and business leadership.
Documentation takes on new meaning	Emails, notes, and timelines may later be reviewed by regulators, auditors, or counsel	Be deliberate about written communications and follow legal guidance on what and how to document.
External scrutiny becomes more likely	Customers, partners, regulators, or investors may ultimately learn about the incident	Coordinate messaging through legal and communications to ensure accuracy and consistency.

Table 5.4 – Key responsibility shifts during privacy incidents

Tip

The key shift is organizational. Security still drives facts and analysis, but decisions are now shaped by legal risk, contractual exposure, and business context. Recognizing this transition early helps avoid missteps that are difficult to undo later.

Once legal and privacy considerations enter the response, how information is handled matters as much as the investigation itself. The next section explains why privilege is important and how security leaders can help preserve it during an incident.

Establishing attorney-client privilege

Establishing **attorney-client privilege (ACP)** means engaging legal counsel early so that certain communications, analyses, and deliberations are protected from disclosure. When privilege applies, discussions conducted for the purpose of seeking legal advice are generally shielded from regulators, litigants, and other external parties.

> **Tip**
>
> Early engagement with legal helps clarify escalation decisions and establish shared accountability across the appropriate stakeholders.

Privilege does not apply automatically, and its application depends on the circumstances and governing law. From a security leader's perspective, three operational practices can support counsel's efforts to establish and preserve it:

- **Timing**: Engage legal before key decisions are finalized or preliminary conclusions are shared. Early involvement allows counsel to frame the legal questions and guide how sensitive analysis is handled. Bringing legal in later does not retroactively protect earlier communications.
- **Intent**: Make clear when a communication is intended to seek or provide legal advice. Routine technical or business discussions do not become privileged simply because an attorney is copied or the communication is labeled "privileged."
- **Structure**: Follow counsel's direction regarding who participates, where sensitive discussions occur, and how outside parties are engaged. For example, legal should help determine how a forensic firm is retained and how its work is directed. Broad distribution or informal sharing may undermine confidentiality and weaken a claim of privilege.

Late engagement can leave earlier work unprotected. For example, if the team has already shared preliminary conclusions by email, documented sensitive analysis informally, or engaged a forensic firm directly through security or IT, some of that work may not be protected under privilege.

For a new security leader, involving legal and other stakeholders can initially feel as though it dilutes your authority, particularly when they challenge your recommendation. In reality, decisions involving materiality, disclosure, or legal exposure should not rest on security alone. Your role is to provide the security facts they need. This creates shared accountability and reduces the likelihood that responsibility is later placed on one executive for a decision the organization should have owned collectively.

Common pitfalls that undermine privilege

Even with legal involvement, privilege can be weakened or completely lost through small, well-intentioned missteps. *Table 5.5* highlights frequent pitfalls and how to avoid them:

Common Pitfall	Why It Creates Risk	What to Do Instead
Using informal communication channels	Messages in instant messaging tools (Slack, Teams) or texts may be forwarded or misinterpreted	Keep sensitive discussions in counsel-directed forums. Be intentional about written communication; emails, notes, and chat messages may later be scrutinized.
Blending legal analysis with operational updates	Dilutes intent and weakens privilege claims	Separate legal deliberation from status reporting.
Over-distributing privileged materials	Broad access undermines legal protection	Limit distribution and only bring a limited number of people under the tent.
Documenting speculation or early conclusions	Preliminary judgments may later be read as facts	Stick to verified facts; let legal guide conclusions. Avoid restating privileged conclusions in non-privileged forums.
Engaging third parties incorrectly	Work may be treated as ordinary business records	Engage firms only through legal when privilege is required.
Assuming privilege applies automatically	Copying legal counsel on a communication does not guarantee protection	Confirm intent, structure, and scope with counsel.

Table 5.5 – Common pitfalls that can weaken privilege

One of the most common mistakes is assuming that others know what ACP means. As a best practice, meetings held under privilege should begin with counsel explicitly stating that the discussion is covered by ACP, especially when new participants join. This reinforces intent and helps preserve protection as teams expand. If they do not take this step, you should ask them to cover the key points above regarding participation, written communication, and documentation.

Case study: when the forensic report was not protected

A large financial services company experienced a major data breach, and affected individuals filed lawsuits after the incident became public. Before the breach, the security team had directly retained a forensic firm to provide routine incident-response services.

After the breach, outside counsel directed the same firm to investigate the incident and prepare a report. However, the work closely resembled the services the firm was already expected to provide under its existing agreement. The report was also shared with business and technical stakeholders who needed the findings for operational and regulatory purposes. As a result, the investigation looked less like a separate legal engagement and more like the company's normal response to a security incident.

During the litigation, the affected individuals requested access to the report. The company argued that it should be protected from disclosure because counsel had directed the investigation. The court disagreed, concluding that the company likely would have produced a similar report even without the lawsuits. The company was therefore required to turn it over.

The lesson here is not about the firm involved but **how** it was engaged. An existing forensic firm can support the technical response, but a separate legal analysis may need to be structured differently. When an incident could lead to litigation or regulatory action, involve legal before assigning the work and allow counsel to determine how the engagement should be structured. As the security executive, you do not need to interpret privilege yourself. You need to recognize when to pause and bring legal into the decision.

Knowing when to escalate further

Not every privacy incident requires outside counsel or external support, but some do. Many incidents could initially be handled in close partnership with internal legal counsel, who understand the business, contractual commitments, regulatory landscape, and the organization's risk tolerance. Internal legal teams are best positioned to guide early response, establish privilege, and coordinate across privacy, compliance, communications, and leadership.

As a privacy incident grows in scope, impact, or visibility, the nature of the support required often changes, requiring further assistance. External firms bring specialized experience when dealing with large-scale/high-impact incidents, regulator interactions, and litigation across multiple organizations. In certain jurisdictions or scenarios, they may also provide clearer privilege boundaries or additional credibility with regulators and auditors.

Here are some of the best tips for navigating this situation from our experience:

- **If counsel recommends engaging an external forensic or incident response firm, view that recommendation as a sign of sound judgment, not as a reflection of security failure**. Independent validation is often seen positively by auditors and regulators, signaling that the organization is taking the incident seriously and seeking objective verification. It is natural to feel defensive in these moments, but this is not about questioning your team's competence—it's about matching the response to the risk.
- **Recognize when you and your team need help.** Incident response is physically and mentally draining. The stakes are high, the hours are long, and fatigue accumulates quickly. After a day, people are tired. After two days, mistakes begin to surface. After three days, burnout and poor judgment become real risks. This is not the moment for a hero mentality. If help is offered (legal, forensic, communications, or operational), take it. You can always decide later how best to use that support. Preserving clarity, judgment, and resilience is far more important than proving you can handle everything alone.

The decision to engage outside counsel or external support is typically made by internal legal, in partnership with security and other stakeholders. Your role as a security executive is to recognize when complexity or visibility is increasing and to raise the question early, before options narrow and risks compound.

Escalation brings the right people into the response, but it does not answer every question. As the facts develop, leaders still need to determine how significant the incident is to the organization and whether it may require broader disclosure. That is where materiality comes in.

Assessing materiality

Materiality is one of the most important determinations made during a security incident and one of the easiest to misunderstand. At its core, materiality asks a simple question: *would this incident matter to someone making decisions about the company?*

The answer shapes disclosure obligations, financial reporting, leadership escalation, and how the incident will be judged over time, often long after the technical response is complete.

For public companies, this determination can affect what the organization must disclose to the market. For instance, a material cybersecurity incident may need to be reported through a Form 8-K, which is used to disclose significant events outside the normal quarterly reporting cycle. The incident may also appear later in a Form 10-Q, the company's quarterly report, if it creates ongoing financial, operational, legal, or risk implications. In practice, this means materiality is the bridge between what the security team learns during an investigation and what the company may need to tell investors, regulators, customers, or other stakeholders.

Tip

For security professionals, it can help to think about materiality the same way you think about incident severity or exploitability. In security, you do not assess risk based on a single signal. You look at multiple factors: impact, likelihood, exposure, and context. Materiality works the same way; it is not a binary test, and it is not based on one data point.

Considering when and how to notify executive leadership and the board

Material incidents require timely escalation. The goal is early awareness with context, not premature conclusions, and not waiting for perfect answers or a final materiality determination.

Do not wait until the materiality assessment is fully concluded before raising potential concerns with your direct line of leadership. Early visibility allows company officers to prepare for decisions that may need to be made quickly, even as facts are still developing.

The C-suite should be informed as soon as an incident is reasonably suspected to be material or when it has the potential to impact financial reporting, regulatory posture, or public trust. Updates are often best delivered verbally, in close coordination with legal, to avoid premature conclusions or unnecessary written records.

The board should be notified once materiality is reasonably established or when the incident presents a significant risk to the company's strategy, financial position, or reputation. The board should never be notified before executive leadership has been informed and aligned. Boards expect a structured assessment, not raw technical detail, and rely on management to bring context, options, and recommendations.

In both cases, notifications should be coordinated with legal and communications teams to ensure accuracy and consistency. Security leaders should focus on providing facts and next steps, while avoiding speculation or definitive conclusions before the assessment is complete.

Case study: when materiality is reassessed after the fact

A public software company experienced a ransomware incident involving systems that stored customer-related data. Early in the response, the company assessed the incident based on the information available at the time and communicated externally that certain sensitive data had not been accessed.

As the investigation continued, technical and customer-facing teams learned additional facts that changed the risk picture. The attacker had accessed and removed sensitive information that was more significant than the company's earlier statements suggested. Yet these facts were not escalated effectively to the people responsible for disclosure decisions.

As a result, later public filings and customer communications did not fully reflect what the company knew internally. The materiality assessment was not revisited in a structured way, and the decision-making process did not clearly show who considered the updated facts, what criteria were applied, or how the company reached its conclusion.

Years later, regulators reviewed the incident and concluded that the company's disclosures were misleading because they did not reflect the full impact of the event. The enforcement action focused less on whether the company made a perfect call in the first hours of the incident and more on whether it had a process to reassess materiality as new facts became available.

At the end of the day, materiality decisions are judged with hindsight and defended with governance. A documented process shared by multiple stakeholders matters more than a perfect call.

> **Note**
>
> Security provides facts, scope, and risk context but should not own the decision alone.

Making the call without owning the risk alone

Materiality should always be assessed by a **cross-functional group**, typically involving legal, finance, compliance, and cybersecurity. The group meets to discuss various aspects of the incident, using previously agreed-upon criteria. Once a recommendation is made, legal factually documents it, sometimes with the help of outside counsel, to include some of the following data points:

- Who participated in the decision
- What facts were known at the time

- Which factors were considered
- The rationale for the conclusion

The recommendation will be shared with executive leadership, such as the **Chief Legal Officer (CLO)**, the **Chief Financial Officer (CFO),** and other designated executives, to make the final decision as to whether the matter is material to the company.

Once a materiality determination is made, additional steps may follow, including disclosure planning, regulatory coordination, investor communications, customer notifications, and board engagement. Those activities are led by legal, finance, communications, compliance, or investor relations, and they fall outside the normal scope of the cyber team.

Your role may still be important, especially if leaders need factual updates, technical timelines, impact analysis, or confirmation of remediation progress. The key is to stay engaged as a source of objective information without taking ownership of decisions that belong elsewhere.

Incidents are high-pressure situations that reveal the technical gaps, the strengths, and the limitations of your team. They test decision-making, communication, resilience, and, most importantly, the people responsible for leading the response. While budgets, contracts, and legal processes help prepare the organization, it is your team that ultimately determines how effectively those plans are executed. Building and sustaining that team is one of your most important responsibilities as a security executive.

Building a high-performing team

Now let's focus on the practical leadership choices that shape your team's effectiveness and longevity. We will explore how to design a sustainable structure that supports your goals and how to invest in your talent.

People are by far the most important factor that will impact your success. Over the years, we have seen how small teams with limited budget and a determined approach can transform a security program end to end. This is crucial now more than ever, with the rise in AI capabilities.

In *Chapter 2*, we introduced the Team Assessment Tool as a starting point for understanding your organization. That assessment should continue as you observe how the team works and performs over time. By now, you should have a clearer view of your team's strengths and development opportunities, along with how they affect day-to-day execution.

With that baseline in place, you are ready to take the assessment to a deeper level. Start by looking at the organization you inherited:

- **Assess whether the structure reflects how work actually gets done.** Misalignment often shows up as friction, delayed decisions, or unclear ownership rather than obvious failures. For example, security architecture may sit under one leader, while other teams

have their own security architects, such as AI and IAM. If these groups are not aligned to a common security architecture model, teams may receive inconsistent guidance or make design decisions that conflict with one another.

- **Look for signs that critical work depends on too few people.** When work falls behind or the same individuals are pulled into every escalation, diagnose the source of the strain before assuming the answer is headcount. For example, if one senior leader or architect is repeatedly needed to support incidents and unblock delivery teams, the issue may be an operating model that relies too heavily on a few trusted people.

Once the structure looks right to you, shift your attention from today's gaps to what comes next.

Review your open roles and evaluate if they are still aligned with your roadmap and where the business is headed. This is also the right time to look inward. Internal mobility can be one of the fastest and most effective ways to close gaps, especially when you have strong performers ready for more responsibility. Promoting or rotating talent signals that growth is possible without leaving the team.

Finally, pressure-test your people strategy against how the company actually operates. Location strategy matters more than many leaders expect. If the organization is moving toward in-office or hybrid work, hiring fully remote talent without alignment can create friction later.

Hiring with intention

Hiring is one of the most visible signals of your leadership. The decision you make here signals your judgment and priorities to the team. It is also one of the easiest places to make mistakes. As your role shifts from manager to executive, hiring is no longer about staffing but rather a core leadership capability.

Effective hiring requires more than opening a requisition and waiting for candidates to appear. It requires clear alignment with recruiting, active involvement throughout the interview process, and disciplined judgment before making the final decision.

Setting expectations with recruitment

Even if you have not done so in the past, working closely with your recruiting partner is a must. That intake call they have been trying to schedule is critical. We strongly recommend you take the time to talk to them about what you are looking for so they can see beyond the hundreds of resumes in front of them.

In many cases, what you need may be very different than what they had in mind. Many leaders assume recruiters understand security acronyms and the qualities needed to succeed in a role. For example, if you are hiring a Head of Incident Management, the recruiter may prioritize

candidates with extensive SOC experience. However, your highest priority may actually be someone who has led large-scale incident response, built strong executive communication skills, and can remain calm under pressure during a crisis. Those nuances are not always obvious unless you explain them.

Be explicit about trade-offs you are willing to make. The more clarity you provide upfront, the faster and more accurately recruiters can filter signal from noise. *Table 5.6* provides an overview of questions you should be ready to answer when initiating the hiring process:

Area	What to Clarify	Why It Matters
Competencies	Skills that are must-haves versus nice-to-haves; be explicit about what you are willing to compromise on, especially for senior roles.	The more senior the role, the harder it is to hire for everything. Clarity here reduces stalled searches and unrealistic expectations.
Background	Years of experience, types of roles the candidate fulfilled (hands-on execution vs. oversight), and how long they've stayed in each position.	Avoids overvaluing tenure without understanding depth, ownership, and relevance to your needs. Also, frequent moves can be a risk signal for some leaders.
Scale of Prior Organizations	The size, maturity, and pace of the environments they have worked in and whether they can adapt to yours.	Candidates from large enterprises may struggle in smaller organizations where everyone has to lean in; the reverse can also be true.
Sector Experience	Whether specialized experience is required, such as in highly regulated environments, or whether a strong generalist can succeed.	Sector familiarity can reduce ramp time and regulatory risk, but it can also narrow the talent pool.
Change Tolerance	Experience operating through transformation, growth, or disruption and how the candidate responds when priorities shift.	Many hires fail not because of skill gaps but because the environment changes faster than they expect.

Area	What to Clarify	Why It Matters
Qualities That Matter Most	Traits critical for success in your environment, such as adaptability, building consensus, operating under pressure, or influencing without authority.	These qualities often determine long-term success after technical skills become table stakes.

Table 5.6 – Potential alignment areas with recruiting

Pipeline-building is also part of this partnership. Share LinkedIn profiles of people you believe would be a good fit. Review resumes together and explain what you liked or did not like about specific candidates. This may feel like extra work at first, but it saves time in the long run. Recruiters who understand how you think are far more likely to present candidates who are aligned.

Tip

Many leaders resist this level of involvement early on, assuming it is not their job. The reality is that investing upfront reduces rework later.

As part of setting expectations, deliberately build a diverse interview panel. Especially in cybersecurity, it can be valuable to include interviewers outside your immediate domain, such as engineering, product, risk, or legal. This helps you see candidates through different lenses, pressure-test how they communicate beyond security, and build early consensus across stakeholders who will eventually work with them.

Staying personally engaged in the interview process

In most corporate environments, recruiting is a shared service, and the role you are hiring for is one of many competing priorities. You will not get special treatment because the role sits in cybersecurity, so if you need to move fast, we recommend that you stay very engaged (even on a daily basis) to unblock decisions and provide feedback. This approach has worked magic in my experience with thousands of candidates.

Note

Proactive engagement changes the dynamic with your recruiter. Many recruiters complain about the level of engagement they get from hiring managers, as they feel like they need to chase them to get their attention. By regularly reaching out to your recruiter, you are signaling to them that you are engaged and eager to get the position filled. Over time, recruiters who know how you think will bring you stronger candidates with less noise.

Even when you are not the formal hiring manager, your involvement still matters. For roles above a certain level, such as principal level, or positions that will greatly influence how the team operates, such as head of security operations, you should be a part of the interview loop. Your role here is less about evaluating technical depth and more about assessing alignment: how candidates think, how they handle ambiguity, and how they show up with others. You can teach technical skills. You can close experience gaps. People skills, humility, and grit are far harder to correct later.

Tip

Be explicit with your team and recruiting partners about where you expect to be involved and what role you will play in the process. Above a certain level, it is reasonable for you to be the final interviewer. In rare cases, you may need to exercise veto authority when something feels misaligned with the culture or leadership standards you are setting.

Recruiters and HR partners also play a critical role at this stage. They interact with hundreds of candidates and see patterns others may miss. Red flags are rarely raised casually. If your recruiter expresses concern, take it seriously. Also, if your HR partner does not approve of a candidate, pause. It typically takes something major for them to make that call. Overriding it often introduces downstream risk that could show up later, in performance, conduct, or team dynamics.

Interviews show how candidates present themselves; they do not always reveal how people behave when pressure is real or when incentives change. This is where external signals and experienced judgment matter most, and where the final decision is often made.

Using references as final signals

Reference checks are where experienced leaders slow down rather than speed up. Even if a recruiter does not offer them to you, you should ask for references. Remember that candidates choose who speaks on their behalf. Your role goes beyond confirming strengths (that is the easy part) to probing areas of concern.

Table 5.7 provides sample questions for your consideration. You do not need to ask all of them, of course. Pick a few and listen carefully to *how* people answer.

Focus Area	**Sample Questions**	**What You're Listening For**
Role and context	How did you work with this person, and in what capacity? What kind of environment were you operating in (scale, pace, pressure)?	Context that helps you interpret answers; relevance to your environment
Judgment and decision-making	Can you share an example of a difficult decision they made with incomplete information? How did they balance speed, risk, and quality?	Ability to make trade-offs, not just follow process
Operating under pressure	How did they show up during high-pressure situations or incidents? What happens when plans change unexpectedly?	Composure, prioritization, and adaptability
Collaboration and influence	How effective were they at building alignment across teams? How did they handle disagreement or pushback?	Maturity, influence without authority, respect for others

Focus Area	Sample Questions	What You're Listening For
Leadership and culture	How would you describe their leadership style? How did they treat people who were junior or outside their direct team?	Signals about humility, empathy, and cultural fit
Growth and self-awareness	What feedback did they struggle with most? Where did you see them grow—and where did you not?	Coachability and self-awareness
Overall recommendation	Would you hire or work with this person again? Why or why not? What should I be most mindful of if they join my team?	Unfiltered insight; hesitation or caveats often matter most

Table 5.7 – Reference check questions for leadership hiring

Lastly, references are external signals. They complement, but do not replace your judgment. We cannot emphasize this enough: *trust your instincts*. If something does not feel right, despite strong interviews and positive referrals, pause. Slowing down here is often the difference between a hire that looks good on paper and one that succeeds in practice.

Hiring is not the finish line; it is the beginning of a much longer leadership responsibility. The best candidates will only reach their potential if they continue to learn, grow, and feel supported after they join the team. Developing talent is what transforms a hire into a long-term contributor and your next generation of leaders.

Investing in your talent

In *Chapter 2*, we talked about recognition and how acknowledging efforts builds trust and reinforces the behaviors you want to see more of. Recognition is only one part of the equation. Sustained performance comes from investment: in skills, confidence, exposure, and a sense that people are growing as individuals and as a team.

Investing in your talent does not require large programs or unlimited budgets. It begins with an authentic intention for people to grow.

A practical way to think about talent investment is through three reinforcing areas: training, coaching, and appreciation, as illustrated in *Figure 5.2*:



Figure 5.2 – Strategies for talent investment

If your best people are learning, growing, and being genuinely recognized, retention often takes care of itself. If they are not, or if recognition feels inauthentic, no amount of compensation will fix it.

Using training strategically

Training is often the first lever leaders reach for. It is most effective when treated as a capability-building decision rather than a default reward or one-off perk.

When funding is available, prioritize opportunities that either broaden perspective or deepen skills. Conferences, formal courses, and certifications can be valuable, but you will rarely be able to offer them to everyone. Create a plan that maps available opportunities to the people who would benefit most.

For example, your organization may receive a limited number of passes to several industry conferences through existing memberships or vendor relationships. Because those opportunities are predictable, decide in advance who should attend and how that learning will be shared with the broader team. This often requires difficult prioritization, especially when more people would benefit than the budget allows.

When funding is limited, or when the allocated training budget has already been used, creativity becomes important. Vendor-led training, local security meetups, and online learning platforms can still provide meaningful development at little or no cost.

For example, you can ask one of your strategic vendors to host a half-day session for your team on a relevant topic, such as cloud security, AI, or incident response. Many industry training providers also offer free virtual conferences or remote sessions that provide strong value without requiring travel or registration fees.

Regardless of which option you choose, look for ways to extend the value beyond those who attend. Ask participants to share what they learned through a short readout or team discussion. This allows the broader team to benefit and makes learning part of how the team works, rather than a personal perk.

Coaching at scale

Coaching is one of the most meaningful investments you can make in your team, but it requires selectivity. Your time is limited, and not every development need requires the same level of personal involvement. The goal is to decide where your direct coaching will have the greatest impact and where other formats can help extend your reach.

One-on-one coaching gives you the opportunity to work deeply with individuals. The trade-off is capacity. You can realistically do this well for only one or two people at a time, so be intentional about who receives that level of personal investment from you. This may include high-potential leaders, individuals stepping into larger roles, or team members navigating moments where focused guidance could change their trajectory.

It is also important to recognize the limits of your own role. Even if you have received coaching from a professional coach, that does not make you one. Partner with HR or talent development teams to understand the tools, frameworks, and resources available to help you coach more effectively. Coaching may feel natural to some leaders, and it can become one of the most rewarding parts of the job, but it still requires practice and humility.

Group coaching can extend your reach. Structured sessions, such as skill-specific workshops, presentation practice, or studying together for a certification, create shared coaching moments. These sessions also help normalize vulnerability and growth, especially for early-career professionals or underrepresented groups that may benefit from stronger peer support.

For example, you might hold a quarterly session for women in cybersecurity, creating a safe space to discuss topics such as career growth, confidence, or navigating difficult conversations. The value is not only in the content; it is in creating a consistent forum where people can learn from one another, form relationships, and see that their experiences are not isolated.

Shadowing sits somewhere between individual and group development. Inviting someone to observe a meeting, a board preparation session, or a difficult stakeholder conversation exposes them to how decisions are made without requiring the same time commitment as formal coaching. Shadowing is often overlooked, but it is one of the lowest-effort, highest-impact ways to help people grow. It gives emerging leaders access to context they would not otherwise see and helps them understand how executive judgment is applied in real situations.

Making appreciation visible

Appreciation is another way leaders invest in their teams. Monetary recognition matters, whether through bonuses, spot awards, or other formal programs, but those options vary widely by organization and are not always within your direct control. This section focuses on practical ways to show appreciation regardless of budget: small, consistent gestures that reinforce that people's effort and impact are seen.

Handwritten notes are one example. Sending a few each month may feel awkward or time-consuming at first, but it becomes a rhythm. In a digital-first world, a handwritten note stands out and signals that a real person noticed someone's contribution, rather than it being acknowledged only through a system or standard message.

If handwritten notes are not your style, use a thoughtful email or message instead. The format matters less than the specificity. A generic "great job" is easy to overlook. A short note that explains what they did and how it helped the team is far more meaningful.

Small tokens of appreciation can also help reinforce identity and pride, such as challenge coins, shirts, or stickers. One team tradition that worked exceptionally well was anniversary shirts. What started as a simple gesture turned into a point of pride, with team members wearing them around the office long after they were issued.

Regardless of what option you choose, the most important point is consistency. Appreciation should not appear only after major incidents, difficult projects, or moments of visible heroics. It should be part of how you lead day to day. Investing in talent is not a single program or initiative, but rather a pattern of behavior. When people see that you are willing to invest time, attention, and thought into their growth and contributions, they are far more likely to invest their energy back into the program.

Notes from the field with Renana

Case study: expanding the security-only lens

Throughout this chapter, we have explored the decisions that move security leadership beyond technology: budget, procurement, legal, and people. None of these disciplines exist in isolation. The most effective security executives learn to evaluate decisions through multiple business lenses, balancing risk with financial, legal, operational, and organizational considerations.

I did not always think that way. Many of the lessons in this chapter were learned the hard way through experiences and mistakes that forced me to rethink how I showed up as a leader.

Early in my career, I approached most challenges through a single lens: cybersecurity. My intentions were good, but my perspective was limited. I focused on technical risk without fully understanding the implications of my decisions. That narrow view made me less effective than I could have been.

Looking at problems through only one dimension led to avoidable missteps. I did not always partner closely enough with procurement, assuming urgency could override the process. I delayed bringing legal into sensitive situations instead of sharing accountability early. I underestimated how much involvement hiring and HR decisions required from me. These were not failures of effort; they were failures of perspective.

Over time, I learned that executive leadership requires operating through multiple lenses at once. Some of these lessons were uncomfortable. A few were humbling. But each one reshaped how I think about leadership. After each major lesson, I made a deliberate effort to reflect, ask better questions, and seek feedback. Growth did not come from getting everything right. It came from treating each experience, big or small, as an opportunity to sharpen judgment.

As my career progressed, the nature of the challenges changed. Early on, I focused on mastering technical craft, including malware analysis, investigations, and incident response. Later, success depended less on technical depth and more on influence, decision-making under ambiguity, and balancing competing priorities. Each stage required broader thinking, stronger partnerships, and a deeper understanding of how the business actually operates.

One of the most important mindset shifts was moving beyond the security-first lens to a business-first lens. It is easy to frame decisions as "security versus the business." In reality, we share the same mission: protecting the organization's ability to operate and grow. The more I invested in understanding how other executives see the world, the more effective I became, not just as a security leader, but as a business partner.

Real impact comes from perspective that goes beyond just domain expertise. Apply multiple lenses. Build humility. Seek input beyond your domain. Put in the work to understand how others think and operate. That is how you move from being technically strong to being organizationally effective, and how hard-earned experience turns into sound judgment.

Summary

In this chapter, we focused on practical leadership decisions that most leaders encounter through their first year and beyond. We explored how to navigate budget, procurement, legal, privacy, and talent considerations, expanding beyond a security-only lens.

Execution depends on more than a strong roadmap. Funding decisions determine what can move forward. Contracts shape vendor accountability and flexibility. Legal alignment affects the way privacy incidents are managed. Talent decisions determine whether the organization has a team that can operate effectively during steady-state conditions and under pressure. While these areas may sit outside the traditional technical comfort zone, they directly influence your long-term success.

Across each of these areas, your role is not to become the finance, procurement, legal, privacy, or HR expert. It is to stay at the right executive altitude, bringing the security perspective while relying on your partners' expertise. Some decisions require shared ownership across the appropriate stakeholders. Your responsibility is to remain engaged without assuming sole ownership of decisions that belong to a cross-functional group.

In the next chapter, we will shift from enablement into specific domains, focusing on how to operationalize defense through strong core security functions. We will cover approaches to maturing incident response, vulnerability management, threat intelligence, SOC operations, and security architecture to help you assess readiness, prioritize improvements, and build a resilient, scalable operating model.

Chapter checklist

- Establish a regular budget review cadence with the finance department and define your *Financial Credibility Metrics*.
- Build minimum viable, recommended, and accelerated funding options using the budget request template.
- Review priority vendor contracts and applicable procurement levers with procurement and legal.
- Confirm privacy incident escalation paths and decision ownership for privilege and materiality with legal, privacy, and finance.
- Align your team structure, hiring priorities, and talent investments with the roadmap.

Additional resources

- IANS + Artico Security Budget Benchmark Report: `https://www.iansresearch.com/resources/ians-security-budget-benchmark-report`

6

Operationalizing Defense: Core Security Functions

The first year of your cybersecurity leadership journey reaches a turning point when strategy turns into execution. By now, you have assessed the landscape, built relationships, defined your vision, and secured the resources needed to act. The next step is to operationalize.

In this phase, you are building the operational backbone that will sustain your security program. The systems, processes, and people you put in place will determine how effectively your organization can detect, respond to, and recover from threats. The goal is to ensure that every defensive function operates as part of a coordinated and repeatable ecosystem that serves the business.

This chapter will help you build that operational foundation. We are going to cover the following key steps:

- Building the operational backbone of a security program
- Building incident response excellence
- Proactive vulnerability and exposure management
- Integrating threat intelligence into decision-making
- Maturing the SOC: People, processes, and technology
- Security architecture as a strategic enabler

Building the operational backbone of a security program

Establishing the operational backbone of a cybersecurity program is one of the most critical milestones in a security executive's first year because while strategy and planning set the direction, operations bring that strategy to life. Without a strong operational foundation, even the most well-crafted security strategies can fail to deliver measurable results or sustain long-term resilience.

Security operations are often one of the most underestimated parts of a security program. That is largely because people expect the operations team to step in and keep things under control when something goes wrong. A missed patch, a misconfigured system, a delayed decision, or a control that was pushed aside can quickly become their problem. One mistake anywhere in the organization can turn into an operational crisis almost overnight.

The backbone of a security program is defined by its ability to execute with precision and predictability.

- **Integrated incident response**: Integration of incident response (which can be part of security operations or not), vulnerability management, threat intelligence, and posture management under a unified governance model. The goal of this integration is to move from ad hoc or reactive activities to a structured and proactive approach where each function feeds into the other.
- **Constant checks for effectiveness**: The cybersecurity leadership role is to ensure these interdependencies are well defined, aligned with business priorities, and continuously measured for effectiveness. Operational excellence in cybersecurity is achieved when protection, detection, and response activities operate cohesively and with clear accountability.
- **Consistent workflow:** Organizations with a higher maturity level develop documented processes, standard operating procedures, and escalation workflows that ensure consistency even under pressure. But a strong operational backbone is not only about that; it is also about culture and discipline.
- **Readiness**: Security operations teams should be trained to respond to incidents with agility but guided by pre-approved playbooks that reduce decision fatigue and human error.
- **Automation and orchestration**: Automation and orchestration technologies can further enhance efficiency by removing manual steps, accelerating response times, and providing executives with real-time visibility into the organization's security posture.

Now let's take a look at how to define and measure your objective and key results.

Defining your objectives and key results

To measure your security program's success, define its **objectives and key results (OKRs)**. This goal-setting framework aligns teams and organizations around clear, measurable outcomes. This framework is comprised of two elements:

- Objective: What do you want to achieve?
  - The objective should be ambitious and qualitative.
- **Key results (KRs)**: How will you know you achieved the objective?
  - The KRs should be specific, measurable, time-bound, and focused on the outcome.

Tip

While the OKR Framework was created in the 1970s by Andy Grove, Intel's former CEO, it was Google that made OKRs a popular framework in 1999, when John Doerr, a former Intel employee, introduced OKRs to Google. The adoption of OKRs at Google proved that this framework helps with data-driven execution and alignment at scale. Nowadays, OKRs have become part of modern tech culture.

Your security program should have a goal, an objective to achieve. This objective will likely change over time, but this is where OKRs work even better, because it will be time-bound. Let's say that your security program objective for the first quarter of the year is to *significantly improve the organization's security posture and readiness to prevent, detect, and respond to cyber threats*. Notice that the objective is intentionally high-level and outcome oriented. Now let's define KRs that make it measurable.

- **KRs – security posture improvement**
  These KRs will help to measure exposure management effectiveness, preventive control maturity, security hygiene at scale, alignment with "shift-left," and proactive security.
  - Reduce critical and high-risk security exposures by 40% across cloud, endpoint, identity, and network assets.
  - Achieve ≥95% compliance with the organization's defined security baseline.
  - Increase asset visibility to 100% for production systems.
  - Reduce mean time to remediate critical vulnerabilities by 30%.

Now let's go to the second set of KRs, this time to measure incident response improvement.

- **KRs – incident response improvement**
  These KRs will help to measure **security operations center (SOC)** effectiveness, quality of detection and alerting, operational readiness, and overall continuous improvement.
    - Reduce **mean time to detect (MTTD)** security incidents by 35%.
    - Reduce **mean time to respond (MTTR)** to high-severity incidents by 30%.
    - Achieve 90% incident playbook coverage for top attack scenarios.
    - Conduct at least two incident response tabletop exercises per quarter, with documented lessons learned and action items.
    - Reduce repeat incidents caused by the same root cause by 50%.

Traditional security metrics often focus on activity (number of alerts, scans, tools deployed). OKRs force a shift toward outcomes, such as:

- Less exposure, not more tools
- Faster response, not more alerts
- Fewer repeat incidents, not just incident closure

Integration across business units

A robust operational backbone also demands integration across business units and IT functions. Security cannot operate in isolation; instead, it must be embedded into business processes, product development cycles, and technology operations. Collaboration between the SOC, IT operations, and application teams is essential to ensure that vulnerabilities are remediated swiftly and that incidents are contained without disrupting business continuity.

This alignment transforms cybersecurity from a technical function into an operational enabler, which supports innovation, regulatory compliance, and overall customer trust.

For new cybersecurity executives, building the operational backbone involves prioritizing foundational capabilities that can deliver visible impact in the first 180 days. This may include formalizing incident management procedures, implementing vulnerability prioritization processes, and introducing exposure management practices such as continuous attack surface monitoring.

Building incident response excellence

A well-designed **incident response (IR)** capability enables an organization to detect, contain, and recover from security incidents efficiently while minimizing business disruption, legal exposure, and reputational damage.

Consider the guidelines below when designing your IR capabilities:

- **Creating a culture of readiness**: For a cybersecurity executive, building and maturing incident response is not simply about producing procedures or technical playbooks; it is about establishing a culture of readiness. In this culture, leaders, technical teams, and business stakeholders clearly understand their roles when the inevitable occurs. When I say inevitable, I'm basically using the concept of Assume Breach, which is one of the pillars of Zero Trust. Incident response is as much of a governance and leadership discipline as it is an operational one.
- **Maintaining an incident response plan**: Every organization should maintain a clearly defined incident response plan that aligns its business objectives, regulatory obligations, and risk appetite. This plan should articulate how incidents are detected, escalated, and resolved, all while also addressing executive-level concerns such as personal liability, regulatory exposure, and fiduciary responsibility.
  The incident response plan must define incident categories, severity levels, communication paths, and reporting mechanisms. These definitions should not only address the needs of different security teams, but also the C-suite and board of directors. You must include clear guidance on when and how critical incidents are communicated, who provides ongoing updates, and how leadership maintains situational awareness throughout the lifecycle of an incident.
- **Defining the process of engagement with external parties**: As we discussed in *Chapter 5*, a mature incident response program also explicitly defines engagement with external parties, including outside legal counsel, digital forensics firms, and cyber insurance providers. These relationships cannot be improvised during a crisis. The plan must specify who initiates contact, under what conditions, and at what stage of an incident, ensuring legal privilege is preserved and insurance coverage requirements are met. This coordination is essential to reducing downstream legal and financial impact while enabling executives to make informed decisions under pressure.
- **Conducting regular drills**: It is imperative that incident response moves beyond documentation, because plans that exist only on paper routinely fail when tested by real-world events. Effective programs are operationalized through regular exercises, simulations, and executive-level tabletop scenarios that include legal, communications, and board engagement. These activities reinforce accountability and expose any gaps in decision-making and communication.
- **Establishing a cross-functional incident response team (IRT)**: Every member of the IRT should understand when to engage, what authority they hold, and how to escalate

issues. The security executive's role is to sponsor this structure, provide oversight, and ensure that communication during a crisis is both timely and accurate.

Maturing incident response capabilities

Maturing incident response capabilities requires evolution in how leaders show up during moments of crisis and how the organization prepares between incidents. This section explores two complementary dimensions of maturity: reactive and proactive. Together, these practices shift incident response into a predictable, trusted function.

Evolving your role during incidents (reactive)

As you step into an executive role, your responsibilities during an incident fundamentally change. While technical depth remains critical, you need to elevate your skillset to the next level. In moments of crisis, how you show up sets the tone for decision-making and trust at all levels of the company.

Show up as a company executive, not just a security leader. Your responsibility extends beyond technical leadership to representing the company as a whole. This may include helping draft or review customer communications or partnering with product teams to define interim mitigations. For example, if the organization experiences a significant security incident that affects customers, you may be asked to review public statements, participate in executive briefings, and explain the situation to key customers or regulators.

Operate across silos and mobilize the organization. Effective incident response requires rapid coordination beyond your immediate team. You should understand escalation paths, decision-makers, and informal networks across the company. This may involve asking for help from IT leaders to support log analysis or deploy a tool across the environment.

Serve as the calm voice in the room. Incidents create stress, urgency, and uncertainty. Your composure sets the tone for the response and keeps teams focused on resolution rather than blame. This may include redirecting conversations that dwell on faults and reframing them around next steps and decision points.

Maintain command of the facts and numbers. Incident data evolves quickly and can become confusing without disciplined tracking. You must understand how the analysis was conducted and maintain precise counts (such as how many employees were targeted in a phishing campaign, how many clicked, how many entered credentials, and how many accounts experienced unauthorized access). These figures will need to be communicated repeatedly to executives, boards, regulators, and potentially three-letter agencies.

Establishing incident response cadence (proactive)

A mature incident response program is defined not only by how it performs during a crisis, but also by what happens between incidents. Establishing regular incident response meetings and

review processes helps the team stay organized, reinforces accountability, and creates opportunities to learn from previous incidents. These regular activities ensure that lessons learned are translated into improvements, making the organization better prepared to respond to future incidents. *Table 6.1* outlines the activities by their cadence, activity, participants, and benefits.

Cadence	**Activity**	**Participants**	**Benefit**
Post major incident	Post-incident retrospective	Incident stakeholders	Captures lessons, drives blameless accountability, identifies root causes, and feeds actionable improvements into playbooks, tooling, and training.
Daily	Shift handoff report and review of tactical items requiring attention	SOC analysts, incident responders, on-call leads	Ensures continuity of operations across shifts, prevents loss of context, and reduces duplication or missed follow-ups. Creates a shared understanding of active incidents, emerging threats, and immediate priorities.
Weekly	Incident and metrics review	SOC leadership, incident response leads, threat intelligence	Identifies patterns, recurring issues, and operational gaps early. Enables course correction and prioritization of remediation work, and reinforces a data-driven operating model.
Monthly	Incident readout to stakeholders outside of security	Security leadership, IT, engineering, legal, privacy, risk, business partners	Brings stakeholders "under the tent," increases transparency, and strengthens cross-functional ownership. Helps non-security teams understand impacts, dependencies, and their role in prevention and response.

Cadence	Activity	Participants	Benefit
Quarterly	Incident trend analysis and thematic review	CISO, security leadership, risk and compliance leaders	Translates operational data into executive insight. Supports executive briefings and board discussions by focusing on trends, business impact, and risk posture rather than individual incidents.
	Quarterly threat intelligence review	SOC leadership, incident response leads, threat intelligence	Lets you review the top threat actors and notable campaigns impacting your industry.
Biannually	Incident response playbook review and update	Incident response leads, SOC leadership, cross-functional partners	Ensures playbooks remain aligned with the current threat landscape, technology stack, and organizational structure. Incorporates lessons learned from incidents and exercises into documented procedures.
At least annually	Meeting with the forensic retainer provider	SOC leadership	Lets you review any changes to engagement models and verify contact details are the same. If using a paid retainer, identify how to use funds prior to year-end.
Annually	Tabletop exercise/Live simulation	Security, IT, legal, communications, executive leadership	Validates readiness, tests decision-making and escalation paths, and identifies opportunities for improvement in both technical response and executive coordination.

Table 6.1 – IR cadence and activities

Together, these cadences transform incident response from a reactive function into a proactive system that continuously improves resiliency and execution.

Tip

You do not need to introduce every cadence at once to mature the program. If capacity or organizational readiness is limited, start with one technical cadence (such as a weekly metrics review or structured post-incident reviews) and one executive cadence (such as a monthly incident readout or an annual tabletop exercise). Establishing even a small number of consistent rhythms builds credibility.

Assessing the current IR plan

When you begin operating in your new role, you might work under the assumption that an incident response program already exists. However, you must verify that it truly works under pressure.

Start by reviewing the current incident response plan, playbooks, and escalation paths to understand how the organization believes it responds, then validate that reality by speaking directly with the people who would execute the plan, such as SOC analysts, IR leads, IT operations, legal, communications, and business stakeholders.

Ask simple but revealing questions: "*Have you used this plan recently? Do you know exactly what to do if an incident occurs? Who makes the hard decisions when impact is unclear?*" Look for gaps between documentation and lived experience, clarity of ownership, and confidence in decision-making. Pay particular attention to executive notification thresholds, legal and regulatory coordination, materiality assessment, and whether lessons learned are tracked to closure.

Before making sweeping changes, consider running or observing a tabletop exercise to see the plan in action. This approach allows you to respect what already exists, quickly identify strengths and blind spots, and build credibility, while ensuring the incident response capability is not just documented, but operational, defensible, and trusted.

Leverage industry standards

In case the organization does not have a well-established incident response plan, you may feel tempted to build one from scratch, focusing on what is important for your organization; however, you should not ignore good practices that have been shared over the years in the industry. For example, **NIST Special Publication 800-61 Rev. 2 – Computer Security Incident Handling Guide** is considered the de facto global standard for incident response. It is one of the most widely adopted incident response frameworks because it is technology-agnostic, flexible, and recognized by organizations across both the public and private sectors.

> **Note**
>
> This discussion and the accompanying examples use the incident response model in NIST SP 800-61 Revision 2. Revision 3 has since superseded it; readers should consult Revision 3 for the latest guidance.

It is an excellent choice for organizations that need to demonstrate a well-defined and defensible incident response process. Even if you choose to customize your incident response procedures, NIST SP 800-61 provides a solid foundation that can be adapted to your organization's size. The IR process focuses on the following phases:

- **Preparation**: Establish a foundation that enables the organization to respond effectively before an incident occurs.
- **Detection and analysis**: Identify potential security incidents and determine their scope, impact, and severity.
- **Containment, eradication and recovery**: Stop the attack, remove the threat, and restore normal business operations safely.
- **Post-incident activity**: Helps the team to learn from incidents and use these lessons learned to strengthen the organization's security posture to reduce the likelihood that another similar incident will occur.

Another option is **ISO/IEC 27035 – Incident Management**, which is very focused on governance, consistency, and auditability. It is well suited if your company is already an ISO-certified organization. But it also fits in with multinational companies and compliance-driven environments. The focus areas are:

- **Incident detection and reporting:** Focus on assuring that security incidents are identified early and reported consistently across the organization.
- **Assessment and decision-making:** Helps to establish severity, impact, and appropriate response to a reported incident.
- **Response and recovery:** Contain the incident, mitigate damage, and restore normal operations securely.
- **Continuous improvement**: Strengthen the organization's incident management capability over time.

It is important to mention that some organizations may adopt a mix of both standards. A company may use NIST 800-61 as their structural backbone and ISO 27035 for governance and audit.

Let's look at an example of a financial services organization operating in North America and Europe, subject to regulatory scrutiny (SEC, GDPR, SOX, local financial regulators) with board-level focus on cyber risk, disclosure, and resilience.

This organization decided to use a hybrid approach in which it will leverage NIST 800-61 to define how incidents are handled operationally. In addition, they will leverage ISO/IEC 27035 to define how incident management is governed, reviewed, and audited.

Table 6.2 shows how the organization leverages NIST 800-61 as the structural backbone for the end-to-end IR lifecycle:

NIST phase	**How it is used**
Preparation	IR plans, playbooks, tooling, training and tabletop exercises
Detection and analysis	SOC monitoring, alert triage and severity classification
Containment, eradication and recovery	Technical response actions and system restoration
Post-incident activity	Lessons learned and root cause analysis

Table 6.2 – Mapping NIST phases for IR

Table 6.3 shows how the organization overlays ISO 27035 governance requirements across every NIST phase:

ISO 27035 focus area	**Governance layer applied**
Incident detection and reporting	Standardized reporting criteria, audit trails
Assessment and decision-making	Defined roles for legal, risk, exec sign-off
Response and recovery	Change control, documentation, accountability
Continuous improvement	Formal reviews, metrics, policy updates

Table 6.3 – Governance layer applied to ISO 27035

Based on those focus areas that were leveraged in each standard, the custom one that fits this organization's needs looks like the diagram in *Figure 6.1*:

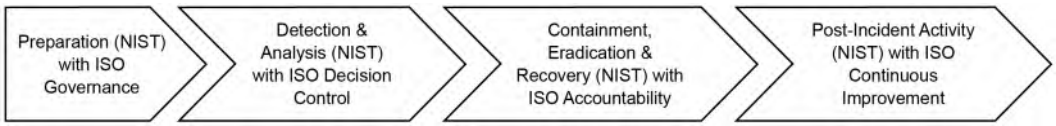


Figure 6.1 – Custom IR process

Now let's look in more detail at each focus area of this custom IR process:

- Preparation (NIST) with ISO Governance
  - Operational (NIST):
    - Build IR playbooks and escalation paths.
    - Train SOC, IT, legal, comms, and executives.
    - Pre-establish external counsel and insurers.
  - Governance (ISO):
    - Define ownership of the IR program.
    - Approve policies through risk committees.
    - Document roles and accountability.

Outcome: IR readiness that is operationally executable and audit-ready

- Detection and Analysis (NIST) with ISO Decision Control
  - Operational (NIST):
    - SOC detects suspicious activity.
    - Analysts validate and classify the incident.
  - Governance (ISO):
    - Severity classification requires a business impact assessment.
    - Legal and risk teams participate in materiality analysis.
    - Decision logs capture why actions were taken.

Outcome: Fast detection combined with defensible executive decisions

- Containment, eradication and recovery (NIST) with ISO Accountability
  - Operational (NIST):
    - Isolate affected systems.
    - Remove attacker access.
    - Restore systems securely.
  - Governance (ISO):
    - Recovery actions follow change-management controls.
    - Executive approval required for high-risk remediation.
    - All actions logged for audit and insurance claims.

Outcome: technical response with clear accountability and traceability

- Post-incident activity (NIST) with ISO continuous improvement
  - Operational (NIST):
    - Conduct lessons-learned sessions.
    - Identify root causes.
  - Governance (ISO):
    - Assign remediation owners and SLA.
    - Track findings to closure.
    - Update policies, controls, and training.

Outcome: Incidents drive measurable maturity improvements, not just reports

Proactive vulnerability and exposure management

Most organizations have no shortage of vulnerability data. Modern scanning tools can identify thousands or even millions of security findings across on-premises environments, cloud workloads, applications, and endpoints.

Yet despite having this wealth of information, many organizations still struggle to demonstrate meaningful reductions in business risk. The problem is rarely a lack of visibility into vulnerabilities; it is determining which weaknesses matter most, how they could realistically be exploited by attackers, and where limited resources will have the greatest impact on reducing the organization's overall exposure. Without that context, security teams often spend considerable effort addressing issues that have little effect on the risks that matter most to the business.

This section marks a deliberate shift away from vulnerability-centric thinking toward an exposure-based approach to risk management. It examines why traditional vulnerability management frequently fails to change outcomes, introduces **continuous threat exposure management (CTEM)** as a practical evolution, and explains how business context, threat intelligence, and continuous validation converge to drive smarter prioritization.

The goal is not to replace existing practices, but to mature them into a model that aligns operational effort with real-world risk reduction. In *Figure 6.2* you have the illustration of this evolution and the different parameters that are used:

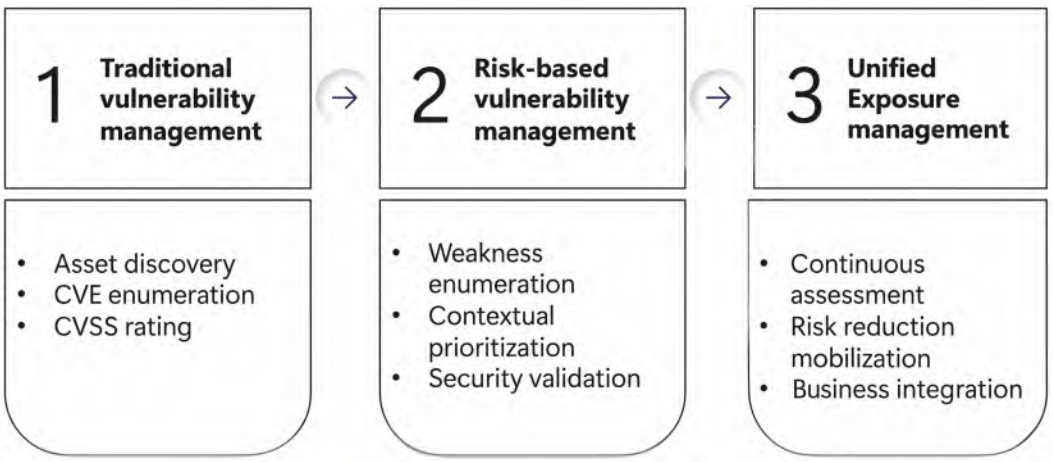


Figure 6.2 – Moving from traditional vulnerability management to unified exposure management

Defining the limitations of traditional vulnerability management

Traditional vulnerability management programs were built to solve an important problem: identifying technical weaknesses at scale. Most rely on periodic scanning, CVE identification, and prioritization through severity-based scoring models such as the **Common Vulnerability Scoring System (CVSS)**. While these mechanisms remain valuable inputs, they are no longer sufficient on their own.

In practice, many programs generate overwhelming volumes of findings with limited guidance on what to address first. Teams are measured on activity (how many vulnerabilities were discovered, patched, or closed) rather than on whether those actions materially reduced the organization's exposure to attack. Over time, this creates a false sense of progress: dashboards improve, but incidents continue.

These programs tend to suffer from three systemic limitations, outlined in *Table 6.4*.

Limitation	Rationale
Prioritizing technical severity over business impact	CVSS base scores describe vulnerability severity; they do not, by themselves, determine the business risk to your organization.
Lacking alignment with real-world threat activity	Vulnerabilities are treated equally regardless of whether they are actively exploited or relevant to the organization's threat landscape.
Encouraging reactive and fragmented remediation	Teams focus on fixing what is easiest or most visible rather than what attackers are most likely to use.

Table 6.4 – Limitation and rationale

The result is a familiar pattern: significant effort, visible activity, and limited risk reduction. Vulnerability counts decline, yet incident frequency and impact remain unchanged. For a cybersecurity leader in their first year, this disconnect creates early credibility challenges with executives who expect security investments to translate into measurable business protection.

Moving from vulnerabilities to exposure with CTEM

A vulnerability represents a weakness, and an exposure represents a condition. An exposure exists when a vulnerability, misconfiguration, or weak control intersects with asset criticality, attacker capability and intent, and the effectiveness of existing defenses. This is why organizations with similar vulnerability counts can experience vastly different risk outcomes.

As security programs mature, prioritization shifts beyond severity scores and patch lists toward understanding attack paths and business impact. The question moves from "How severe is this vulnerability?" to "How could this be used, what would it enable, and what would it affect?"

Continuous Threat Exposure Management provides a structured way to operationalize this shift. CTEM does not eliminate vulnerability management; instead, it builds on it. Vulnerability scanning remains a foundational input, but CTEM enriches that data with threat intelligence, attack simulation, identity and cloud exposure analysis, and continuous validation. This reflects how modern adversaries operate: exploiting combinations of conditions rather than isolated flaws.

Rather than treating risk as a static list of findings, CTEM frames exposure as a dynamic condition that changes as assets, threats, and controls evolve. At its core, instead of asking "What vulnerabilities do we have?", CTEM asks a different question: "Which exposures, if exploited by real adversaries, would meaningfully impact our organization, and how likely is that to occur?" This distinction is crucial as cybersecurity risk is not defined by the presence of a vulnerability alone, but by the intersection of attack paths, asset criticality, threat activity, and control effectiveness.

By introducing CTEM in the first year, you shift the conversation from activity to outcomes. This creates early alignment with executives, focuses limited resources on what truly matters, and establishes a modern risk language that supports better decisions during incidents, audits, and investment discussions.

Applying the CTEM framework

CTEM is not a one-time assessment; it is a continuous cycle. Its value comes from repetition, refinement, and feedback. Each iteration improves visibility, sharpens prioritization, and reduces exposure as the environment and threat landscape evolve. The framework is commonly described through five interconnected phases: scoping, discovery, prioritization, validation, and mobilization. While often presented sequentially, mature organizations operate several phases in parallel. These steps align with the CTEM framework according to Gartner, which is shown in *Figure 6.3*:

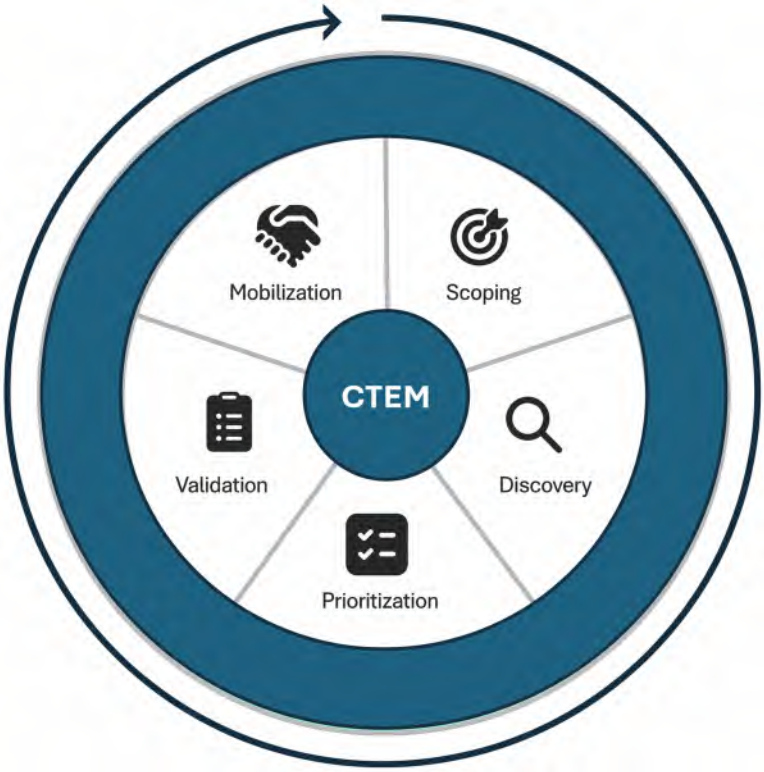


Figure 6.3 – CTEM framework according to Gartner

The following list explains each phase:

- **Scoping**: In this phase, you will map and rank the organization's most important assets throughout the exposure landscape, ensuring protection efforts directly support business goals and operational impact.
- **Discovery**: Now is the time to establish a structured and repeatable discovery process to identify organizational assets, continuously assess their risk profiles, and maintain clear visibility into how changes in the environment affect overall security exposure.
- **Prioritization**: Next, you will prioritize risks by evaluating how easily they can be exploited, the potential impact on the business, and the effectiveness of existing controls. This will help focus the efforts toward the most consequential exposures rather than attempting to address every issue.
- **Validation**: Now comes the part where you need to validate the effectiveness of security controls by exercising them through attack simulations, red team activities,

and scenario-based analysis. This will ensure that defenses can withstand real-world threats and operating conditions.

- **Mobilization**: Lastly, you will drive remediation efforts through well-defined ownership, measurable milestones, and continuous improvement cycles. This will enable the organization to steadily reduce security exposure over time.

Scoping: establish executive alignment

The first step in the adoption of CTEM is to ensure that executive leadership has the right understanding of what CTEM is and what it is not. Clearly articulate that CTEM is about reducing material risk, not adding another security tool or process. Define success in business terms: reduced attack paths to crown jewel assets, faster remediation of exploitable exposures, and improved visibility into risk trends over time.

Scoping: identify crown jewel assets

Work with business and IT leaders to identify crown jewel assets, including critical applications, sensitive data, key identities, and core cloud workloads. Without this context, exposure prioritization becomes generic and ineffective. It is imperative that you work with stakeholders across the organization to have the right level of visibility across different workloads and ensure that they provide an accurate list of crown jewel assets.

Discovery: identify assets and exposures

Where you will keep this list varies according to your organization's tooling. You will see different approaches to keeping up this list, from spreadsheets to **configuration management databases (CMDBs)**. While this can be a valid approach, there are a lot of disadvantages, such as manual updates of this list, high maintenance in terms of access control, and lack of integration with other tools.

The ideal scenario is to have this automation done by a unified platform, such as Security Exposure Management, or for cloud-specific workloads you can also rely on a **cloud-native application protection platform (CNAPP)**. Tools under those categories will do the automatic discovery and keep this information in a single dashboard (the so-called "single pane of glass"). As new high-level assets are added, this platform will automatically discover, classify, and make them available in the dashboard.

Assess the current state of exposure by aggregating inputs from different vulnerability scanners, cloud security posture tools, identity systems, endpoint security, and network configurations.

This automatic aggregation and correlation rely on Exposure Action Platforms, also known as Security Exposure Management or Remediation Operations tools; these automate and streamline the process of managing and fixing security vulnerabilities. Many **Cloud Service**

Providers (CSPs) offer native tools that can help you with your CTEM journey. The only thing to watch out for is the cost of integrating any on-prem tools into the cloud.

Here you should leverage data and tooling that already exist in the environment. However, if the company does not have the right level of visibility on that, you will need to introduce new cloud security tools to perform those tasks.

Prioritization: rank exposures using threat context

Enrich exposure data with **threat intelligence (TI)** to understand which weaknesses are actively exploited and by which threat actors. This step transforms CTEM from a theoretical exercise into a threat-informed program grounded in real attacker behavior.

Once this enrichment is set up, you can prioritize attack paths, privilege relationships, internet exposure, and control gaps. This adds a series of risk factors, which is much better than just raw CVE counts. In the next section of this chapter, we will go over more details about integrating TI into decision-making.

Redefine success metrics and move away from KPIs such as "vulnerabilities closed per month" and toward metrics like:

- Reduction of exploitable attack paths to critical assets
- Mean time to remediate high-risk exposures
- Percentage of exposures validated as mitigated

By using these metrics, you are reinforcing CTEM's outcome-driven mindset and tailored prioritization.

Validation: confirm defensive effectiveness

Regularly validate whether remediation actions reduce exposure using attack simulation, red-team insights, or breach-and-attack techniques. Use these insights to refine prioritization models, improve detection coverage, and close control gaps.

Establish regular collaboration between security, IT operations, cloud teams, identity teams, and application owners. Ensure that countermeasure controls that were implemented are validated by the proper stakeholders before deployment.

Mobilization: from insight to action

Mobilization is not about handing teams a list of issues; it is about providing direction. Exposure findings must be translated into:

- Clearly defined remediation actions
- Ownership by specific teams (IT, cloud, identity, app owners)
- Expected outcomes (what risk is reduced and why it matters)

You must ensure that every remediation task answers the following question: "*What exposure does this reduce, and what business risk does it mitigate?*" Make sure to also maintain executive visibility and support. Regular updates to leadership should show progress against high-risk exposures (review *Chapter 2* for more information about meeting cadences), highlight blockers that require leadership intervention, and demonstrate how CTEM investments reduce real-world attack potential. By using this approach, you keep CTEM aligned with strategic priorities and prevent it from devolving into a purely technical exercise.

When it comes to addressing these recommendations, you also need to take into consideration the organization's appetite for self-healing, or what is also called auto-remediation. It is important to acknowledge that not all security issues can be auto-remediated. Incorrect or poorly scoped remediation can break applications or workflows, and this poses a risk in production environments. If an auto-remediation breaks a production system, you will not only deal with downtime but also lose trust from the leadership. Trust erosion is hard to recover from once automation causes outages.

With that in mind, consider starting the self-healing strategy by focusing on low-risk, high-confidence scenarios. Common scenarios would be closing public storage access, enforcing MFA, and fixing misconfigurations with known safe defaults. In addition, you can also consider:

- Repeatable control failures that already have approved remediation steps
- Policy-driven violations, not ambiguous threats

Tip

Auto-remediation is only effective when foundational capabilities are already in place. Because self-healing is still a relatively new concept, building trust in automated actions is critical. If the organization is not there yet, focus on strengthening those core components first. Where readiness exists, begin with low-risk, high-return use cases to build confidence while safely reducing exposure.

In summary, the goal of this phase is to be able to prove that exposure insights lead to meaningful action, that security efforts reduce real risk, and that the organization can react faster to adversaries.

Integrating threat intelligence into decision-making

For a cybersecurity leader entering a new organization, the first year is not only about stabilizing operations but also about establishing how decisions are made. If the organization already uses **threat intelligence (TI)** as part of its decision making, then you need to

understand how it is used. But if it does not, then you have a great opportunity to establish a new process to integrate TI into decision-making.

Threat intelligence is often treated as a passive feed of indicators or an isolated analyst function, which is not the best way to leverage this type of insight. When effectively integrated, threat intelligence guides strategy, priorities, investments, and executive communication.

If threat intelligence is positioned early as a decision driver, it becomes embedded in governance, budgeting, and culture. If it is delayed or marginalized, it risks becoming an isolated function with limited influence.

A cybersecurity leader should enable intelligence-driven decision-making as early as possible. This is critical to avoiding tool sprawl, misaligned investments, and miscommunication with executives.

Tactical, operational, and strategic TI

As a cybersecurity leader, you should recognize that not all TI serves the same purpose, nor the same audience.

Tactical TI focuses on near-term, operational relevance. Tactical TI's primary audience is SOC analysts, incident responders, and detection engineers. Tactical TI helps answer questions such as:

- What should we block, detect, or hunt today?
- How are current campaigns bypassing defenses?

Tactical threat intelligence should be automated, contextualized, and operationalized to drive prompt response. It should inform immediate action, not be manually consumed or elevated as strategic insights.

> **Tip**
>
> In cases of high visibility, such as an active exploitation campaign or critical vulnerability, best practice is to share a brief written update to establish a clear record of awareness and response.

Operational threat intelligence sits between tactical and strategic intelligence and is often the most underutilized. It focuses on adversary **tactics, techniques, and procedures (TTPs)**, attack paths, and campaign patterns over time. Operational threat intelligence supports questions such as:

- How do attackers typically gain initial access in our environment?

- Which techniques are most likely to succeed given our controls?
- Where are defensive gaps most likely to be exploited?

Its primary audience includes threat hunters, detection engineers, exposure management teams, and incident response leaders. Operational threat intelligence plays a critical role in prioritizing exposures, informing CTEM validation activities, and shaping detection and response strategies based on how adversaries operate.

Strategic threat intelligence operates at a different level, since it focuses on adversary intent, capability, and targeting patterns. In addition to that, it also considers threat actor motivations and preferred industries, long-term trends, and geopolitical or economic drivers of cyber activity.

Strategic TI's primary audience includes executive leadership, risk committees, and boards. This audience is expecting to obtain answers to the following questions:

- Which threat actors are most relevant to our business model?
- Where should we invest to reduce long-term risk?
- How is the threat landscape evolving over the next 12–24 months?

Building an intelligence-led defense

An intelligence-led defense is not defined by how much intelligence is collected, but by how consistently intelligence shapes decisions. The use of TI at this level helps to shift security from reactive response to proactive risk reduction. You can leverage frameworks such as MITRE ATT&CK to provide a shared language to connect intelligence with defensive capabilities. This will enable security teams to see where detection or prevention gaps align with known adversary behavior.

In the first year, cybersecurity leaders are often overwhelmed by competing demands. For instance, a newly discovered vulnerability may compete for attention and resources with an ongoing cloud security initiative, an upcoming regulatory audit, and remediation commitments from a recent penetration test. TI can help to answer a critical question: "*Which of these exposures is most likely to be exploited by adversaries targeting organizations like ours?*" By integrating intelligence with exposure management, leaders can focus remediation on attack paths that matter, rather than treating all findings equally.

Figure 6.4 represents the different stages of TI and how various groups will consume it.

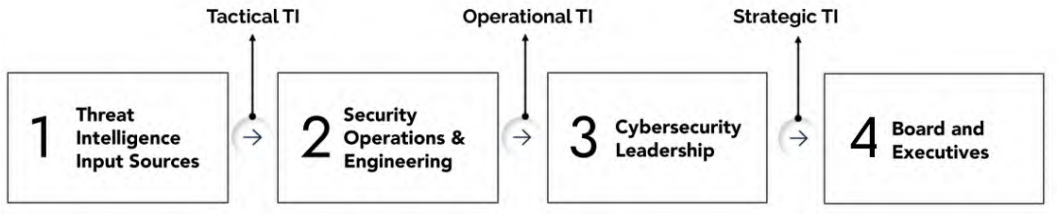


Figure 6.4 – TI from raw to decision-making

By building an intelligence-led defense, cybersecurity leaders do not need to simply report that "*X vulnerabilities were closed*;" instead, the cybersecurity leader can include in their report something like "*We reduced attack paths used by ransomware operators targeting companies in our sector by 42% this quarter.*" This helps to bring clarity, build confidence, and trust.

With that in mind, you can use the four-phase approach described in *Table 6.5* to build an intelligence-led defense over a 12-month period.

Phase	Tasks	Considerations	Timeline
Establish the foundation	Define the purpose of threat intelligence	Define intelligence as an enabler of prioritization and risk reduction. Align intelligence objectives with business risk, not tool coverage. Set the expectation that intelligence will guide what to fix first.	Months 0–3
	Identify intelligence consumers and decision points	Identify tactical consumers: SOC, IR, detection engineering. Identify operational consumers: cloud, identity, vulnerability teams. Identify strategic consumers: CISO, CIO, risk committees, board.	

Phase	Tasks	Considerations	Timeline
	Separate tactical and strategic intelligence streams	Avoid using tactical indicators to justify strategic decisions.	
Integrate intelligence into operations	Operationalize tactical intelligence	Map threat intelligence to detection logic using frameworks such as MITRE ATT&CK. Automate ingestion of relevant indicators where possible. Use intelligence to guide proactive threat hunting, not only alert response.	Months 3–6
	Embed intelligence into exposure management and CTEM	Correlate intelligence with attack paths, identity privileges, and cloud exposure. Prioritize remediation based on likelihood of exploitation, not severity scores alone.	
	Establish continuous validation loops	Validate whether controls disrupt known adversary techniques. Use red teaming, purple teaming, or attack simulation where appropriate.	
Enable leadership and governance	Develop an executive intelligence narrative	Focus on intent, likelihood, and impact. Avoid technical detail unless directly tied to risk. Highlight trends affecting the organization's industry or geography.	Months 6–9

Phase	Tasks	Considerations	Timeline
	Integrate intelligence into security governance	Use intelligence to shape security roadmaps and investment priorities. Reference intelligence during risk acceptance and exception decisions.	
	Establish regular intelligence briefings	Conduct operational intelligence briefings with SOC and engineering weekly or every two weeks. Conduct monthly meetings for exposure and CTEM intelligence review. Conduct quarterly meetings for strategic threat briefing with executives and board.	
Measure, mature, and continue to improve	Define metrics that reflect outcomes	Reduce exploitable attack paths tied to active threats. Improve detection coverage against high-risk adversary techniques.	Months 9–12
	Reinforce cultural adoption	Reinforce that intelligence informs priorities, not opinions. Promote collaboration between intelligence, operations, and leadership.	
	Continuously refine the intelligence program	Periodically reassess which threat actors matter most. Retire low-value feeds and focus on relevance. Align intelligence maturity with business and technology changes.	

Table 6.5 – Building intelligence-led defense

The value of strategic threat intelligence also depends on *where the intelligence comes from.* Do not rely on a single commercial feed or vendor to define the threat landscape for your organization. Build an intelligence ecosystem that combines multiple sources. Commercial security vendors can provide research on threat actors, campaigns, malware, and emerging attack techniques. Government agencies can provide advisories, vulnerability information, and intelligence about nation-state and critical infrastructure threats. **Information Sharing and Analysis Centers (ISACs)** and **Information Sharing and Analysis Organizations (ISAOs)** can provide sector-specific intelligence and allow organizations facing similar threats to share information. Industry trade groups, trusted peer networks, open-source intelligence, and internal telemetry from your own incidents and security operations can provide additional context. The goal is not to consume as much intelligence as possible, but to identify a set of trusted sources that are relevant to your industry, geography, technologies, and business model, and then correlate that external intelligence with what you are seeing inside your own environment.

Maturing the SOC: people, processes, and technology

The first year leading a cybersecurity program is not about building a "perfect" SOC; it is about evaluating the operating model, correcting structural weaknesses, and creating momentum toward maturity. Although definitions of SOC maturity vary, this book focuses on how effectively the SOC responds to existing threats, prepares for future risks, and bridges the gap between them. A successful first-year strategy focuses on clarity of roles (people), repeatability of execution (process), and tool enablement (technology).

One of the first strategic decisions that a cybersecurity leader should take in the first year is defining how the SOC operates. While there are many best practices for the SOC, and each security vendor will enumerate some of those, it is important to state that there is no universal best model, only what best aligns with organizational scale, sector, and risk profile.

To understand how the SOC operates, you need to be familiar with the common SOC operational modes:

- **Centralized SOC**: One core team manages detection and response. This model provides consistency, easier governance, and tooling standardization.
- **Distributed SOC**: Regional or business-unit SOC teams aligned to local operations. This model provides better context and faster local response while allowing higher coordination and governance complexity.
- **Virtual/Hybrid SOC**: In this model you usually have federated teams using shared platforms, telemetry, and playbooks. This model has grown over time in cloud-first and

global organizations. While the adoption of this model is not as common as the others, it is worth mentioning for awareness.

> **Tip**
>
> One priority for your first year is to establish clear ownership, escalation paths, and decision authority, regardless of the model for specific actions such as shutting down production assets or responding to time-sensitive customer inquiries. Ambiguity here leads to missed detections and delayed response.

The organization that you have joined likely already has an operational SOC, and if this is the case, you need to better understand how this SOC is currently operating. Ideally, the SOC should have clear analyst tiers and responsibilities (Tier 1–3, threat hunters, incident commanders).

You should also assess the SOC analysts' (people) current state and potentially address burnout risk by reducing noise and repetitive tasks. You should also upskill SOC analysts to think beyond alerts and toward threat behavior and impact.

Many SOCs stall because they rely on manual processes. As you revise the current SOC processes, ensure that you standardize triage, investigation, containment, and escalation. You should automate and enable the alignment between SOC workflows, incident response, and crisis management.

In addition to that, make sure to:

- Introduce post-incident reviews to drive continuous improvement.
- Introduce new metrics (if not already included) such as number of incidents by category, mean time-to-detect, and time-to-contain.

Nowadays, there is a big opportunity to enable scale with the use of AI. However, trust in AI is built gradually and with transparency. AI should be positioned as a decision supporter, not a replacement for SOC analysts, mainly in the first year. Some tasks for which you can leverage AI to enhance your SOC include:

- Correlating signals across identities, endpoints, cloud, and networks
- Prioritizing alerts based on behavior and exposure
- Reducing false positives through contextual analysis

Leveraging the MITRE ATT&CK framework

MITRE Corporation is a U.S.-based, not-for-profit organization that operates **federally funded research and development centers.**

The MITRE ATT&CK framework is a globally adopted knowledge base that documents and categorizes real-world adversary behavior across the cyberattack lifecycle, focusing on **TTPs** observed in the wild. Its purpose is to provide a common, structured language that enables security teams to understand how attackers operate, map threats to defensive controls, assess detection and response coverage, identify gaps, and prioritize improvements based on realistic attack scenarios rather than theoretical risks. Many organizations use MITRE to drive conversations at different levels of the security organization.

Encourage the SOC to leverage the MITRE ATT&CK framework to use common language and a structured view of adversary behavior. One advantage of integrating this framework with your SOC is to map detections, investigations, and response actions to specific tactics and techniques used by real-world threat actors. This improves detection coverage, highlights visibility gaps, and enables analysts to understand why an alert matters in the context of an attack chain.

The goal is to shift the SOC from reactive alert handling to a more threat-informed and hypothesis-driven operating model, where investigations are guided by attacker behavior rather than tool-generated noise. In addition, MITRE ATT&CK strengthens SOC maturity by enabling measurable improvement and collaboration across teams. For example, detection engineering teams can prioritize use cases based on high-risk techniques, red and purple teams can validate controls through MITRE ATT&CK-aligned simulations, and SOC leaders can report progress using clear, defensible metrics such as technique coverage and dwell time reduction.

The red team is responsible for testing the security controls by using techniques that simulate an attack. The objective is to find potential areas of compromise before the bad actors do it. The lessons learned from those exercises (penetration testing) will be used by the blue team to strengthen its defense.

The purple team plays a critical role in the SOC by acting as the bridge between offense and defense. This ensures that threat simulations directly improve detection and response capabilities rather than remaining isolated exercises. Within the SOC, the purple team uses the MITRE ATT&CK framework as a shared language to:

- Design attack scenarios.
- Map detections to specific techniques.
- Validate whether alerts, investigations, and response actions trigger as expected.

Maturing your SOC from reactive to predictive

To transform your SOC from reactive to predictive, you need to move your mindset from responding to alerts to anticipating threats. Do not make the mistake of thinking that it is only about automation, because it is not. If you just automate a reactive SOC, you get faster chaos.

The diagram shown in Figure 6.5 has the set of expectations for each pillar (People, Process, and Technology):

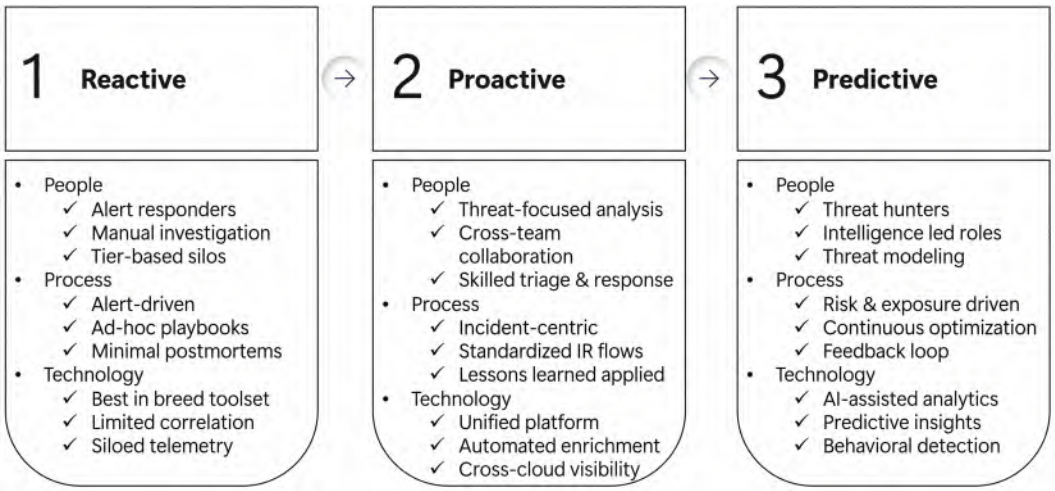


Figure 6.5 – SOC maturity journey

You should use the preceding figure as a roadmap for sequencing change, not as a checklist to rush through. This can be helpful in the first year to guide realistic expectations for progress. Keep in mind that reaching a fully predictive SOC within your first year as a cybersecurity leader is neither realistic nor advisable, unless you have joined an organization that is already operating in proactive mode. Realistically, the predictive capabilities depend on mature data quality, consistent processes, analyst expertise, and trusted automation.

The common approach for the first year is to use it as a foundation-building phase. Success should be defined by escaping reactivity and creating sustained momentum toward predictive operations over multiple years, rather than prematurely adopting advanced analytics that the organization is not yet ready to operationalize.

Security architecture as a strategic enabler

Early architectural decisions, such as identity models, network segmentation, cloud landing zones, and control placement, directly shape the effectiveness of security operations. When architecture is weak or fragmented, every other security domain compensates with manual controls, exceptions, and reactive processes. A well-defined architecture creates leverage, allowing security capabilities to scale, integrate, and operate consistently across the organization.

A first-year priority is establishing clear architectural principles that guide all technology decisions, with Zero Trust at the core. Zero Trust is a big topic, and we could write an entire

book just on architecture principles using Zero Trust, but for the purpose of this chapter, let's just summarize the goal of Zero Trust within this context. Zero Trust reframes security from perimeter-based assumptions to continuous verification of identity, device posture, workload integrity, and access context.

This approach, combined with strong segmentation, limits blast radius by reducing the impact of compromised credentials, misconfigurations, or lateral movement. A well-defined set of architecture controls that leverage the principles of Zero Trust will help to enforce least privilege, isolate critical assets, and ensure that trust is never implicit. These choices materially reduce risk and simplify downstream security operations.

Another important consideration for a well-designed security architecture is to embed *secure-by-design* principles into architecture standards and engineering workflows. In the first year, the cybersecurity leader should focus on shifting security "left" by influencing how systems are designed, built, and deployed, before SOC alerts, vulnerabilities, or incidents occur. This includes defining reference architecture, secure defaults, approved patterns, and guardrails for cloud, identity, and application development. When security is built into the architecture, remediation becomes the exception, not the norm, and teams spend less time fixing avoidable issues.

Table 6.6 has an example of key tasks that can be done in the first year. You can use this table as the foundation template and customize your plan according to your organization's needs.

Task	Goals	Sample Activity	Timeline
Establish or uplift the Architectural Baseline and Direction	Understand the current state architecture. Define principles, not solutions. Build alignment with technology and business leaders.	Inventory identity, network, cloud, endpoint, and application architectures. Define Zero Trust architectural principles. Establish secure-by-design standards.	Months 0–3

Task	Goals	Sample Activity	Timeline
Design Guardrails and Embed Secure-by-Design	Translate principles into enforceable controls. Shift security left without slowing delivery.	Define reference architectures for common workloads. Implement policy guardrails. Embed security requirements into CI/CD pipelines.	Months 3–6
Apply Zero Trust to High-Value Scenarios	Demonstrate measurable risk reduction. Build credibility through outcomes.	Apply Zero Trust controls to critical assets. Strengthen identity as the control plane.	Months 6–9
Operationalize and Measure Architectural Impact	Ensure architecture influences daily decisions. Connect architecture to SOC and IR outcomes.	Validate segmentation and access controls during incidents. Track metrics such as the number of secure-by-design deployments.	Months 9–12

Table 6.6 – Example first-year security architecture tasks

Keep in mind that this is not a Zero Trust implementation plan, and you should not think of Zero Trust implementation as a one-year project. Zero Trust and secure-by-design are operating models, not projects. Trying to fully implement Zero Trust in one year often results in partial controls, widespread exceptions, and operational friction. In the first year, your job is to make sure the organization builds forward, securely, deliberately, and with purpose.

An important part of secure-by-design is moving toward software-defined security architecture, where security requirements are encoded into the platforms, templates, and development workflows engineers already use. Security should not depend entirely on people remembering to consult a security document or having repeated conversations with the security team. Define security requirements as part of the architecture's **non-functional**

requirements (NFRs) and, wherever practical, enforce them through **infrastructure as code (IaC)**, policy as code, approved application and cloud templates, and CI/CD or **AI development lifecycle (AIDLC)** pipelines. For example, an approved cloud deployment template might automatically require encryption, centralized logging, managed identities, private connectivity, and approved network configurations.

A CI/CD pipeline can automatically scan source code and dependencies, validate Infrastructure as Code against security policies, and prevent a deployment when defined security requirements are not met. For AI applications, the same approach can embed requirements for model and data access, dependency validation, secrets protection, testing, and governance into the AIDLC rather than adding them only after the application is ready for production.

The objective is to create a consistent and opinionated architecture that makes the secure path the easiest path for engineering teams. Architecture standards still require collaboration between security, engineering, product, and platform teams, but the outcome of those conversations should increasingly be translated into reusable and enforceable controls. Instead of a security architect repeatedly telling individual teams how a workload should be secured, the organization's development platforms and deployment pipelines should apply those expectations consistently. This approach reduces configuration drift, limits dependence on manual reviews, and allows security architecture to scale as the organization builds more applications, cloud workloads, and AI-enabled systems.

Summary

In this chapter, you learned critical aspects of the transition between cybersecurity strategies and execution by understanding the importance of building a durable operational backbone during a security leader's first year. You learned how incident response, exposure management, threat intelligence, SOC maturity, and security architecture must operate as an integrated system rather than isolated functions. You learned how to establish clear operational cadences, governance rhythms, and outcome-driven metrics such as OKRs. In addition, you learned about incident response maturity, executive decision-making during crises, and the value of combining industry standards such as NIST 800-61 and ISO/IEC 27035 into a hybrid, defensible response model.

You also learned the importance of shifting vulnerability management toward CTEM and how business context, threat intelligence, and validation activities enable meaningful risk reduction. Lastly, you learned about security architecture, in particular Zero Trust and secure-by-design principles.

In the next chapter you will learn more about how to protect the crown jewels, which includes identity, access, and data security.

Additional resources

- MITRE ATT&CK Framework: `https://bit.ly/CISOBook15`
- Gartner (CTEM): `https://bit.ly/CISOBook16`
- NIST SP 800-61 Revision 2: `https://bit.ly/CISOBook17`
- NIST SP 800-61 Revision 3: `https://csrc.nist.gov/pubs/sp/800/61/r3/final`
- Zero Trust Architecture (NIST Special Publication 800-207): `https://bit.ly/CISOBook18`

7

Protecting the Crown Jewels: Identity, Access, and Data Security

Protecting the crown jewels involves knowing which identities matter most, which privileges are excessive, which data carries regulatory or competitive weight, and which cloud configurations introduce risk. The preceding work requires disciplined governance, thoughtful architecture, and a willingness to simplify complexity into business-aligned priorities.

Crown jewels include identities, data, systems, and digital assets that, if compromised, could materially affect your organization's trust, revenue, operations, or reputation. In today's environment, your assets are no longer confined to a data center rack or guarded by a firewall. They live in cloud platforms, SaaS applications, developer pipelines, APIs, and now increasingly within machine and AI-driven identities. The perimeter has dissolved. Identity has taken its place. Data has become fluid. Accountability for data protection sits squarely at the leadership level.

This chapter will walk you through what it means to define and prioritize critical assets, why identity has become the new security control plane, and how mature identity and access management reduces real business risk. The following topics will be covered:

- What are the "crown jewels"?
- Identity as the new security perimeter
- Understanding and classifying critical data
- Data protection strategies across the data lifecycle
- Managing third-party and supply chain risk

What are the "crown jewels"?

For a security executive entering a leadership role, one of the earliest and most consequential responsibilities is deciding where security attention truly belongs. Time, budget, and talent are always limited, while the list of potential threats continues to grow. Treating all assets as equally critical is not feasible, and in practice it dilutes focus and weakens protection. The concept of **crown jewels** exists precisely to address this challenge: it helps leaders concentrate protection efforts on the assets whose compromise would cause the greatest harm to the organization.

In the past, organizations often defined crown jewels in narrow technical terms. For instance, a particular database, a financial system, or a production server housed in a corporate data center might have been considered the most valuable asset to protect. While these elements still matter, this view no longer reflects how modern enterprises operate. Today's organizations must deal with a more diverse set of technologies, such as cloud services, new ways of working that include full-time remote work, and new challenges introduced by supply chains.

As a result, crown jewels now extend beyond individual systems. Sensitive data is almost always at the top of the list, including customer records, employee information, financial data, intellectual property, and regulated datasets. Equally important are identities, namely user accounts, administrative roles, service accounts, application identities, and automated workloads that access systems and data on behalf of the business. Critical business processes also qualify as crown jewels when their disruption would halt operations, prevent revenue generation, or significantly damage customer trust. In addition, trust relationships, such as those with cloud providers, vendors, and strategic partners, are also now considered assets. Compromised trust relationships can give attackers indirect access to otherwise well-protected systems and data.

> **Note**
>
> What distinguishes a crown jewel is not its technical sophistication or its direct monetary value, but the impact of its loss, exposure, or misuse. Compromising a less secure third-party vendor can give attackers access to the organization's critical assets.

For new security executives, identifying crown jewels is as much a business exercise as a technical one. As discussed in *Chapter 1*, it requires conversations with business leaders, legal and privacy teams, compliance stakeholders, and technology owners. The goal is to understand how the organization creates value, what it must protect to continue operating,

and where a failure would be most damaging. This understanding will evolve over time and should be revisited as strategies, technologies, and regulatory obligations change.

The need to protect identity and data

Cyber incidents are often described using technical terminology: malware infections, phishing attacks, ransomware outbreaks, or cloud misconfigurations. While these descriptions are accurate, they can obscure a more important pattern. In many cases, attackers succeed not by defeating advanced security technologies, but by abusing legitimate access or poorly protected data.

Compromised credentials are still one of the easiest ways for attackers to get a foot in the door. In real-world investigations, the use of stolen credentials shows up as a leading initial action, and phishing and credential-based access are consistently reported as common attack pathways. Once an attacker signs in as a "legitimate" user, the damage often comes from what that identity can do.

Overly broad permissions, weak access governance, and gaps in monitoring can turn a single compromised login into lateral movement, privilege escalation, or access to sensitive systems and data. That is exactly why widely used security guidance emphasizes least privilege: users and processes should only have the access they need to do their job, and no more. In parallel, many data exposure events are not the result of sophisticated attacks; they happen because sensitive data ends up in the wrong place or is made accessible through misconfiguration or lack of oversight (for example, public-facing storage or unmanaged "shadow" data repositories).

For executives, this pattern reframes how security investments should be evaluated. Identity and access management, data classification, and data protection are core risk-reduction mechanisms. Strong network security and endpoint protection remain necessary, but they cannot compensate for weak identity governance or a lack of visibility into data assets.

Cybersecurity leaders should balance responding to threats with proactively protecting the crown jewels of identity and data. Most modern breaches do not begin with sophisticated zero-day exploits; they begin with valid credentials used in the wrong context. That reality demands an identity-first security strategy. Leaders should enforce strong identity governance through least privilege, **just-in-time (JIT)** access, MFA , and continuous monitoring of sign-in behavior. Every identity, human or machine (or an AI agent), should be treated as a potential entry point. Access decisions should be contextual, risk-based, and continuously validated.

Protecting identity means understanding not only who has access, but why they have it, whether it is still justified, and what could happen if that identity were compromised. At the same time, protecting identity without protecting data leaves the mission incomplete. Security executives should pair strong access controls with:

- Data governance
- Clear classification of sensitive information
- Strict control over where it is stored
- Continuous auditing of permissions and proactive detection of abnormal data access patterns

Reducing the likelihood of a breach requires protecting the crown jewels of identity and data together; a compromised identity can cause significant harm when it provides access to critical assets, as shown in *Figure 7.1*:

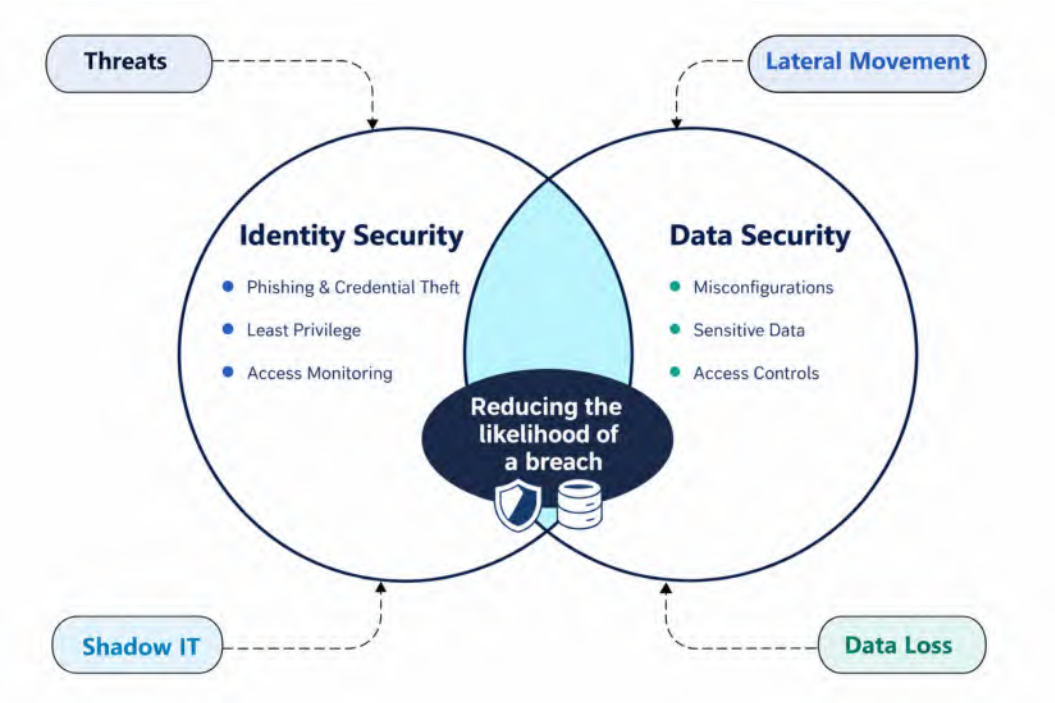


Figure 7.1 – Reducing the likelihood of a breach by prioritizing identity and data security

By aligning identity protection with data visibility and governance, leaders can reduce the likelihood that a single stolen credential will escalate into widespread exposure. In practice, this means going beyond simply protecting identities and ensuring that identity signals are integrated with data governance decisions. For example, classify sensitive data so the organization knows where its most valuable information resides, enforce least-privilege access so users can only access the data required for their roles, continuously review permissions to remove unnecessary or stale access, and implement conditional access or risk-based authentication for users accessing sensitive repositories. This integrated approach not only reduces the likelihood of security breaches but also strengthens executive confidence in how the organization controls access to its most sensitive systems and information.

Identity as the new security perimeter

For decades, cybersecurity strategies were built around a simple assumption: protect the network and you protect the organization. However, the way you build and operate technology has fundamentally changed. Cloud platforms, SaaS applications, remote work, mobile access, APIs, automation scripts, and AI-driven services have dissolved the traditional perimeter.

For cybersecurity leaders, this is more than a technical shift. It is a mindset transformation. If identity is now the new security perimeter, then the protection of identities and the data they access becomes the primary risk-reduction strategy.

Consistent identity and data controls help the business expand access without losing accountability. As new applications and services are introduced, define who can access sensitive information, under what conditions, and how that access will be reviewed.

Note

When executives understand that most breaches begin with identity misuse rather than firewall failure, resource allocation begins to shift accordingly.

To operationalize identity as the new perimeter, leaders should prioritize the elements from the following table, which provides an example activity and a suggested priority level:

Priority	Activity	Description
1	Establish identity as a Tier-1 risk category	Treat identity compromise as a Tier 1 enterprise risk by prioritizing identity governance, strong authentication, and **privileged access management (PAM)**. In practice, this means enforcing phishing-resistant MFA for privileged and high-risk users, implementing PAM to eliminate standing administrative privileges and require JIT access, conducting regular access reviews to remove excessive or stale permissions, and strengthening identity governance processes to ensure users receive only the access required for their roles.
2	Mandate strong authentication everywhere	Enforce MFA for all users, including administrators. Gradually but steadily eliminate legacy authentication protocols. Require conditional access policies that evaluate risk signals before granting access.
3	Adopt a Zero Trust access model	Require explicit verification for each access request. Use device posture, user risk, and behavioral analytics in decision-making. Minimize implicit trust based on network location.
4	Continuously monitor identity risk	Deploy tools that detect anomalous sign-ins, impossible travel, and suspicious behavior. Integrate identity alerts into the SOC workflow. Track metrics such as risky sign-ins, dormant accounts, and privileged account exposure.
5	Align identity and data protection strategies	Ensure identity governance and data classification programs are tightly integrated. An identity-centric strategy must protect access to the organization's crown jewels: identity and data.

Table 7.1 – Prioritization of activities

Every leader will find an organization at a different maturity level. If your organization is lower on its **Capability Maturity Model Integration (CMMI)** maturity for IAM (*Chapter 11* discusses program maturity and a consistent maturity scale), start with items four and five listed in the preceding table. Through the remediation of incidents identified by continuous monitoring, you will start addressing some of the legacy issues. For instance, through data protection, you will identify data in places where it should not be kept. You can then start changing the policies that allowed data to be written there in the first place to prevent recurrence.

Human and non-human identities

When leaders hear "identity," they often think of employees. However, modern enterprises operate with two broad categories of identities: human and non-human.

Human identities are your employees, administrators, contractors, and partners. They can be further categorized into **privileged human identities**. These privileged human identities include system administrators, cloud subscription owners, and domain admins and represent *high-value targets*. For instance, a single compromised admin account can lead to a full tenant takeover or data exfiltration.

Non-human identities include service accounts, workload identities, APIs, automation scripts, **robotic process automation (RPA)**, containers, and increasingly AI agents. As a matter of fact, in a study done by **International Data Corporation (IDC)** and sponsored by Microsoft, by 2028 there will be more than 1.3 billion AI agents deployed across the globe. In a secure environment, these agents will need to be controlled by an identity management system.

> **Note**
>
> Human identities are still the most visible attack vector for attacks such as phishing, credential reuse, social engineering, and MFA fatigue.

Cybersecurity leaders should protect human identities by enforcing **role-based access control (RBAC)**, removing standing global administrator privileges, implementing **JIT** access for high-risk roles, and conducting quarterly access reviews for privileged roles (ideally doing this in an automated manner).

Non-human identities introduce a more subtle and often more challenging way to implement governance to reduce risk.

Some of the factors that make non-human identities challenging to govern are inherently based on the usage scenario. Some of these scenarios include:

- Service accounts with hard-coded passwords
- Cloud workloads with excessive permissions
- API keys embedded in applications
- Automation scripts running with administrative rights
- AI agents that access internal data sources

Because they operate silently in the background, they can become persistent footholds for attackers. Cybersecurity leaders should treat AI agents and workload identities with the same rigor applied to human administrators. Consider the actionable tasks below when planning your identity management for non-human identities:

Task	**Description**
Inventory all identities	Create a centralized identity inventory across cloud and on-premises environments. Include service accounts, APIs, and workload identities. Track ownership and business justification for each identity.
Apply least privilege to non-human identities	Remove broad contributor or owner roles from workloads. Scope permissions to specific resources. Eliminate shared service accounts where possible.
Protect secrets	Eliminate hard-coded credentials. Use managed identities or secret vaults. Enforce automated credential rotation policies. Search for secrets and API keys across instant messaging tools (such as Teams or Slack) and in knowledge-sharing sites (such as SharePoint or Confluence).

Task	Description
Monitor AI agent behavior	Establish baselines for normal API and workload activity. Alert on abnormal data access patterns. Review token usage and privilege escalation attempts.

Table 7.2 – Identity management considerations for non-human identities

Business risk of identity sprawl and privilege creep

Identity risk does not usually explode overnight. It accumulates quietly as accounts and permissions grow without sufficient oversight. Two patterns drive this silent escalation: identity sprawl and privilege creep.

Identity sprawl happens due to the uncontrolled growth of accounts across systems. As organizations grow, identities multiply based on SaaS applications provisioned, DevOps pipelines created, and mergers and acquisitions that also introduce external directories. Without strong governance, dormant accounts remain active. Orphaned accounts persist after employees leave, and what was supposed to be temporary access becomes permanent.

On the other hand, **privilege creep** usually occurs when employees change roles but retain old permissions. Another common scenario is when temporary project access is never revoked. The result is an expanding blast radius, which means that a compromised low-level account with accumulated privileges can cause major damage to the environment.

Unmanaged accounts are another reality that security leaders must address pragmatically. In a well-designed identity governance program, these accounts should be rare, but legacy systems, embedded applications, and older infrastructure often still rely on local or hard-coded credentials. Instead of ignoring them, treat them as high-risk assets: inventory them, eliminate shared passwords, rotate credentials regularly, vault them in a PAM solution, and monitor their activity aggressively.

From an executive perspective, unmanaged identities increase risk in three dimensions, as shown in the following diagram:

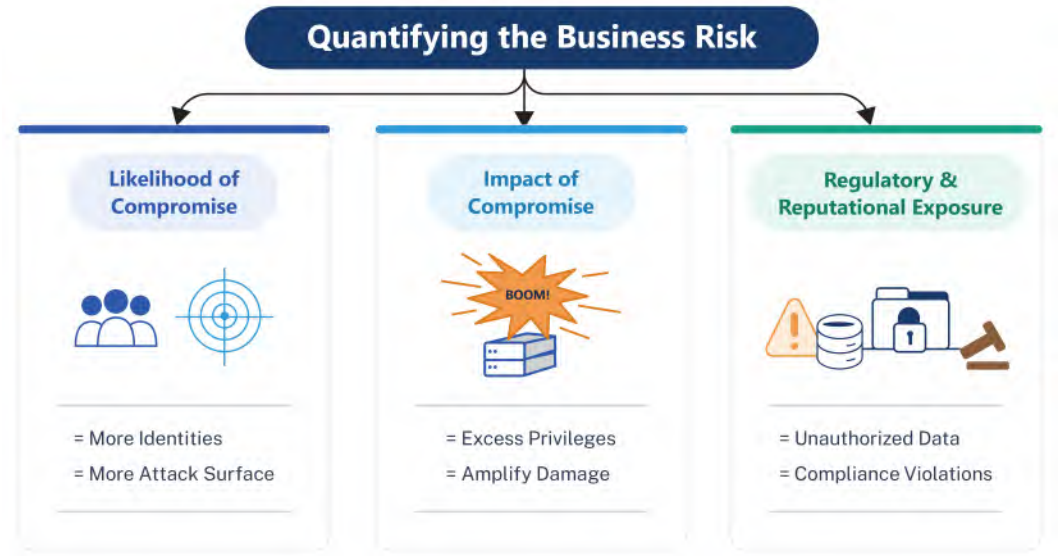


Figure 7.2 – Quantifying the business risk

Note

Identity sprawl and privilege creep silently undermine risk-reduction efforts unless actively managed.

Another important consideration regarding identity is birthright permissions. These birthright permissions are access rights that are automatically granted to individuals based on their role, department, or group membership. They are often inherited through **role-based access control** models. While this approach streamlines onboarding and operational efficiency, it can also lead to excessive standing access if not regularly reviewed. In situations such as layoffs, workforce reductions, or insider threat investigations, organizations must be able to rapidly revoke or suspend access without waiting for formal offboarding workflows. This access model is typically achieved through:

- Centralized identity management
- Emergency access revocation procedures
- Disabling privileged group memberships

- Enforcing JIT access models
- Temporarily suspending accounts pending investigation when necessary

The ability to quickly strip permissions without disrupting broader operations is a critical control for limiting blast radius during high-risk personnel events. Cybersecurity leaders should translate these risks into structured programs, and to do that, consider the following steps:

- Step 1: Implement lifecycle governance
  - Automate onboarding and offboarding.
  - Immediately disable accounts upon termination.
  - Link identity provisioning to HR systems.
  - Require periodic recertification of access.
  - Align identity lifecycle events with data lifecycle controls (classification, retention, and access revocation) to ensure access to sensitive data evolves or is removed as roles and business needs change.
- Step 2: Conduct regular access reviews
  - Perform quarterly privileged access reviews.
  - Require business owners to attest to necessity.
  - Remove unused roles and permissions.
  - Track review completion metrics.
- Step 3: Reduce standing privilege
  - Replace permanent admin roles with JIT access.
  - Enforce time-bound elevation.
  - Log and audit all privileged sessions.
- Step 4: Measure and report identity risk
  - Identify the number of privileged accounts.
  - Identify dormant accounts older than 90 days.
  - Identify accounts without MFA.
  - Identify service accounts with global permissions.
  - Measure access review completion rates.
  - Identify employees who retained access post-termination.
- Step 5: Protect the crown jewels of identity and data
  - Protect critical data repositories.

- Protect highly sensitive systems.
- Protect privileged administrative pathways.

The next section examines how to identify and classify critical data.

Understanding and classifying critical data

If identity is the control plane of modern security, data is the ultimate objective. Attackers rarely break in just to prove they can. They log in to steal, manipulate, encrypt, or expose something of value. That "something" is almost always data. Increasingly, this includes a long-term strategy known as **harvest now, decrypt later (HNDL)**. This involves adversaries exfiltrating encrypted data today with the expectation that future advances in quantum computing will allow them to decrypt it. In this context, sensitive data with long-term value, such as intellectual property, state secrets, health records, or strategic communications, faces risks. This reality reinforces the urgency of strong data governance today and the strategic transition toward quantum-resistant cryptography to protect information whose value extends well beyond the lifespan of today's encryption standards.

For cybersecurity executives, the question is no longer whether data protection matters. It is whether the organization truly understands which data matters most, where it lives, who can access it, and what would happen if it were exposed.

You can't protect what you don't know exists

You can start with a simple question in an executive meeting: *"What are our top 10 most sensitive data assets?"* If the room goes quiet, that is a visibility problem; in other words, no one knows the answer because they don't know where the sensitive data is located. The reality is that even if you know what those data assets are, copies of your most sensitive data are likely also stored in other places across the environment, including places where they should never reside, such as QA or Dev environments.

The cost of unknown or unclassified data shows up in three ways: blind spots in risk management, inefficient spending, and regulatory exposure. This is shown in the following diagram:

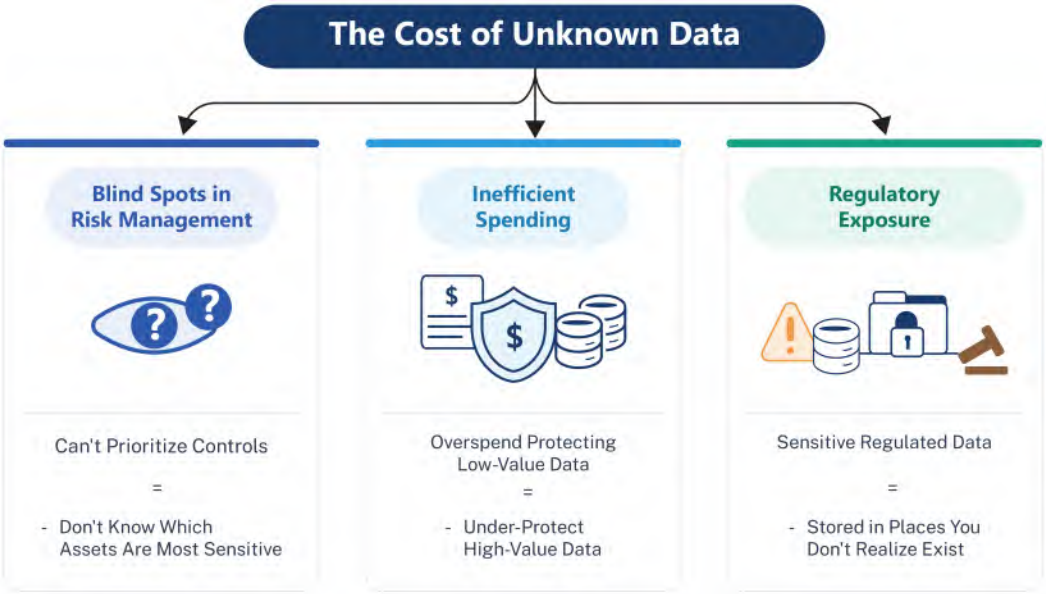


Figure 7.3 – Cost of unknown data

Each of the preceding pillars is explained in more detail below:

- **Blind spots in risk management:** You cannot prioritize controls if you do not know which assets are most sensitive.
- **Inefficient spending:** Teams overspend protecting low-value data while under-protecting high-value data.
- **Regulatory exposure:** Sensitive, regulated data might be stored in places where the organization does not even realize it exists.

Shadow data is usually accidental and not malicious. However, it still creates exposure because it is often outside standard governance processes. Also, it might not inherit the correct access controls, and it is rarely reviewed or reclassified. Cybersecurity leaders should move from reactive data protection to deliberate data understanding.

Consider the actionable tasks below when planning your data protection:

Task	Description
Launch a data discovery initiative	This should be a cross-functional business effort that includes: • Identifying where structured and unstructured data resides • Cloud, SaaS, file shares, collaboration tools, and backups • Systems tied to revenue, customers, and regulated data
Map data to business processes	Ask business leaders across the company to identify: • What data do you need to operate? • What data would materially impact revenue if unavailable? • What data would damage trust if exposed?
Identify crown jewel datasets	Establish a small, executive-approved list of: • Highly sensitive customer data • Financial reporting data • Intellectual property • Regulated personal information • Strategic plans
Measure unknown data risk	Track indicators of unknown data risk, including: • Percentage of storage without classification labels • Orphaned storage locations • Publicly accessible data repositories • Excessively permissive access policies

Table 7.3 – Considerations for data protection

If you don't know where to start, launch the data discovery initiative in an area of the environment where you have the least visibility. For instance, security leaders are constantly being told there is nothing to worry about in Dev or QA; hence, the security controls do not

have to be so strict. However, in most cases, it is the opposite. Follow this effort with a change to policy in your data protection tools so you do not continue to build more tech debt.

Data classification models for executives

One of the most common mistakes in data governance is over-engineering classification. Some organizations create 10 or more labels, which only leads to confusion and low adoption. Executives need simplicity; in other words, your classification needs to be easy to understand, communicate, and operationalize.

Your organization might already have a data classification policy in place, set up by legal, privacy, and compliance.

The four-tier data classification model shown in *Figure 7.4* presents an example of that:

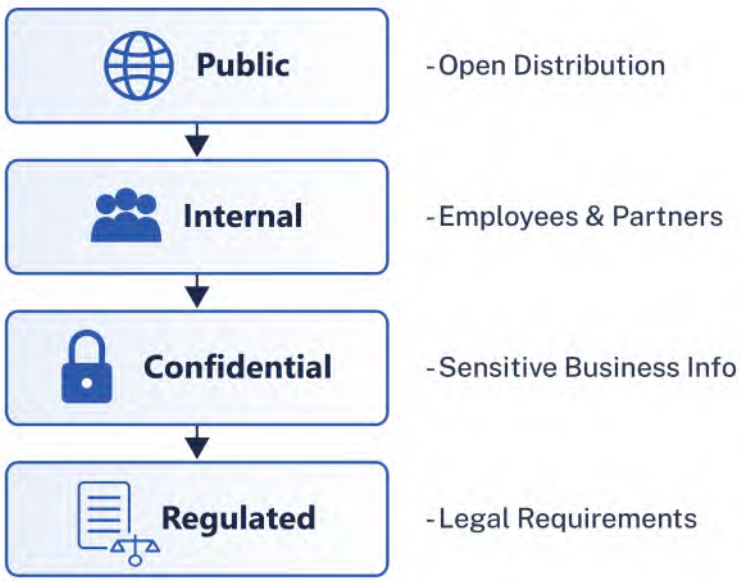


Figure 7.4 – Four-tier data classification model

Each data classification tier is explained in more detail below:

- **Public**: Information intended for open distribution. Examples include marketing materials and public reports.
- **Internal**: Information intended for employees and authorized partners. Examples: internal communications, operational documents.

- **Confidential:** Sensitive business information that could cause harm if exposed. Examples: customer data, financial projections, proprietary research.
- **Regulated:** Data governed by legal or industry requirements. Examples: personal data, health information, payment data.

These categories resonate at the executive level because they connect directly to business impact and regulatory obligations. Executives understand risk in terms of financial risk, competitive disadvantage, and legal exposure. Security leaders should translate data categories into impact narratives; for example, *confidential data exposure could impact revenue*, or *regulated data exposure could trigger fines and lawsuits*.

Ownership and accountability for data

A recurring issue in many organizations is unclear ownership. You can confirm that by asking questions such as: *Who owns this dataset? Who decides on retention? Who is accountable for its protection?* If the answer is "information technology (IT)" or "Security," there is a governance gap. A healthy data governance model distinguishes responsibilities.

The following table shows examples of accountability according to different functions:

Function	Description
Business unit	• Define data value • Approve access • Accept risk
Security	• Define protection standards • Monitor for abuse • Enforce policy compliance
IT	• Implement technical controls • Maintain infrastructure • Support lifecycle management
Legal and Privacy	• Interpret regulatory requirements • Guide retention and breach notification obligations

Table 7.4 – Accountability according to different functions

While accountability and clarifying roles and responsibilities are important, your organization is likely to have a data breach at some point. It only takes one file stored in the wrong location. Even if you try your best, some mistake is going to happen. If not to you directly, then it can occur with a third-party provider who had access to your environment at some point in time. For this reason, security leaders should focus on increasing visibility across the environment.

Many security leaders focus their energy on chasing tickets. Your data protection tools will identify a gap, and your team will go chase it. While remediation is necessary for certain data types, creating policies that will stop data from being written to unapproved locations to begin with is more beneficial in the long term.

In the end, protecting data is not simply about labeling files or applying encryption. It is about protecting the trust that customers, partners, employees, and shareholders place in the organization. When sensitive customer information is exposed, trust can take years to rebuild. When proprietary product designs, source code, research, or strategic plans are stolen, the organization might lose competitive advantages that took years to develop. It is also about meeting regulatory obligations, and, most importantly, it is about safeguarding the crown jewels that define the organization's future. Cybersecurity leaders who anchor data protection in business value elevate security from a technical function to a strategic imperative.

Data protection strategies across the data lifecycle

Many times, when people think about data protection, their most immediate solution is "Encrypt everything." While encryption is important, if that is the entirety of the strategy, it is not a feasible solution, and the organization will remain exposed. Data does not sit still; it is created, shared, processed, copied, archived, backed up, analyzed, exported, and sometimes forgotten. It moves across laptops, SaaS applications, APIs, cloud workloads, data lakes, AI pipelines, and backup systems. Protecting it requires more than a checkbox control. This approach requires understanding the data lifecycle and applying the right protections at the right stage.

Your responsibility as a cybersecurity executive is to ensure that governance, oversight, and accountability exist throughout the entire data lifecycle, from data collection and classification to storage, use, sharing, archival, and secure disposal. Achieving this requires close partnership with privacy, legal, compliance, data owners, and business leaders to establish clear policies, define ownership, and ensure that data is handled consistently regardless of where it resides.

Governing the data lifecycle while keeping privacy in mind means making deliberate decisions at every stage. Before data is collected, ask whether it is truly necessary for the intended business purpose and whether less sensitive information could achieve the same objective. As data is classified and stored, ensure that retention periods, access controls, encryption requirements, and geographic residency align with regulatory and contractual obligations.

When data is shared internally or with third parties, verify that access follows the principles of least privilege and that appropriate contractual and technical safeguards are in place. Finally, when the data is no longer needed, establish repeatable processes for secure archival or disposal so information is not retained longer than necessary. Privacy defines what should happen to data throughout its lifecycle, while cybersecurity provides the controls that help ensure those decisions are consistently enforced. Together, they create a governance model that protects sensitive information while enabling the business to use data responsibly and confidently.

Data stages

To ensure that data protection is in place, you need to understand that the data can be in three stages: data at rest, data in transit, and data in use. *Figure 7.5* presents these stages and the suggested protection:

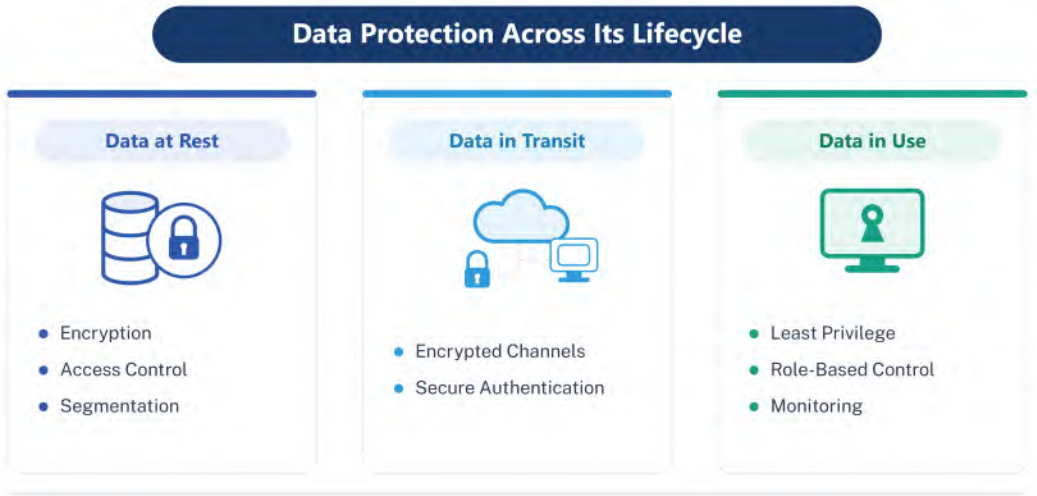


Figure 7.5 – Data stages

The following table has more details about each data stage and the suggested protection:

Stage	Description	Suggested protection
At rest	Data at rest is information stored somewhere: • Databases • File shares • Cloud storage • SaaS repositories • Backups	Protection at this stage includes: • Encryption at rest • Tokenization • Anonymization • Strict access control • Segmentation
In transit	Data in transit is data moving: • Between user and application • Between services • Across APIs	Protection here focuses on: • Encrypted communication channels • Secure API authentication • Certificate management • Data loss prevention
In use	This data is the one: • Displayed on a screen • Processed by an application • Queried in analytics tools	Protection here focuses on: • Least-privilege access • Role-based access control • Monitoring abnormal data queries • Data masking

Table 7.5 – The stages of the data and suggested protection

Cybersecurity executives should also ensure that there are actions across all three states, which include:

- Require documentation from workload owners of how sensitive data is protected at rest, in transit, and in use.
- Ensure that controls scale across cloud and on-prem environments. Apply consistent security controls, such as encryption, access management, and monitoring regardless of where data resides, to reduce security gaps and simplify governance.
- Tie protection requirements to classification levels. Define security requirements based on data sensitivity so that more sensitive information receives stronger protections, such as stricter access controls, encryption, and enhanced monitoring.

Encryption and key management

Encryption is one of the most powerful tools you have to protect sensitive information. However, when it is implemented without strong governance, it can create a dangerous sense of comfort.

NIST has mandated the deprecation of quantum-vulnerable encryption algorithms (for example, RSA-2048, ECC-256) by 2030 and the adoption of **post-quantum cryptography (PQC)** standards for critical systems. All systems using 112-bit security and legacy algorithms (**Rivest–Shamir–Adleman (RSA)**, **Elliptic Curve Digital Signature Algorithm (ECDSA)**, **Diffie–Hellman (DH)**) must be phased out, especially for national security systems.

Encryption depends entirely on how cryptographic keys are managed. If those keys are stored insecurely, shared too broadly, handled without separation of duties, or fully controlled by a third party without visibility, then the protection becomes fragile. At that point, encryption may exist on paper, but its real-world effectiveness is questionable.

This situation is why executives need to focus less on technical specifications and more on governance. The critical questions to consider are straightforward:

- Are the keys quantum-ready?
- Who generates the encryption keys?
- Who has the authority to rotate or revoke them?
- Who monitors and audits their use?
- And what is the plan if a key is compromised?

These responsibilities are not technical details for engineers alone; they are business risk questions that determine how resilient the organization truly is. Strong governance also requires separation of duties. No single administrator should be able to access sensitive data, manage the encryption keys that protect it, and control the audit logs that track activity.

Dividing these responsibilities reduces insider risk, improves accountability, and strengthens the organization's compliance posture.

Backup and recovery

Ransomware attacks do not always aim just to steal data. In some cases, they aim to make it unavailable or to extort organizations by threatening exposure. A backup and recovery strategy is therefore not an IT operational task; it is a fundamental component of executive risk management. Every organization should assume that, at some point, systems may become unavailable due to ransomware, human error, hardware failure, or a natural disaster. The question is not whether backups exist, but whether the organization can recover its most critical business operations within an acceptable timeframe. For example, a company might successfully restore its data after a ransomware attack, but if the recovery takes several days instead of the four-hour recovery objective established by the business, the financial and operational impact can still be significant. As a security executive, your role is to ensure that backup and recovery capabilities are regularly tested, aligned with business recovery objectives, and capable of supporting the organization's resilience when an incident occurs.

Cybersecurity executives should ensure the level of data resilience by asking the following questions:

- Are backups immutable?
- Are they protected from administrative tampering?
- Are they tested regularly?
- When was the last successful recovery exercise?
- How long would full restoration take?
- What data would be permanently lost?

Additionally, you need to establish clear recovery objectives for critical systems, including defined **recovery time objectives (RTOs)** and **recovery point objectives (RPOs)**. These targets set expectations for how quickly systems must be restored and how much data loss the organization is willing to tolerate.

Further, restoration should not be theoretical. Regular recovery testing should be required to ensure backups can actually be restored under pressure and within the agreed timelines. Backup environments themselves should be isolated from everyday production administrative accounts to prevent attackers from disabling or encrypting them during a breach. Finally, ransomware readiness should be embedded into executive-level simulations through tabletop exercises that test decision-making under stress.

Your organization's backup strategy should never stand alone; it must be tightly aligned with broader business continuity planning so that recovery efforts support the organization's most critical operations when it matters most.

For instance, in certain ransomware instances, companies knowingly choose to pay their ransom as their recovery strategy. If that is the case at your company, it is recommended to check the deductible of your cyber insurance policy, what services are covered, and whether you are limited to a specific incident response firm. It is your responsibility to document and communicate the risk, as there is no guarantee the data would be actually restored.

Note

When cybersecurity executives adopt a lifecycle perspective, they move beyond checkbox security. They create layered, adaptive protection that reflects how data actually moves and evolves inside the organization.

While backups and recovery capabilities help organizations restore operations after an incident, resilience also depends on the security of the partners, vendors, and service providers that support the business. As organizations increasingly rely on third parties for cloud services, software, managed services, and critical business functions, their security posture becomes closely intertwined with your own. For a security executive, protecting the organization means looking beyond internal systems and extending risk management to the broader ecosystem in which the business operates.

Managing third-party and supply chain risk

If you ask most boards what keeps them up at night, supply chain risk is near the top of the list, and for good reasons. Some of the most damaging security incidents in recent years did not start inside the organization at all. They started with a vendor, a software provider, a managed service partner, or a compromised update mechanism.

Modern enterprises do not operate alone. They are deeply interconnected ecosystems of cloud providers, SaaS platforms, payment processors, logistics partners, consultants, outsourced developers, and managed security providers. Every integration, every API connection, and every shared dataset increases business capability but also expands the attack surface.

Each third party introduces risk in at least one of four ways, as shown in *Figure 7.6*:

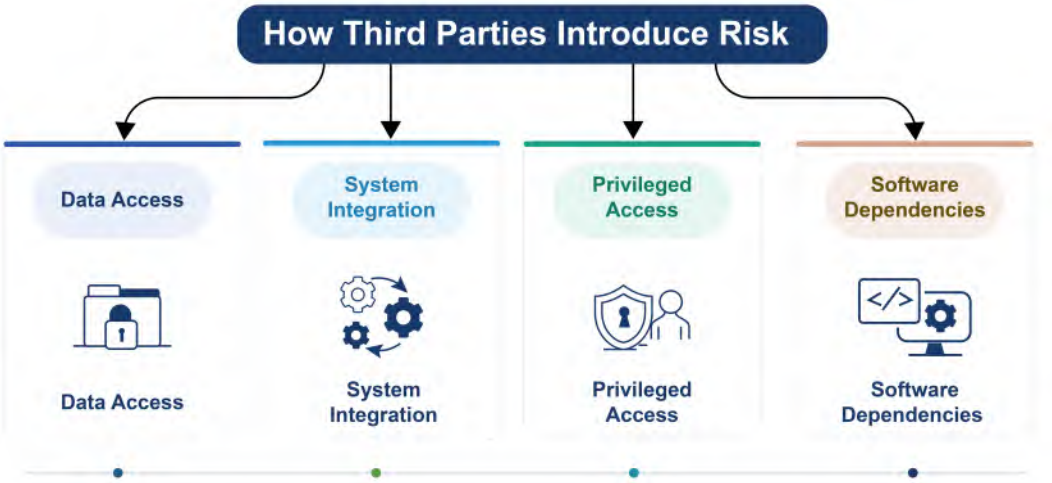


Figure 7.6 – Third-party risks

Third-party risk extends well beyond the security posture of a vendor. The relationship itself often creates new paths that attackers can exploit. As organizations increasingly rely on cloud providers, software vendors, managed service providers, and business partners, security executives must understand the different ways these relationships can introduce risk. They must also ensure that appropriate controls are in place.

One common risk vector is data access. Vendors frequently require access to sensitive business information to deliver their services, whether it is customer data, financial records, intellectual property, or operational information. Before granting access, organizations should ensure that the vendor receives only the minimum data necessary to perform its function, that the data is protected through encryption and appropriate access controls, and that contractual agreements clearly define how the data will be used, stored, retained, and securely deleted.

A second risk vector is system integration. Modern business applications rarely operate in isolation. Third-party solutions often integrate directly with identity providers, cloud platforms, enterprise applications, and APIs to exchange data or automate business processes. While these integrations improve efficiency, they also expand the organization's attack surface. Security executives should ensure that integrations use secure communication channels and strong authentication mechanisms, and that they are periodically reviewed to confirm they remain necessary and appropriately configured.

Another significant area of concern is **privileged access**. Some vendors require administrative or elevated privileges to support systems, perform maintenance, or troubleshoot issues. If these accounts are compromised, attackers may gain broad access to the organization's environment. To reduce this risk, privileged access should follow the principles of least

privilege and JIT access whenever possible, with all privileged activities logged, monitored, and reviewed regularly.

Finally, organizations should carefully manage **software dependencies**. Commercial software, open-source libraries, and third-party components have become integral parts of modern applications. Vulnerabilities within these dependencies can quickly become organizational risks, even if the organization's own code is secure. Security leaders should establish processes to inventory software dependencies, monitor newly disclosed vulnerabilities, validate software updates, and understand how critical third-party components support key business services.

Taken together, these risk vectors demonstrate why third-party risk management extends beyond completing vendor questionnaires. Effective governance requires continuous visibility into how third parties access data, integrate with systems, receive privileged access, and contribute software to the organization's technology ecosystem. By understanding these relationships, security executives can better prioritize controls that reduce supply chain risk while enabling the business to continue benefiting from trusted external partners.

When you connect to a vendor, you are implicitly extending trust. That trust might be justified, but it must be governed. Executives often assume that if a vendor is large or well-known, it is secure. However, reputation is not a control. Even highly mature organizations experience breaches.

Cybersecurity leaders should help the organization to switch the mindset that treats third-party risk as an extension of enterprise risk instead of as an isolated IT function. The following table lists action items that should be considered:

Actionable Item	**Description**
Create a centralized inventory of third parties	You cannot manage risk if you cannot enumerate. Work with procurement and finance to build a living inventory of vendors, SaaS providers, and partners.
Categorize vendors by risk tier	Not all vendors are equal. Classify them based on data sensitivity handled, level of system integration, privileged access requirements, and regulatory impact.
Map data flows	Document where sensitive data flows to external entities. Include APIs, batch transfers, and integrations.

Table 7.6 – Action items to incorporate third-party risk as part of enterprise risk

Fourth-party risk

Most security executives are familiar with the concept of third-party risk. A new category has emerged over the last few years. **Fourth-party vendor risk** refers to the exposure an organization inherits from the vendors used by its own third-party providers. Even when a company has strong oversight of its direct suppliers, those suppliers often rely on their own subcontractors for cloud hosting, analytics, software components, or specialized services. Each of these downstream entities can introduce vulnerabilities or weak security practices that ultimately affect the organization's data and operations. Because these relationships are often opaque, security executives might have limited visibility into who these fourth parties are, what data they access, or how well they protect it.

Additionally, the rise of artificial intelligence has amplified this challenge. For example, a payroll provider (your third-party vendor) might use an external AI service to analyze employee data for fraud detection or anomaly spotting. That AI service—your fourth-party vendor—may store or process sensitive information in ways that you never directly approved. If the AI provider suffers a breach, misconfigures its model-training environment, or uses the data for unintended purposes, your organization still bears the impact despite having no direct contractual relationship. This illustrates why modern supply-chain security requires not only evaluating third-party controls but also demanding transparency into the AI tools and subcontractors embedded within their services.

You can address this exposure by requiring security and AI-specific addendums in all third-party contracts that obligate vendors to disclose and manage their own critical subcontractors. These addendums should mandate transparency into any AI tools or model-training environments used by fourth parties, along with enforceable requirements for data handling, security controls, and incident notification. This ensures that even when your vendors rely on AI-driven services, the downstream risks remain governed, auditable, and contractually enforceable.

Identity and access risks in the supply chain

Earlier in this chapter, we stated that identity is the new perimeter. Within this context, you can affirm that third-party identities are often the weakest gate. Vendor access frequently becomes a blind spot because it does not fit neatly into internal HR-driven identity governance processes. Contractors, consultants, and service accounts might be provisioned quickly to meet business deadlines and rarely reviewed afterward. The most common identity risks in vendor relationships are:

- Shared vendor accounts are used by multiple individuals.
- Excessive permissions granted "temporarily" and never removed.

- Long-lived service accounts with broad access.
- Limited visibility into which vendor employee accesses systems.
- Weak MFA enforcement for third-party users.

These gaps create ideal entry points for attackers. If a vendor's internal security fails, its compromised credentials may become your problem. Apply Zero Trust principles to vendor access: verify explicitly and grant no implicit trust based on the vendor relationship. Vendor identity and access should follow the same discipline as internal privileged access, which includes applying the principles of least privilege, ensuring that identities are time-bound, enforcing strong authentication, and ensuring that logging and monitoring are enabled for these identities.

Cybersecurity leaders should educate the organization that there is no security justification for giving vendors broader access than employees. The following table has a list of action items that should be considered:

Actionable Item	**Description**
Prohibit shared accounts	Require named accounts for all third-party users.
Enforce strong authentication	Apply MFA and conditional access policies to vendor identities.
Implement JIT access	Provide elevated access only when needed and automatically revoke it.
Conduct periodic access review	Business owners should attest to continued necessity of vendor access.
Log and monitor vendor activity	Integrate third-party access monitoring into the SOC's standard workflow.
Secure BYOD environments	Enforce device compliance checks, require **mobile device management (MDM)** enrollment, and restrict access from unmanaged or non-compliant personal devices.

Actionable Item	Description
Control VDI access	Route vendor and high-risk third-party access through hardened VDI environments. The hardening should include session recording, clipboard restrictions, and data exfiltration controls.

Table 7.7 – Action items for least privilege

Effective governance begins before a contract is signed, with a thoughtful risk assessment that evaluates how the vendor will access data, integrate with systems, and impact regulatory exposure.

A vendor questionnaire completed during onboarding might provide a snapshot, but it does not equal ongoing assurance. Not all third parties present the same level of risk, which is why many organizations classify vendors into tiers based on factors such as the sensitivity of the data they access, the level of system integration, the privileges they receive, and how critical they are to business operations. While the naming convention varies across organizations, **Tier 0** vendors typically represent the highest-risk or most business-critical relationships, whereas **Tier 3** vendors generally have limited access to systems or sensitive information and pose lower overall risk. This classification helps organizations prioritize their risk management efforts and allocate resources where they will have the greatest impact.

Once vendors are classified, the depth and frequency of security assessments should reflect their risk tier. Tier 0 vendors may require comprehensive due diligence before onboarding, annual or continuous security reviews, periodic evidence of control effectiveness, executive oversight, and close monitoring of significant security changes or incidents. By contrast, applying the same level of rigor to every Tier 3 vendor would consume valuable resources without meaningfully reducing organizational risk. Lower-risk vendors might only require a basic security review during onboarding and periodic reassessment thereafter. A risk-based approach allows the security team to focus its efforts on the third parties that could have the greatest impact on the organization's operations, data, or customers.

From there, security expectations must be written clearly into the contract itself, including specific data protection standards, encryption requirements, defined breach notification timelines, and coordinated incident response responsibilities. Contracts should also include the right to audit and transparency around subcontractors, so there are no surprises about who else might be handling your data.

Supply chain risk management is not something cybersecurity can carry alone. It is, by nature, cross-functional. None of the above approaches can work in isolation. Legal and procurement

teams must be active partners to ensure that security commitments are enforceable and aligned with the organization's broader risk posture. Further, procurement plays a critical role in enforcing contractual standards and ensuring vendors cannot bypass required security language. Legal teams define liability boundaries and compliance obligations, shaping how risk is shared and managed. Privacy professionals evaluate data transfer implications, particularly when regulated or cross-border data is involved.

Business leaders, for their part, must validate whether a vendor is truly necessary and explicitly accept any residual risk when security gaps cannot be fully closed. When these functions work together, third-party governance becomes a structured business discipline rather than a paperwork exercise. The following table has a list of action items that should be considered by cybersecurity leaders:

Actionable Item	**Description**
Define third-party incident playbooks	Include escalation paths and decision-making authority.
Test vendor breach scenarios	Conduct tabletop exercises that simulate supplier compromise.
Predefine communication strategies	Align legal, PR, and executive messaging in advance.
Maintain rapid access revocation capabilities	Ensure vendor accounts can be disabled immediately.
Review data minimization practices	The less sensitive data vendors hold, the lower the impact of compromise.

Table 7.8 – Action items for third-party governance

Summary

In this chapter, you learned that protecting your organization's "crown jewels" begins with clarity. Before investing in tools or launching new initiatives, leaders must agree on what truly matters: the identities that grant access, the sensitive data that fuels the business, the intellectual property that differentiates it, and the systems that keep operations running. You saw that most breaches, regardless of how they start, ultimately come down to failures in identity control or data protection. You also learned that safeguarding these assets is not a technical delegation exercise; it is an executive responsibility. Governance, prioritization,

funding, and cross-functional alignment all sit at the leadership level. When executives treat identity and data as strategic assets rather than IT concerns, the organization's security posture changes fundamentally.

You also learned that identity has become the modern security perimeter. In cloud-first and SaaS-driven environments, network boundaries no longer define trust; authentication, authorization, and continuous validation do. This chapter walked you through how unmanaged identities, privilege creep, and overlooked service accounts quietly increased risk over time, and why mature IAM, least privilege, just-in-time access, and privileged access management are essential risk controls. It reframed Zero Trust as an operating model grounded in verifying explicitly and assuming breach, not as a product to purchase. On the data side, you learned that protection starts with understanding what you have, classifying it in practical ways, and assigning clear ownership. From encryption governance and DLP to backup resilience and ransomware readiness, data protection was positioned as a business continuity strategy. Finally, this chapter highlighted how third parties and supply chain relationships extend your attack surface, reinforcing that vendor access, contractual governance, and ongoing oversight are critical components of protecting what matters most.

Protecting identities, controlling access, securing data, and managing third-party risk are some of the most important responsibilities of a security organization, but technology alone is not enough to sustain these efforts. Lasting security requires clear governance, well-defined accountability, consistent decision-making, and a shared understanding of risk across the organization. As a security executive, you will quickly discover that many of the most important decisions are not about selecting the right security control; they are about balancing business priorities, regulatory obligations, operational realities, and organizational risk. The need for a decision framework is where governance, risk, and compliance (GRC) becomes essential. In *Chapter 8*, you will explore how to establish governance structures, build an effective risk management program, develop meaningful policies and standards, and create the decision-making framework that enables security to support the business while managing risk effectively.

Additional resources

- IDC Report: `https://bit.ly/CISOBook19`

8

Navigating the Landscape: Governance, Risk, and Compliance (GRC)

By the time you reach this chapter, you have already assessed the organization, built relationships, established credibility, evaluated your security posture, and started shaping strategy. **Governance, risk, and compliance (GRC)** is where many of those efforts begin to converge. While some executives view GRC as a collection of audits, policies, and regulatory obligations, experienced leaders understand that GRC is really about decision-making. It provides the structure that helps organizations make consistent, defensible, and risk-informed decisions.

Earlier in the book, we discussed understanding the business, identifying crown jewels, assessing culture, and creating alignment with stakeholders. GRC builds upon those foundations. Without understanding the business, risk decisions lack context. Without relationships, policies become documents that no one follows. Without strategy, compliance becomes a checkbox exercise disconnected from business outcomes.

The role of a security executive is not to eliminate all cyber-related risk. That is impossible. The role is to help the organization understand risk, make informed decisions, and document those decisions in a way that provides a valid paper trail both in-house and externally facing. In this chapter, we will explore the following topics:

- GRC as a leadership function
- Considerations regarding risk management
- Compliance as a baseline, not the finish line

GRC as a leadership function

One of the first mindset shifts you need to make as a security executive is moving from seeing GRC as a back-office function to seeing it as a leadership capability. GRC answers questions that are deeply connected to how your organization operates. "*What are our greatest risks? Who can accept risk? Who owns remediation? What is the escalation path when teams disagree? What evidence is required to prove that a control is working? How does the company determine whether an incident must be reported?*"

These questions cannot be answered by technology alone. For instance, a vulnerability management platform may tell you that a critical vulnerability exists, but it will not decide whether a production system can be taken offline during a revenue-critical period. A data discovery tool may identify sensitive data, but it will not decide whether a business unit has the right to keep collecting it. Those are governance decisions.

When governance is missing, security teams often become the default owner for every uncomfortable decision. That may feel empowering at first, but it is neither scalable nor sustainable. A mature governance model clearly defines decision ownership, ensuring that responsibilities are shared across the organization rather than concentrated within the security team.

In many cases, security has both the authority and the responsibility to make decisions related to the security program itself, such as establishing technical standards, deploying protective controls, or responding to active threats.

Business decisions, however, are different. When a decision involves accepting risk, balancing security against cost or time-to-market objectives or determining whether a business objective justifies a particular level of risk exposure, the ultimate decision should rest with the appropriate business owner. Security provides the expertise, explains the risks and potential consequences, recommends a course of action, and ensures the decision is properly documented and, when necessary, escalated through the appropriate governance channels. Understanding this distinction is fundamental to effective governance.

Note

Security owns the security program. The business owns business risk. The most successful organizations bring both groups together to make informed decisions that balance protection with business objectives.

A well-designed GRC program creates shared accountability by establishing clear decision-making processes, defined ownership, and documented risk acceptance. Note that this program does not eliminate disagreements between security and the business, nor does it prevent the business from viewing security as an obstacle when priorities conflict. Instead, it creates a structured governance process that requires those conversations to happen openly and ensures that the rationale behind risk decisions is documented.

Rather than allowing security to become "the team that simply says no" or the business to quietly accept risk without visibility, governance brings the appropriate stakeholders together. The goal is to discuss the trade-offs between risk, business value, speed, compliance, customer trust, and operational impact. For instance, if a business chooses to accept a risk after understanding the potential consequences, effective GRC ensures that its decision is:

- Documented
- Assigned to the appropriate risk owner
- Escalated through the organization's governance process (if needed)

This process is captured in *Figure 8.1*:



Figure 8.1 – What GRC delivers

This kind of paper trail creates accountability and provides valuable context for future audits, regulatory reviews, incident investigations, and executive discussions. Additionally, a security executive earns credibility by ensuring every significant risk decision is informed, transparent, and made through the appropriate governance channels.

Now, if you step back, you will realize that risk management is the foundation of GRC. Without a consistent way to identify, evaluate, treat, and monitor risk, the organization will make decisions based on personal preference, urgency, politics, or whoever speaks the loudest in the meeting. While a framework might not remove judgment, it will create consistency around how judgment is applied.

Many organizations use established models such as NIST, ISO, **Factor Analysis of Information Risk (FAIR)**, **Committee of Sponsoring Organizations of the Treadway Commission (COSO)**, or internal enterprise risk management methodologies. In most cases, your first step should be to understand whether the company already has an enterprise risk framework. If one exists, align cybersecurity risk management to it instead of building a completely separate process. This will help you integrate with the broader risk organization and avoid creating a parallel universe that executives struggle to understand.

The framework you choose should be simple enough to use and strong enough to defend. If the model requires months of training before teams can document a risk, it is probably too complicated. If the model produces vague risk statements that cannot be mapped to business impact, it is probably too shallow. The right balance depends on the organization, but the framework should always support decision-making. Consider two different approaches. In one organization, every new risk must go through a lengthy assessment requiring dozens of fields, multiple scoring models, and approvals from several committees before it can even be added to the risk register. As a result, teams delay documenting risks because the process is too time-consuming. In another organization, risks are simply described as "high," "medium," or "low," with little explanation of the business impact, affected assets, or proposed mitigation. When executive leadership reviews the risk register, they have no clear basis for prioritizing investments or making informed decisions. Neither approach is effective. The goal is to adopt a framework that is simple enough for teams to use consistently while providing enough structure and context to help leaders understand the business impact, prioritize remediation efforts, and make defensible risk decisions.

Developing security policies and standards

Policies are one of the primary mechanisms through which governance becomes operational.

Policies and standards communicate expectations, define responsibilities, and provide a basis for accountability. Think of policies as management's written expression of intent. They communicate how leadership expects the organization to operate. Standards translate that intent into specific requirements. Procedures then explain how those requirements are executed on a day-to-day basis. A simple way to think about the relationship is shown in *Figure 8.2*:

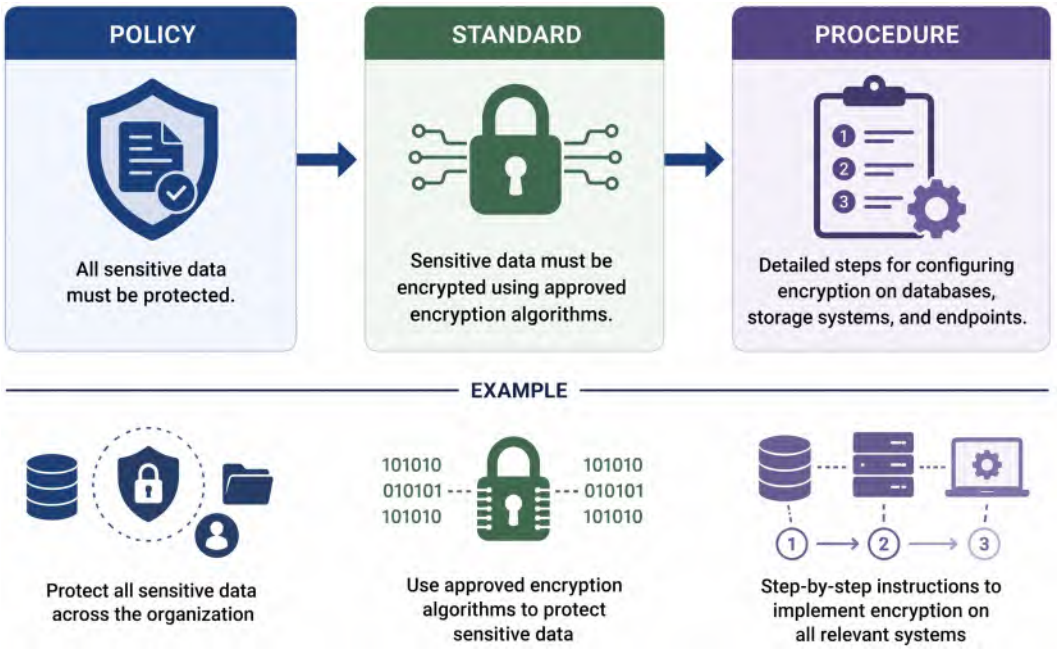


Figure 8.2 – Correlation between policy, standard, and procedure

Policy development should not happen in isolation. Security may draft the content, but legal, HR, privacy, compliance, technology, and business stakeholders should review it.

Note

In today's world with AI, it is easy to update policies to align with risk standards. Most organizations that already have policies have established a review cadence.

This does not mean every stakeholder gets to dilute the policy until its requirements become so broad or ambiguous that they are difficult to implement or enforce. It means the policy must be operationally realistic, legally sound, and aligned with how the business works.

Keep policies clear by avoiding unnecessary jargon. Define terms and state who owns the policy, who it applies to, what is required, how exceptions are handled, how often the policy is reviewed, and what happens when requirements are not followed. Consider the difference between a poorly written policy and an effective one. A policy that states, "Users should use strong passwords whenever possible," leaves too much room for interpretation. What qualifies as "strong"? When is it not possible? Who determines compliance? By contrast, a clearer policy might state, "*All workforce users must authenticate using MFA. Passwords must comply with the organization's password standard, and exceptions require documented approval from the information*

security team." Similarly, a statement such as "*Sensitive data should be protected*" provides little guidance, whereas "*Confidential and restricted data must be encrypted at rest and in transit using approved encryption standards, and access must be limited to authorized users based on business need*" clearly communicates the expectation, identifies the applicable data, and establishes how compliance can be evaluated. Well-written policies eliminate ambiguity, making them easier to implement, audit, and consistently enforce across the organization.

Many organizations struggle because they blur the boundaries between policies, standards, and procedures. Security teams often write highly technical policies that should have been standards or procedures instead. The result is a policy document that nobody outside the security team can understand.

For example, a policy might state that "*All sensitive data must be encrypted to protect the confidentiality and integrity of organizational information.*" That establishes the organization's expectation and applies broadly across the business. A standard would then specify the approved encryption algorithms, minimum key lengths, and technologies that must be used to meet the policy. Finally, a procedure would provide the step-by-step instructions for enabling encryption on databases, cloud storage accounts, laptops, or other systems. If the policy instead included algorithm names, configuration settings, or implementation steps, it would become unnecessarily technical and difficult to maintain as technologies evolve. Keeping policies focused on *what* must be achieved, while standards and procedures define *how* it is achieved, makes the governance framework easier to understand, implement, and update.

As part of your governance framework, establish a formal policy hierarchy. While the exact structure may vary, most mature organizations maintain the levels shown in the following table:

Document Type	**Purpose**	**Audience**
Policy	Defines management intent and expectations	Entire organization
Standard	Defines mandatory requirements	Control owners and technical teams
Procedure	Defines how activities are performed	Operational teams
Guideline	Provides recommended practices	Broad audience

Table 8.1 – Types of documents and their purposes

Another common mistake is writing policies for auditors instead of employees, often using overly legalistic or excessively technical language. Auditors may review policies, but employees are the people expected to follow them. If the language is inaccessible, adoption suffers.

Another important aspect of a mature governance program is measuring policy effectiveness. However, it is rarely something you can fully accomplish during your first year as a security executive. At this stage, your priority should be understanding the organization's existing policies, identifying obvious gaps, establishing ownership, and putting the right governance processes in place.

Tip

Think of your first year as laying the foundation rather than trying to optimize every aspect of the program.

As you become more familiar with the organization, begin identifying a small set of indicators that can help measure whether policies are having the intended effect. For example, if your organization introduces a policy requiring MFA for privileged accounts, simply measuring policy compliance may not tell the whole story. You should also track indicators such as the percentage of privileged accounts protected by MFA, the number of authentication-related security incidents, the number of approved policy exceptions, and findings from access reviews. Together, these metrics provide a better indication of whether the policy is being consistently implemented and whether it is achieving its intended objective of reducing identity-related risk.

You do not need a sophisticated dashboard on day one. Instead, start collecting information that will allow you to establish a baseline and identify trends over time. Some useful questions to begin exploring include:

- Do employees understand the intent behind the policy requirements?
- Are policy exception requests increasing or decreasing?
- Are the same policy violations occurring repeatedly?
- Do internal or external audits consistently identify the same control deficiencies?
- Have security incidents revealed gaps between documented policies and actual practices?

You may not have all the answers during your first year, and that is perfectly normal. The goal is to establish a process for continuously evaluating policy effectiveness rather than assuming that publishing a policy automatically changes behavior. As your governance program matures and more operational data becomes available, these indicators will help you determine which

policies are driving the desired outcomes and which ones need to be updated, clarified, or reinforced through additional training and communication.

Policy development checklist

Before publishing or materially changing a security policy, validate the following checklist:

- Business objective and policy purpose are clearly defined.
- The scope identifies who and what the policy applies to.
- Policy owner and approving authority are documented.
- Legal, privacy, compliance, HR, and relevant business stakeholders have reviewed the content.
- Regulatory and contractual obligations were mapped where applicable.
- Language avoids unsupported absolutes unless intentionally required.
- The exceptions process is defined, including approval authority and expiration dates.
- Enforcement expectations are clear and realistic.
- Operational standards or procedures exist to support implementation.
- Review cadence is documented, usually annually or when major changes occur.
- Communication and training plans are prepared before publication.
- Metrics exist to measure adoption, compliance, and effectiveness.

Considerations regarding risk

During your first year, risks will come from many places. Some will appear during the listening tour, and others will come from vulnerability assessments, penetration tests, audits, incident reports, threat intelligence, architecture reviews, privacy assessments, vendor reviews, and customer requirements. The challenge is organizing risks in a way that allows your organization to act.

Also, it is important to emphasize that you should not treat every finding as a risk. A finding is an observation, and a risk explains why the observation is important. For example, "server X is missing patches" is only a finding. A stronger risk statement would be "Because internet-facing systems supporting the customer portal are missing critical patches, there is an increased likelihood of unauthorized access that could disrupt customer transactions and trigger contractual or regulatory notification obligations." The second version connects the condition to the business consequence. This distinction matters because executives make decisions based on consequences rather than technical detail. You may care about the vulnerability identifier, the affected package, and the exploitability score, but your executive team cares

about revenue impact, customer trust, operational resilience, legal exposure, and reputational damage. Your job is to translate that without oversimplifying.

Tip

A helpful tip is to write risk statements using a consistent pattern: [business impact] could occur if [threat event] were to exploit [condition].

Risk appetite and risk tolerance

Risk appetite defines the amount and type of risk an organization is willing to pursue or retain in support of its objectives. Risk tolerance is more specific. It defines the acceptable variation around a particular objective or metric. These concepts may sound theoretical, but they become very practical during real decisions.

Consider a company preparing to launch a new digital product. The product team wants speed, but the security team has identified weaknesses in authentication, logging, and data handling. Meanwhile, the legal team is worried about privacy commitments and the finance team is focused on quarterly revenue. Finally, the CEO wants to meet the market window. Without a defined risk appetite, the discussion can quickly become subjective, with decisions driven by individual opinions rather than an agreed-upon framework for balancing business opportunity and risk. With a defined risk appetite, leaders can evaluate the decision against agreed principles.

As a new security executive, do not assume that your personal tolerance for risk is the same as the organization's tolerance for risk. This is a common trap. Many security leaders come from technical backgrounds where the instinct is to reduce risk as much as possible. That instinct is valuable, but executive leadership requires a broader view. The organization may decide to accept certain risks because the business opportunity is significant. Your responsibility is to ensure the risk is understood, documented, approved by the right authority, and monitored. You should facilitate risk appetite conversations with senior leadership and the board. Start with business scenarios rather than abstract definitions. Ask the following questions:

- What level of downtime is acceptable for critical systems?
- Would the company delay a product launch for unresolved security issues?
- Which data types are considered most sensitive?
- What types of regulatory exposure are unacceptable?

The answers will help you shape practical thresholds.

Once these discussions take place, document the outcomes and translate them into actionable governance artifacts. The agreed-upon risk appetite should not remain as meeting notes or

presentation slides. It should be reflected in your risk management framework, risk scoring methodology, policy exceptions process, and decision-making criteria. For example, if leadership determines that customer-facing services can tolerate no more than one hour of unplanned downtime, that threshold should influence resilience investments, disaster recovery objectives, and incident response priorities. Similarly, if the organization identifies customer data as its highest priority, that decision should be reflected in data protection controls, monitoring capabilities, and investment planning. As the business evolves through acquisitions, new products, or changes in strategy, revisit these conversations periodically to ensure that the organization's stated risk appetite continues to align with its business objectives and the current threat landscape.

The risk register as a system of accountability

The risk register is often one of the most misunderstood artifacts in a GRC program. In weak programs, it becomes a spreadsheet where risks go to be archived. In mature programs, it becomes a system of accountability. It shows what risks exist, who owns them, what is being done, what decisions were made, and whether the residual risk is acceptable.

Ownership is the most important field in the risk register. Security may identify a risk, but the business usually owns the consequence. For instance, if a payment platform has a resilience issue, the business owner of the payment process must be part of the decision. If a development team is not meeting secure coding requirements, engineering leadership must own the remediation plan. *Security cannot own every risk simply because the word security appears in the description.*

A risk register should be reviewed on a regular cadence by the appropriate stakeholders. At a minimum, individual risk owners should periodically review the risks assigned to them to validate their status, reassess likelihood and impact, and update remediation plans. Consider the following approaches for critical, high, and low risks:

- **Critical risks** may require executive leadership attention or escalation to the board, depending on the organization's governance structure.
- **High risks** should also be reviewed by the cybersecurity leadership team or the organization's risk committee.
- **Lower risks** may be reviewed quarterly as part of routine governance activities.

The cadence should reflect the severity, business impact, and remediation timeline. What matters is that the risk does not disappear after the initial conversation but remains visible until it is mitigated, formally accepted, transferred, or closed through the organization's governance process.

Third-party and contractual risk

Build on the supplier assessments, access controls, and contractual protections discussed in *Chapter 7*. Review termination provisions with legal and procurement teams as part of the organization's contractual risk assessment.

Third-party risk should also be integrated into the risk register. If a vendor presents residual risk that exceeds tolerance, the business sponsor should own the decision. Procurement, legal, security, and the business must work together. Security can recommend controls, but the business must understand the dependency. The following table shows an example of risk register fields:

Field	Purpose	Practical Guidance
Risk ID	Creates a unique reference for tracking and reporting	Use a consistent naming convention such as CYR-2026-001.
Risk statement	Explains condition, threat events, and business impact	Avoid purely technical findings; connect to operational, financial, legal, or reputational consequences.
Business owner	Identifies who owns the decision and outcome	Security may identify the risk, but the affected business function should usually own it.
Likelihood and impact	Supports prioritization and comparison	Use defined criteria so scoring does not change based on personal preferences.
Current controls	Documents existing safeguards	Be factual; do not overstate control effectiveness.
Treatment plan	Explains mitigation, transfer, avoidance, or acceptance	Include milestones, dependencies, and target dates.

Field	Purpose	Practical Guidance
Residual risk	Shows what remains after treatment	Residual risk should be explicitly accepted when above tolerance.
Approval history	Records who approved decisions and when	This is especially important for exceptions and risk acceptance.

Table 8.2 – Risk register fields

Self-identified risks

One of the signs of a mature security program is that it consistently identifies its own risks before someone else does. During your first year, you should not view audits, regulatory assessments, or customer reviews as the primary mechanism for discovering weaknesses. These activities provide valuable independent validation, but they should confirm what you already know and not surprise you.

There is an important leadership benefit to proactively identifying risks. When your team documents a significant risk before an internal audit, external auditor, regulator, or customer discovers it, you demonstrate that your governance processes are working. You also have the opportunity to explain the context, describe the remediation plan, identify the business owner, and communicate the expected timeline for resolution.

This does not mean every audit finding represents a failure. Independent assessments often bring valuable perspectives and identify opportunities for improvement that internal teams may overlook. However, over time, your objective should be to reduce the number of significant findings that are first identified by external parties.

Roles and responsibilities

As your governance program matures, clearly defining responsibilities becomes just as important as identifying risks. One framework that many organizations adopt is the *Three Lines of Defense* model, which is represented in *Figure 8.3*:

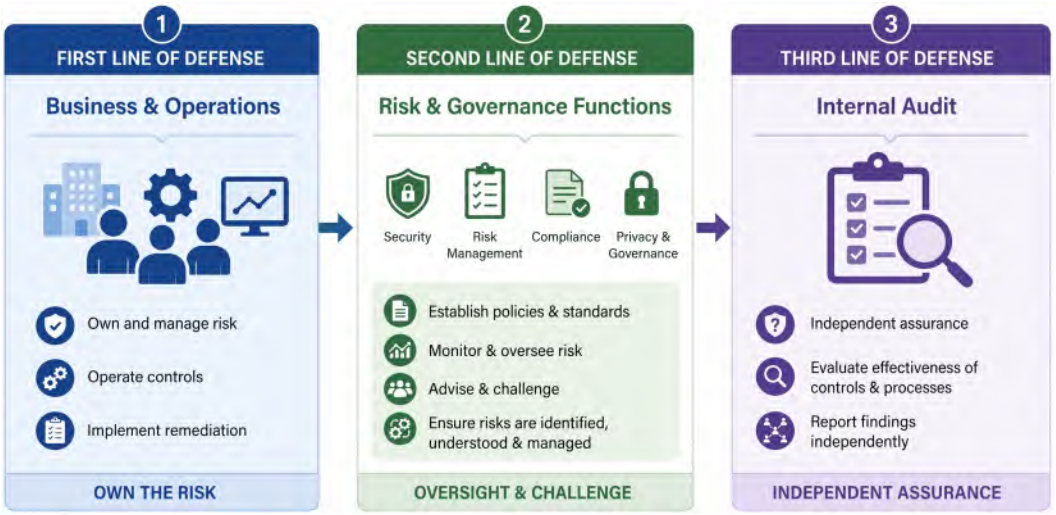


Figure 8.3 – Three Lines of Defense

The *first line of defense* consists of the business and operational teams. They own the processes, systems, and day-to-day activities that create or manage risk. They are responsible for operating controls, addressing identified risks, and implementing remediation plans. In other words, they own the risk because they own the business process.

The *second line of defense* includes functions such as information security oversight, enterprise risk management, compliance, privacy, and other governance teams. Their role is to establish policies, define standards, provide oversight, advise the business, monitor risk, and challenge whether controls are operating effectively. Security executives may have first-line responsibilities for operating controls, second-line responsibilities for oversight and challenge, or both, depending on the organization's operating model. Define these responsibilities explicitly.

The *third line of defense* is internal audit. Unlike the first two lines, Internal Audit operates independently and provides objective assurance that governance processes and controls are functioning as intended. Internal Audit should not be designing controls or managing risks; its role is to evaluate whether the first and second lines are effectively fulfilling their responsibilities.

Understanding these roles helps prevent one of the most common governance mistakes, which is assuming that security owns every cybersecurity risk. Security owns the security program. The business owns business risk. Internal Audit provides independent assurance, while external parties validate the organization's overall effectiveness.

Measuring what matters most

As your risk management program matures, the risk register should become more than a repository of individual risks. It should provide meaningful metrics that help leadership understand how the organization's overall risk posture is evolving.

Rather than reviewing risks one at a time, establish a regular cadence with risk owners to review trends across all major security domains, such as identity, endpoint security, cloud security, application security, data protection, third-party risk, resilience, and compliance. These reviews create accountability while also helping identify systemic issues that affect multiple business areas.

Examples of useful risk management KPIs include:

- Number of critical risks by security domain
- Percentage of high-risk items with approved remediation plans
- Percentage of risks with identified business owners
- Number of risks accepted versus mitigated
- Average age of high-risk findings
- Percentage of overdue remediation activities
- Number of policy exceptions by business unit
- Third-party risks exceeding the organization's risk tolerance
- Trends in residual risk over time

These metrics should not be collected simply because they are easy to measure. Each KPI should help answer a question that leadership cares about: *Are we reducing our overall exposure? Are we making progress on our highest priorities? Are risk owners taking action?*

For example, if the percentage of critical business systems meeting vulnerability remediation objectives declines from 92% to 78%, establish why performance deteriorated, confirm the responsible owner's corrective plan, and escalate decisions beyond that owner's authority. Chapter 9 explains how to present these trends to executives and the board.

Compliance as a baseline

Compliance is necessary, but it is not the same as security. Many organizations have learned this lesson the hard way. They passed audits, maintained certifications, and still experienced significant incidents. Compliance only tells you whether certain requirements were met at a particular point in time. Security asks whether the organization is resilient against the threats it actually faces.

That said, do not dismiss compliance. Compliance requirements often create useful baselines, executive attention, and funding justification. They can also force discipline in areas that might otherwise be ignored. For example, a regulatory requirement to perform annual access reviews may initially be viewed as a compliance exercise. However, organizations often discover inactive accounts, excessive privileges, or users who have retained access after changing roles. Addressing these findings not only satisfies the regulatory requirement but also strengthens identity security and reduces the risk of unauthorized access. Similarly, requirements to maintain audit logs or test backup and recovery processes frequently improve incident response capabilities and operational resilience. In these cases, compliance serves as the catalyst, but the organization ultimately gains meaningful security improvements that extend well beyond passing an audit.

The key is to avoid treating compliance as the final objective; instead, use it as a foundation.

It is important to emphasize that compliance is usually the responsibility of the **chief compliance officer (CCO)**. If the company is too small, this function usually sits under legal. Enterprise-wide compliance requires expertise across legal, regulatory, and business domains. However, the security executive must work closely with the CCO.

With that in mind, you should identify the regulations, contractual commitments, industry standards, customer requirements, and internal policies that apply to your environment. Examples (since the exact list depends on the business) may include the following:

- Privacy regulations
- Financial sector requirements
- Healthcare obligations
- Payment card requirements
- Public company disclosure rules
- Government contract requirements
- Regional breach notification laws

Once obligations are identified, map them to controls. A single control may satisfy multiple requirements. For example, centralized logging may support incident response, audit requirements, regulatory investigations, and customer assurance. Mapping obligations to controls reduces duplication and helps you demonstrate that investments serve multiple purposes.

One practical approach is to create a compliance control matrix. List all applicable regulations and standards across the top and your security controls along the side. As you map them together, you will often discover that many requirements overlap. MFA, for example, may support regulatory requirements, cyber insurance obligations, customer contractual

commitments, and internal security standards simultaneously. This exercise not only reduces duplicated effort but also helps justify investments because you can clearly demonstrate the broad value of each control. The following table presents an example of a compliance control matrix:

Security Control	**NIST CSF**	**ISO 27001**	**GDPR**	**PCI DSS**	**Business Benefit**
Multifactor authentication	X	X	X	X	Reduces unauthorized access and credential theft
Centralized logging & SIEM	X	X	X	X	Improves incident detection, investigation, and reporting
Vulnerability management program	X	X		X	Reduces exposure to known vulnerabilities
Backup and recovery program	X	X		X	Improves business resilience and recovery capabilities

Table 8.3 – Security controls mapping to industry standards; PCI DSS stands for ***Payment Card Industry Data Security Standard***

While *Table 8.3* provides an example of some controls, you can use the following industry standards for a complete list of security controls:

- CIS Critical Security Controls v8: `https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-800-53-rev-5`
- Secure Controls Framework:

```
https://securecontrolsframework.com/start-here/set-theory-relationship-mapping-strm
```

Note

The value of a compliance control matrix is not the spreadsheet itself. The value comes from helping leadership understand that a single security investment often supports multiple business objectives simultaneously.

More recently, a new generation of AI-powered GRC capabilities has begun to emerge. Instead of simply storing compliance information, these platforms use automation and AI agents to actively assist GRC professionals throughout the compliance lifecycle. For example, an AI agent can automatically identify new regulatory requirements, determine which existing controls may already satisfy them, highlight potential gaps, recommend policy updates, assign remediation tasks to the appropriate control owners, and continuously monitor whether evidence is being collected. During an audit, these same capabilities can automatically gather supporting documentation from multiple systems, answer auditor questions based on organizational policies, and prepare evidence packages with minimal manual effort.

This represents an important shift in how organizations approach governance. Instead of spending weeks preparing for periodic audits, GRC teams can move toward continuous compliance, where evidence collection, control monitoring, and regulatory mapping occur throughout the year. Further, security leaders gain better visibility into their compliance posture, auditors receive more consistent evidence, and operational teams spend less time on administrative activities and more time improving security.

As a security executive, you should pay attention not only to the risks addressed by compliance frameworks but also to the risks they do not address. Regulations and industry standards are inherently reactive. They are developed through lengthy legislative, regulatory, and industry processes, often taking years to evolve. By the time a new requirement appears in a regulation, the threat it addresses is usually already well understood by attackers and defenders alike.

This is why compliance should never be your primary source of intelligence for emerging threats. If you are learning about a new risk because a regulator finally included it in a standard, you are already behind. Effective security leaders continuously monitor the threat landscape, technology trends, and changes in the business environment long before they become regulatory requirements.

Quantum computing is an excellent example. While most regulations do not yet require organizations to adopt quantum-resistant cryptography, security leaders should already be evaluating which critical assets depend on today's public-key cryptography, identifying

systems that will require cryptographic agility, and developing long-term migration plans. Waiting until regulations mandate these changes could leave the organization years behind in its preparedness.

Instead of limiting the discussion to "*Are we compliant*?" security leaders should broaden the conversation by asking, "*Are we prepared for the threats most likely to impact our business?*" Those are fundamentally different questions. The first measures whether the organization satisfies a defined set of requirements. The second evaluates whether today's controls can effectively defend against today's and tomorrow's attack techniques.

Note

Approaching security from this perspective often changes priorities. Rather than investing solely to satisfy the next audit or regulatory assessment, organizations begin prioritizing initiatives based on threat intelligence, business risk, and exposure. Compliance continues to provide an important baseline, but strategic investments are driven by the evolving threat landscape, the organization's risk appetite, and the potential business impact of a successful attack. This shift transforms compliance from the primary objective into one of many inputs used to make informed, risk-based security decisions.

Another practical recommendation is to involve compliance, legal, privacy, internal audit, and security teams in periodic control rationalization exercises. Over time, organizations tend to accumulate controls, reports, and assessment activities that no longer provide meaningful value. Some controls become redundant, while others address risks that no longer exist. Periodic reviews help ensure that resources remain focused on controls that reduce meaningful risk rather than simply generating evidence for audits.

If an audit requires evidence collection, use that opportunity to validate operational effectiveness. If a regulation requires annual reviews, expand the review to include emerging threats and business changes. If customers request security assessments, use recurring themes to identify opportunities for program improvement. Every compliance activity should generate value beyond simply satisfying an auditor.

Governance committees

A governance committee gives structure to risk decisions. Depending on the size, industry, and maturity of the organization, cybersecurity may be discussed through one or more governance forums. Some organizations establish a dedicated Cybersecurity Steering Committee or Cyber Risk Committee that focuses exclusively on cyber-related risks and initiatives. Others incorporate cybersecurity into a broader Enterprise Risk Committee or Risk Operating

Committee, where cyber risk is evaluated alongside operational, financial, legal, and strategic risks. At the board level, cybersecurity oversight is commonly assigned to the Audit Committee, the Risk Committee, or a combined Audit and Risk Committee, although some organizations establish a dedicated Technology or Cybersecurity Committee.

Regardless of the committee structure, the objective remains the same: ensure that cybersecurity risks are reviewed by the appropriate stakeholders and that significant decisions are made through a defined governance process.

The committee should include the people who can make decisions or influence action. Depending on its purpose, typical members may include the following:

- Security
- Legal
- Privacy
- Enterprise risk management
- Compliance
- Internal audit
- Technology and infrastructure
- Product or engineering
- Finance
- Human resources
- Representatives from major business units

Note that not every committee needs the same membership. For example, a cybersecurity steering committee may focus on security, technology, legal, and product leaders, while an enterprise risk committee will typically include executives from multiple business functions. Board committees generally receive summarized information from executive management rather than participating in operational discussions.

Each governance forum should have a clearly defined charter that outlines its responsibilities, decision authority, meeting cadence, membership, and escalation process. Operational committees may meet monthly to review remediation progress, policy exceptions, and emerging risks, while executive or board committees often meet quarterly to review the organization's overall cyber risk posture, significant incidents, regulatory developments, and strategic investments.

Each committee's focus should reflect its charter and decision authority, with operational forums managing execution and executive or board forums providing strategic oversight. Typical agenda items include the following:

- Review of significant cybersecurity and enterprise risks
- Progress on risk remediation activities
- Policy exception requests and risk acceptance decisions
- Internal and external audit findings
- Regulatory readiness and compliance status
- Major security incidents and lessons learned
- Third-party and supply chain risks
- Security implications of major business initiatives
- Emerging threats and changes to the organization's risk profile

Tip

Do not build a committee that is too large to function, but do not limit membership so much that decisions lack authority. Effective governance committees are not intended to replace operational decision-making. Their role is to provide oversight, facilitate informed discussions, resolve cross-functional issues, and ensure that significant risk decisions are appropriately documented, approved, and escalated when necessary.

Many of the topics discussed in governance committees have legal and regulatory implications. Decisions involving significant security incidents, potential regulatory reporting obligations, major third-party breaches, policy exceptions, or risk acceptance may require guidance from legal counsel to ensure the organization fulfills its contractual and regulatory responsibilities while protecting its legal interests. As a result, security executives should develop a close working relationship with the legal team long before a crisis occurs.

Attorney-client privilege is often misunderstood. Simply copying a lawyer on an email does not automatically make communication privileged. Privilege rules vary by jurisdiction and context. Work closely with legal counsel to understand how the organization expects sensitive investigations and legal communications to be structured and documented. This is especially important during security incidents, internal investigations, regulatory reviews, and assessments that may uncover significant control deficiencies.

Summary

GRC is not simply about compliance, audits, or policy management. It is the operating system for risk-informed decision-making. It helps the organization understand risk, assign ownership, document decisions, prepare for audits, respond to regulatory obligations, and maintain trust with customers, regulators, executives, and the board.

As a security executive, you do not need to personally own every GRC activity. You do need to understand how the system works and where it is failing. You need to make sure risk decisions are not hidden, policies are not disconnected from reality, audits are not treated as surprises, and regulatory reporting is not improvised during a crisis.

Strong governance protects the organization before incidents occur, during incidents, and long after incidents are over. It gives you a defensible way to explain what was known, what was decided, who approved it, and what actions were taken. In the first year as a cybersecurity executive, that discipline can make the difference between leading with confidence and constantly reacting to chaos.

Strong governance establishes the foundation for informed decision-making, but those decisions only achieve their intended impact when they are communicated effectively. As a cybersecurity executive, your ability to explain risk, justify investments, present security outcomes, and influence stakeholders is just as important as the governance processes you put in place. In the next chapter, we will explore how to communicate cybersecurity in business terms, tailor your message to technical and non-technical audiences, present confidently to executive leadership and boards of directors, and build the communication skills that transform security leaders into trusted business advisors.

Additional resources

Governance and risk management:

- NIST Cybersecurity Framework (CSF) 2.0: `https://bit.ly/CISOBook20`
- NIST SP 800-37 Rev. 2 – Risk Management Framework for Information Systems and Organizations: `https://bit.ly/CISOBook21`

Security governance and controls:

- CIS Critical Security Controls v8: `https://bit.ly/CISOBook22`

Governance, risk, and compliance standards:

- ISO 31000 – Risk Management: `https://bit.ly/CISOBook23`

Board governance:

- National Association of Corporate Directors (NACD) – Cyber-Risk Oversight: `https://bit.ly/CISOBook24`

Part 3

Sustaining and Influencing

This part focuses on the leadership practices that help the program gain momentum across the organization. You'll learn how to engage executives and the board, cultivate shared ownership for security, measure and communicate the program's impact, and protect your capacity to lead. By the end of this part, you'll be equipped to broaden security's reach across the organization, maintain momentum, and remain effective as a leader.

This part of the book includes the following chapters:

- *Chapter 9, Speaking the Language: Mastering Executive Communication and Board Reporting*
- *Chapter 10, Championing Change: Cultivating a Security-First Culture*
- *Chapter 11, Proving Your Impact: Measuring Success and Demonstrating Value*
- *Chapter 12, The Resilient Leader: Sustaining Leadership and Managing Burnout*
- *Chapter 13, Conclusion: Beyond the First Year – A Journey of Continuous Evolution*

9

Speaking the Language: Mastering Executive Communication and Board Reporting

"*The art of communication is the language of leadership*," wrote James Humes. Few areas of a cybersecurity executive's role reflect that more clearly than communicating with senior leaders. As your responsibilities expand, the ability to clearly explain risk, priorities, and progress becomes just as important as building the program itself. Even the strongest security strategy will struggle to gain traction if leaders do not understand why it matters and what decisions it requires.

At the executive level, the conversation shifts. Technical accuracy remains essential, but it is no longer enough. Executives are responsible for business outcomes, which means they need to understand how cybersecurity risks affect operations, customers, revenue, and reputation. The role of the security leader is to translate complex technical realities into clear insights that enable informed decisions.

This chapter focuses on the communication skills required to operate effectively at the executive level. Specifically, this chapter covers:

- Translating security risk into business impact
- Building your reporting framework
- Preparing for executive and board sessions
- Showing up for the meetings

By the end of this chapter, you will have practical tools, templates, and frameworks to help structure executive updates, guide high-stakes discussions, and communicate cybersecurity priorities in a way that drives understanding and action. While you may not control every decision that follows, strong communication ensures that leaders are equipped to make informed choices and that security remains clearly connected to the business it protects.

Translating security risk into business impact

One of the first times I experienced this communication gap was early in my consulting career. During an engagement with a Fortune 500 company, my team and I identified malware on several employee laptops. Excited by the discovery, I requested time with the CISO and walked into his office the same day ready to walk him through everything we had learned: the malware, how it maintained persistence, how it evaded detection, and why we believed it had compromised several endpoints.

After a few minutes, he stopped me and asked a simple question: "*Okay... so what do I do with that?*" The question caught me off guard. From my perspective, I had explained the technical problem clearly. From his perspective, I had not answered the questions that mattered, such as "What does it mean for the business?" or "What decisions do you need from me?"

I experienced similar moments with other executives. Over time, I realized I did not need deeper technical explanations—I needed a different communication playbook.

The purpose of this section is to help you make that same shift. Executive communication should provide clarity and context to support better decision-making. *Table 9.1* highlights common communication habits that become less effective with executive audiences. *Table 9.2* presents practical ways to reframe them.

Common Mistake	**What It Looks Like**
Providing too much technical detail	Diving into tools, CVSS scores, malware behavior, or technical mechanics that obscure the business impact. "This issue has a CVSS score of 8.7 and affects multiple code libraries."
Acting in a defensive way	Focusing on why an issue happened, who made the mistake, or attempting to justify past decisions instead of focusing on the path forward. "The code was pushed without proper review."
Explaining the facts but not the impact	Sharing information without helping leaders understand why it matters or what decisions are required. "The incident impacted our APIs."

Common Mistake	What It Looks Like
Using vague or contextless qualifiers	Using words such as *many, some, more, less, large,* or *small* without enough context to understand the scale or significance. "We have many overdue critical vulnerabilities."
Focusing only on problems	Presenting security as a continuous stream of issues without balancing the discussion with progress, mitigation, or planned actions. "Our environment is vulnerable to ransomware."

Table 9.1 – Common executive communication mistakes

I experienced another version of this challenge later in my career while briefing a group of executives on a critical vulnerability with company-wide impact. I described the situation using language that felt completely natural to me: it was a zero-day, we had compensating controls in place, and many assets were affected. Some people nodded along. As the conversation continued, it became clear that not everyone understood what those terms meant or how concerned they should be.

More importantly, I had not clearly explained what I needed from them. Eventually, one of the executives asked, "What do you want us to do?" That question exposed the real gap in my update. The information was technically accurate, but I had not translated it into the context the audience needed. I should have explained the scale of the exposure, what the compensating controls meant for the remaining risk, and whether I needed a decision, additional support, or simply their awareness.

Recognizing these communication patterns is the first step. The next question is how to reframe those same messages in a way that helps executives understand the business impact and make informed decisions.

Communication Principle	Executive Perspective
Lead with business impact before technical detail	Explain how the issue affects customers, operations, revenue, regulatory obligations, or strategic objectives before discussing the underlying technology. "This vulnerability exposes customer data in one of our internet-facing applications. We have mitigations in place, remediation is underway, and we do not expect customer impact."

Communication Principle	**Executive Perspective**
Focus on accountability and the path forward	Describe what is being done to reduce risk, who owns the response, and if leadership support or decisions are needed. "The issue has been contained, Engineering is deploying the fix, and we expect full remediation by Friday. No executive action is required at this time."
Answer "So what?"	Every update should clearly explain why the topic matters and what action, if any, is expected from leadership. "The incident disrupted a customer-facing service for 30 minutes. Service has been restored, and we are implementing additional controls to reduce the likelihood of recurrence."
Quantify the context	Replace vague qualifiers with specific numbers, percentages, or trends that help leaders understand scale. "12 of our 150 internet-facing applications have overdue critical vulnerabilities, down from 21 last quarter."
Balance risk with progress	Be transparent about challenges while also communicating improvements, momentum, and the organization's plan to reduce risk over time. "Ransomware remains one of our highest risks. Since the last update, we have completed immutable backups, expanded MFA coverage, and reduced recovery time by 40%."

Table 9.2 – Executive communication principles

A strong executive update clearly explains what has changed, why it matters to the business, and whether awareness, alignment, or action is needed. Before walking into any executive session, pause and ask yourself one simple question: "What is the bottom line, and what do I need from the audience?" If you cannot answer that in one or two sentences, your message is probably not ready.

Once you are clear on the message you need to deliver, the next step is deciding how to structure that information consistently for executive and board audiences.

Building your reporting framework

One of the most effective ways to improve executive communication is to establish a reporting framework. Every organization has its own reporting culture. Some expect a formal presentation deck, while others prefer a written briefing, a dashboard, or a live discussion. Before creating new materials, ask how executive updates are typically delivered and whether established templates already exist. Adapting to your organization's reporting style is often more effective than introducing your own.

You also need to understand what your audience values. Rather than assuming you know what executives want to hear, ask them. Many leaders will tell you directly which information helps them evaluate risk or make decisions.

When their priorities are less clear, questions such as "What keeps you up at night?" or "Which cyber risks concern you most?" can reveal insight into the issues they care about. Those conversations should shape both the content of your framework and the emphasis of future updates.

Once you understand the organization's reporting culture and what your audience values, design a reporting framework that can serve as the foundation for future updates. Start by defining the overall flow of the discussion, then identify the reporting elements that support it. The reporting framework provides the recurring structure, while elements such as the threat landscape, risk posture, compliance posture, roadmap, and industry incidents provide the content within it.

You do not need to include every reporting element in every update. Select and emphasize them based on the audience and what has meaningfully changed. For example, a significant security incident, a material shift in risk exposure, a major regulatory development, or a change to the roadmap may justify a focused update outside the normal reporting format**.** A quarterly update may provide a broad view of the risk posture and roadmap, while a discussion following a significant industry incident may focus more on exposure and preparedness.

Once you choose the reporting elements, organize them into a structure leaders can recognize across updates.

Choosing consistency over ad hoc structure

Once you establish your reporting framework, use the structure consistently enough so that the audience becomes familiar with its flow. This consistency applies to how the information is organized, not how often you provide updates. A recognizable structure helps executives quickly locate information, compare it with prior updates, and focus on what has changed.

Imagine that a new ransomware campaign begins targeting organizations in your industry. Leadership wants to understand your exposure and the actions underway. You arrive prepared, but the update is organized differently from the previous quarter. The last presentation was structured by security domain; this one is grouped by business unit. Several familiar metrics have been replaced, the threat landscape appears in a different part of the deck, and the scoring methodology has changed.

Instead of discussing the organization's exposure, executives spend the first several minutes trying to orient themselves. Questions shift from "How exposed are we?" to "Is this score different from last quarter?" and "Where is the information we reviewed previously?" The conversation becomes focused on the format rather than the actual risk. That loss of time can make it harder to secure the alignment or support you need, whether you are proposing a new investment, reallocating resources, or asking leaders to accept a particular level of risk.

A consistent framework reduces this kind of friction. By using the same structure each time, you create a shared mental model with your audience. This allows you to focus on the substance of the discussion and also gives executives confidence that they know how to interpret the information being presented.

Note

Consistency does not mean that every update should be identical to the previous one. The reporting framework should remain recognizable, while individual reporting elements can be added, removed, or emphasized differently as risks and priorities change.

Selecting reporting elements for executive updates

The reporting elements that follow are some of our personal favorites. Each addresses a different question that leaders commonly ask, from understanding the current threat environment to evaluating risk posture, compliance, roadmap progress, and preparedness for industry incidents. You do not need to use every element in every update. Select and adapt those that best support the conversation you need to have.

These elements are not intended to be exhaustive. You may find other useful approaches through peers, internal reporting practices, or guidance from organizations such as IANS and Gartner. Focus on the elements that provide the clearest insight into the issues your audience needs to understand and the decisions they may need to make.

The threat landscape

The threat landscape reporting element is designed to orient executives to the external and internal forces shaping the organization's security risk at a given point in time. Our purpose here is to establish context: what risks matter most right now, how they connect to the business, and how the cybersecurity team is responding to them. When utilized well, this section becomes the anchor for the rest of the update, providing clarity and focus for metrics, priorities, and decisions.

Achieving clarity requires prioritization. You will not be able (and should not try) to cover every threat because too much information dilutes the key message. This section is about providing context, not a threat intelligence briefing.

The most effective approach is to concentrate on the top 6–8 risks that could impact the business. *Figure 9.1* illustrates one way to present the threat landscape to executives. Each column highlights a significant threat facing the organization, and the trend indicator shows whether that threat has increased, remained stable, or decreased since the last update.

Together, these trends help leaders quickly identify where risk is evolving and determine which areas deserve deeper discussion. Supporting details can be referenced during the conversation if additional context is needed.



Figure 9.1 – Sample cyber threat landscape slide

Tip

When presenting the threat landscape, consider both threats to your enterprise environment and threats that affect your customers, products, or services. For example, an increase in **account takeover (ATO)** attacks may have little impact on your corporate network but could significantly affect customer fraud losses and trust.

How you use this reporting element should evolve based on where you are in your reporting cadence:

In your first update, the threat landscape helps establish a baseline for future discussion. This is your opportunity to align the audience on the threats that matter most, the business exposure, and what actions are already underway to manage them. These may include risks such as ransomware, third-party compromise, data loss, or emerging regulatory exposure. Establishing this initial view gives leaders a consistent point of reference as the same threats evolve and new ones emerge in future updates.

In the follow-up updates, the role of the threat landscape shifts from education to status reporting. Rather than reintroducing the full landscape, focus on what has changed since the previous update. Which risks are trending up or down, and what did you do to drive that? Where has the organization made measurable progress in reducing exposure? These might include improving endpoint coverage, reducing critical vulnerabilities, or strengthening third-party controls. What external developments, such as a new ransomware campaign, a peer

incident, or a regulatory change, materially alter your priorities? This approach reinforces continuity and keeps the discussion oriented toward progress.

We recommend starting executive updates with the threat landscape because it sets the tone for the entire conversation. It grounds priorities in reality, provides context for operational metrics and investment opportunities, and helps executives understand *what* is being presented and *why* it matters.

Tip

Executive materials often become long-lived artifacts and may be reviewed outside their original context. The goal is not to withhold information, but to exercise judgment. Try to capture high-level risk and mitigation in writing while reserving sensitive nuance for live discussion, and always consult with your legal team when in doubt.

The following are sources of information to consider when framing the threat landscape:

- General external threat intelligence reports and briefings published by technology and cybersecurity vendors. Examples include annual threat reports, incident-response analyses, vulnerability research, and updates on active threats.
- Industry-specific intelligence from organizations such as the **Financial Services Information Sharing and Analysis Center (FS-ISAC)** or the **Health Information Sharing and Analysis Center (H-ISAC)**. These may include member alerts, sector-specific threat briefings, peer intelligence, and reports on attacks affecting similar organizations.
- Internal security data, including incident trends and near-miss analyses. Examples may include increases in phishing attempts, recurring causes of security incidents, attempted account compromise, or events that were detected before resulting in material impact.
- Business and technology changes that may affect exposure. Relevant sources may include transformation roadmaps, acquisition plans, cloud migration updates, product-launch documentation, or discussions with business and technology leaders. For example, entering a new market, adopting a new cloud platform, or launching a client-facing application may introduce new risks that should be reflected in the threat landscape.

Industry or peer security incidents

The threat landscape provides a broad view. An industry or peer incident reporting element allows you to focus on one event in greater depth and connect it directly to your organization. These incidents often attract executive attention because they make an abstract risk immediate and tangible.

This is effective because it connects external events to internal preparedness and helps answer a question many leaders are already thinking:

"*Could this happen to us, and how prepared are we?*"

The goal is not to retell the story in detail but to help others, less technical in certain instances, understand the implications. A simple structure can guide the conversation, and may address the top three questions:

- What happened: A brief description of what occurred.
- Why did it happen: The conditions or control failures that contributed to it.
- What would it mean if it happened at our company: The potential implications for your organization.

Use a visual when it can explain the sequence of events more clearly than text. *Figure 9.2* illustrates one way to present the incident flow while limiting the discussion to the details that matter most.



Figure 9.2 – Sample industry incident deep dive slide

After establishing what occurred, shift the discussion inward. Explain whether a similar scenario could affect your organization, which controls you already have in place, and whether additional work may be needed. If gaps exist, acknowledge them and describe the actions underway without turning the discussion into a detailed remediation review.

Leaders often hear about breaches in the news or from peers before the next update takes place. By proactively addressing relevant incidents, you control the narrative rather than reacting to it. It demonstrates awareness, preparedness, and a forward-looking mindset.

Tip

If time is limited, this content can be incorporated into the threat landscape slide or the risk posture as a short callout.

Sources to consider when selecting an incident:

Select incidents that are recent, relevant to your business, and useful for evaluating internal preparedness. The purpose is not to cover every major breach, but to identify the external events most likely to support a meaningful internal risk discussion. Sources may include:

- **Public statements and disclosures from the affected organization:** These may include breach notifications, company updates, regulatory filings, or investor communications that explain what occurred and how the organization responded.
- **Regulatory or government reporting related to the incident:** Enforcement notices, public findings, technical advisories, or law enforcement updates may provide additional insight into the cause, impact, or control failures involved.
- **Post-incident analyses:** Reports from forensic firms, security researchers, insurers, or other parties may help explain the attack path, contributing factors, and lessons that are relevant to your environment.

The risk posture

If the threat landscape explains what is happening around you, the risk posture explains what it means for the organization. This element translates external and internal signals into exposure. At its core, it answers two questions executives deeply care about: *How exposed are we, and are we getting better?*

The risk posture is also an expectation-setting tool. In the aftermath of a breach, executives and boards often realize they did not fully understand the true state of the security program beforehand.

It is easy to present metrics that appear stable and reassuring, with everything labeled as 'green' or 'on track'. Some cybersecurity executives are under constant pressure to show that view. I recall one organization from my consulting days that had just completed an extensive control review. On paper, everything looked solid. Shortly after, the company experienced a major data breach. Leadership's immediate question was "*If everything was going well, why did this happen?*"

That is why the risk posture should provide a candid view of exposure rather than a collection of reassuring metrics. The goal is to help leaders understand where meaningful risk remains, even when individual controls or compliance activities appear to be performing as expected.

A heatmap is one of the most common visual tools for this purpose. By mapping the organization's top risks across impact and likelihood, you provide an intuitive view of exposure without requiring technical interpretation. To keep the visual readable, focus on the 10 to 12 risks most important to the organization rather than attempting to represent the entire risk register. *Figure 9.3* illustrates one simple way to present the risk posture using a heatmap.

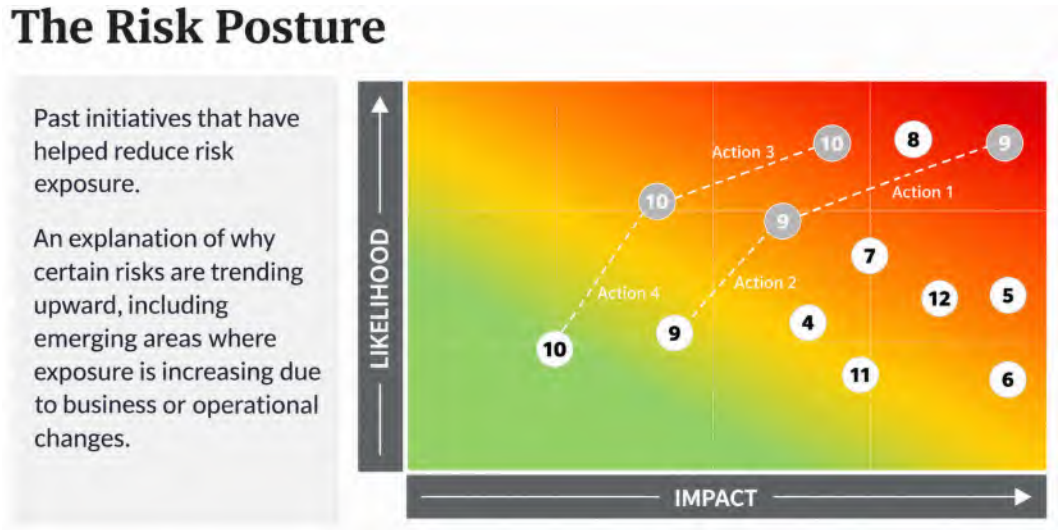


Figure 9.3 – Sample cyber risk posture heatmap. Gray markers indicate earlier risk positions; white markers indicate current risk positions.

Note

Note, however, that some security executives prefer not to use heatmaps. The scoring can create a sense of precision that the underlying assessment may not support, particularly when likelihood and impact depend heavily on judgment. An alternative is a prioritized risk view that lists each risk alongside its business impact, current exposure, direction of travel, and the action underway. This format provides more context and makes it easier for certain executives to understand the risk. The right visual is one that reflects your organization's risk methodology and supports an informed executive discussion.

How you use the heatmap should evolve with your reporting cadence:

In the first update, establish the baseline. Provide a candid view of the organization's most critical risks, such as unauthorized access, data breach, phishing, and quantum computing. Leaders should leave with a clear understanding of the current state, the areas requiring the greatest attention, actions already underway, and the time horizon for meaningful improvement.

In follow-up updates, focus on progress and movement. Show which risks have improved, remained stable, or increased and explain what is driving the change. For example, exposure may decline following improvements in endpoint coverage, reductions in critical vulnerabilities, or stronger third-party controls. It may increase because of business expansion, changes in the technology environment, or newly identified control gaps. This turns the heatmap from a point-in-time assessment into a consistent view allowing executives to see risk reduction or standing in place.

The left-hand panel of *Figure 9.3* can provide context behind changes in particular risks. This may include:

- Initiatives that have helped reduce risk exposure
- Future initiatives expected to drive improvement
- Factors causing a risk to remain stable or trend upward
- Emerging areas where exposure is increasing due to business or technology changes

This discussion also provides an opportunity to set expectations about the nature of cybersecurity risk. Leaders may reasonably ask when a particular risk will be resolved or when the program will reach its desired state. Explain that risk management is continuous and not a one-time project with a clear finish line. Progress in one area may coincide with new exposure as the business and threat environment change. Success is reflected not in eliminating risk altogether, but in understanding it, responding deliberately, and demonstrating meaningful improvement over time.

Sources to consider when framing the risk posture:

A meaningful risk posture is developed by bringing together information from across the organization. No single document or data source will reveal the organization's complete exposure.

Some risks will be readily visible through an assessment, control finding, or performance trend. Others may emerge only when information is considered together. A growing number of near misses, for example, may appear manageable until viewed alongside delayed remediation or an upcoming technology change.

You can use the following inputs together when framing the risk posture:

- Enterprise threat assessments and risk reviews
- Security metrics and performance trends
- Incident patterns and near-miss analysis
- Internal audit findings and control evaluations
- Business and technology changes that affect exposure

The maturity assessment

The threat landscape explains what is happening around you, and the risk posture explains what it means for the organization today. The maturity assessment evaluates the capabilities in place to manage that exposure across key security domains such as identity and access management, vulnerability management, incident response, and data protection. This section helps answer an important executive question: "*Are we where we should be compared to expectations, peers, and industry benchmarks?*" It provides a structured view of maturity across domains and helps leadership understand whether the organization is keeping pace, catching up, or falling behind.

A mature program may still carry significant risks, particularly as the business and threat environment evolve. Present the maturity assessment and risk posture as complementary views rather than interchangeable measures.

Many security teams perform an annual risk assessment, often facilitated by an external assessor. These reviews produce an executive summary report that includes a maturity model visualization, commonly shown as a spider diagram. This view shows current maturity across major security domains, highlighting where capabilities are strongest and where further development may be warranted. It can also provide comparisons with a prior assessment or a relevant industry benchmark. *Figure 9.4* illustrates this approach.

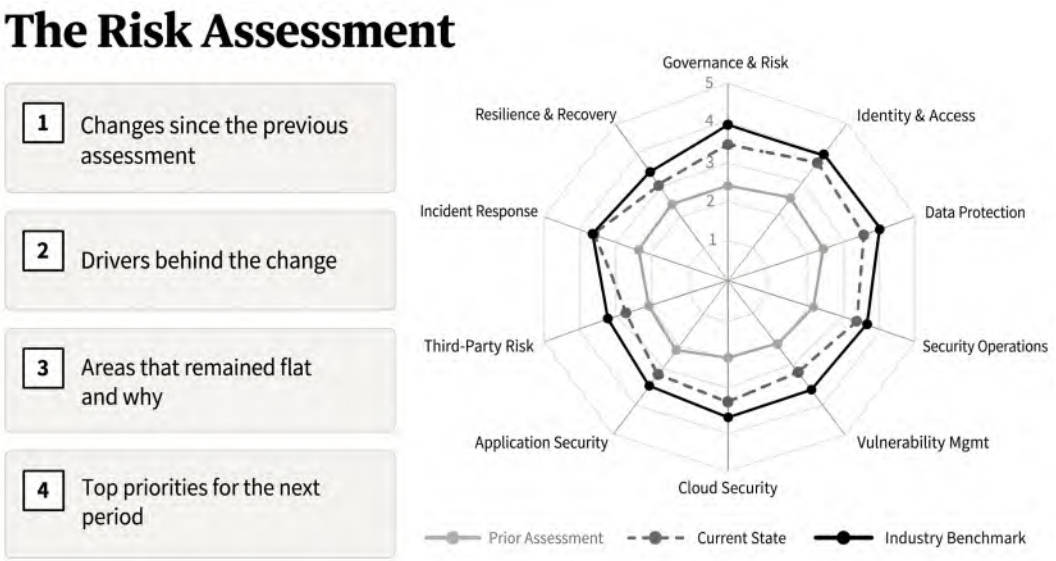


Figure 9.4 – Sample risk assessment

Like any assessment, this diagram represents a snapshot in time. I have seen organizations rated at Level 3 across every domain still experience a significant breach. An external assessment provides an independent validation within a defined scope, but it is not an assurance that the organization is secure. Use the results as an input rather than as a definitive statement about the organization's security. As earlier, how you use this element is going to change based on where you are in your reporting cadence.

In your first update, provide your interpretation of the assessment. This is particularly important when the review was completed before your tenure. Executives will naturally look to you for interpretation. "*Do you agree with the ratings? Which gaps are most critical to address? How are the results being integrated into your roadmap and workplan?*" Even when two domains receive similar maturity ratings, business risk may justify prioritizing one over the other. You will need to explain the prioritization given competing priorities. This is an opportunity to show that the assessment is helping shape the program, even though it is a static report.

In follow-up updates, the emphasis shifts to progress since the previous assessment. Year-over-year comparisons are particularly powerful here. Movement across domains demonstrates whether investments, staffing, and initiatives are translating into measurable maturity gains. If additional budget was allocated to strengthen a specific capability, this is where you can show how that investment is improving the program. Expanded identity governance, for example, may improve maturity in access management. A domain may also remain unchanged because a multiyear initiative is still underway. This context helps executives interpret the scores without treating every change (or lack of change) as a pure measure of performance. Apart from the information shown in *Figure 9.4*, provide the following additional context for leaders to interpret the movement:

- Changes since the previous assessment
- Drivers behind the change
- Areas that remained flat and why
- Top priorities for the next period

This figure also surfaces an important leadership moment. I recall a case where a risk assessment showed the organization was relatively mature across several domains. The immediate follow-up question from leadership was: "*If we are already mature, why do we need further investment?*"

Moments like these highlight the importance of painting a balanced picture. You could address a question like this by explaining that achieving a certain maturity level does not mean risk has been eliminated. It means the organization has built strong foundations and that they should continue to evolve as the threat landscape, business priorities, and regulatory expectations change.

One question you should expect during the presentation is: Who are we being compared against? Be prepared to explain how the benchmark was constructed. Start by understanding how many organizations were included and whether they are really comparable based on revenue, geographic reach, and business complexity. Consulting firms may not include this detail in the first draft of the assessment.

We recommend asking for it before the results are finalized so you can understand it and explain the comparison with confidence during the executive briefing. For example, if you work for a fintech company with $10 million in revenue, a comparison with a large global bank may not be particularly meaningful. The bank likely has a much larger cybersecurity budget and a program designed for a different scale and level of complexity. The benchmark may still provide useful context, but leaders need to understand its limitations before drawing conclusions.

The following sources should be considered when framing the risk assessment reporting elements:

- The current assessment report and prior-year reports, providing the basis for showing progress over time
- Maturity model evaluations aligned to security frameworks such as NIST CSF
- Benchmarking information that explains how the peer group was selected

The compliance posture

The previous elements help leaders understand the organization's cybersecurity exposure and its ability to manage that risk. This one answers a different question: "*Are we compliant?*" While security reflects how well the organization is managing risk, compliance reflects how well it is meeting external expectations set by regulators, auditors, and industry frameworks. For organizations in heavily regulated industries, including financial services and healthcare, compliance posture is a central part of executive reporting. It explains how external requirements influence priorities and why certain initiatives may need to move faster with executive sponsorship. Even in less regulated environments, it provides a useful view of how the organization is meeting applicable obligations. Compliance offers a structured way to demonstrate alignment with formal expectations and manage legal, reputational, and regulatory risk.

This element should focus on three core areas:

- **Regulatory and compliance developments**: Describe new or evolving requirements that affect the organization, including the introduction of new controls or heightened expectations. Explain how readiness is being tracked and identify any areas where meeting the requirements may require additional effort or leadership support.
- **Regulatory exams and audit outcomes**: Summarize the severity and broader themes of recent findings. Explain how the findings are being driven to closure and what actions are underway to address the underlying gaps.
- **Annual audit schedule**: Provide a visual view of the year's planned and completed reviews so executives can quickly understand whether the program is progressing against the annual plan. Highlight any delays or changes that may require attention.

The goal is not to catalog requirements, but to surface what has changed and whether any new risks or obligations are emerging. Executives do not need to understand every control; they need to understand the implications for the organization.

Compliance reporting should be developed in partnership with legal and compliance, as well as the second line of defense where that structure applies. These teams provide important context on regulatory expectations and the status of examinations or findings. The security

executive brings the operational perspective and explains how those requirements affect the program. Prior to the meeting, review the content with these partners before presenting it to executives or the board. Align on the facts and resolve any differences in interpretation.

Figure 9.5 illustrates an executive-level approach to present compliance posture using a structured summary:

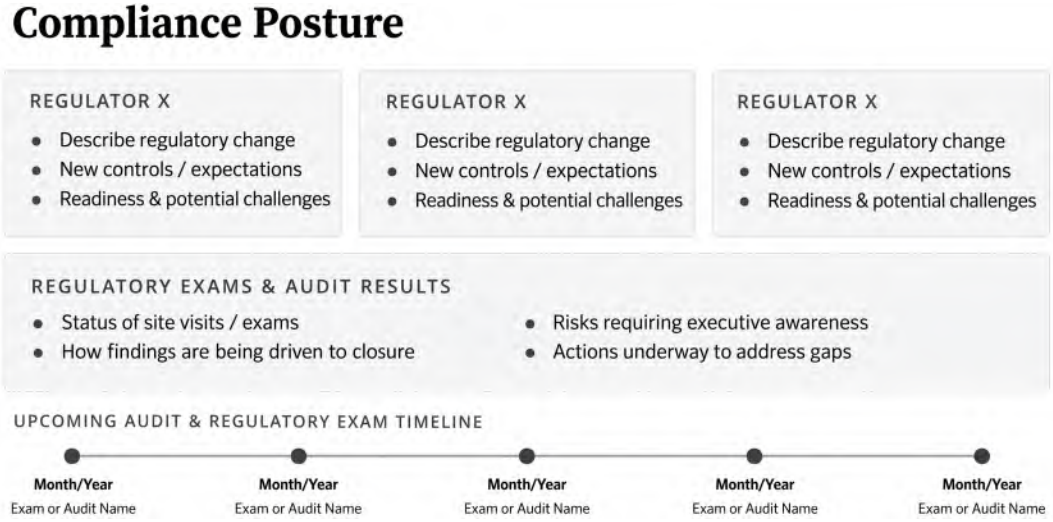


Figure 9.5 – Sample compliance posture update slide

In your first update, establish **the organization's current compliance posture.** It should reflect your understanding of key obligations, major frameworks, and any areas requiring immediate attention. This is an opportunity to highlight upcoming regulatory changes, known gaps, or areas where the organization may face increased scrutiny. For example, an approaching regulatory examination may accelerate readiness work, while a new reporting requirement could affect existing processes. Leaders should leave with a clear understanding of the organization's most significant compliance obligations and where support may be needed.

In subsequent updates, focus on what has changed. Highlight new requirements or the outcome of a recent examination. Show whether previously reported findings are progressing toward closure and explain any issue affecting the expected timeline. This creates continuity and helps leadership understand how the organization's compliance posture is evolving.

Over time, this element becomes an important signal of governance maturity. A stable compliance posture with manageable findings and predictable regulatory engagement builds confidence. Recurring findings or unresolved gaps, on the other hand, may indicate structural weaknesses that require attention.

Sources to consider when framing the compliance posture:

- Recent regulatory exams and supervisory reviews
- Internal and external audit results
- New or evolving regulatory requirements
- Compliance program tracking tools and remediation plans
- Upcoming regulatory deadlines or milestones

The roadmap

If the previous elements explain the organization's current environment and exposure, the roadmap answers the natural next question: **How are we responding?** It connects the threat landscape, risk posture, security maturity assessment, and compliance posture to a sequenced set of initiatives. Leaders should be able to see how current priorities address the most significant risks and support the program's longer-term direction.

Chapter 4 introduced the Sun Diagram Model as a way to present the three-year roadmap. Use it here to show how priorities and investments will evolve over time. The roadmap helps leadership answer another top-of-mind question: Are we investing in the right capabilities and addressing them in the right order?

This element should support the narrative that the roadmap is not a static plan. When the organization's exposure or business direction shifts, explain how the sequence of work has been adjusted in response.

Figure 9.6 illustrates a high-level, multi-year security roadmap using the Sun Diagram format introduced in *Chapter 4*.

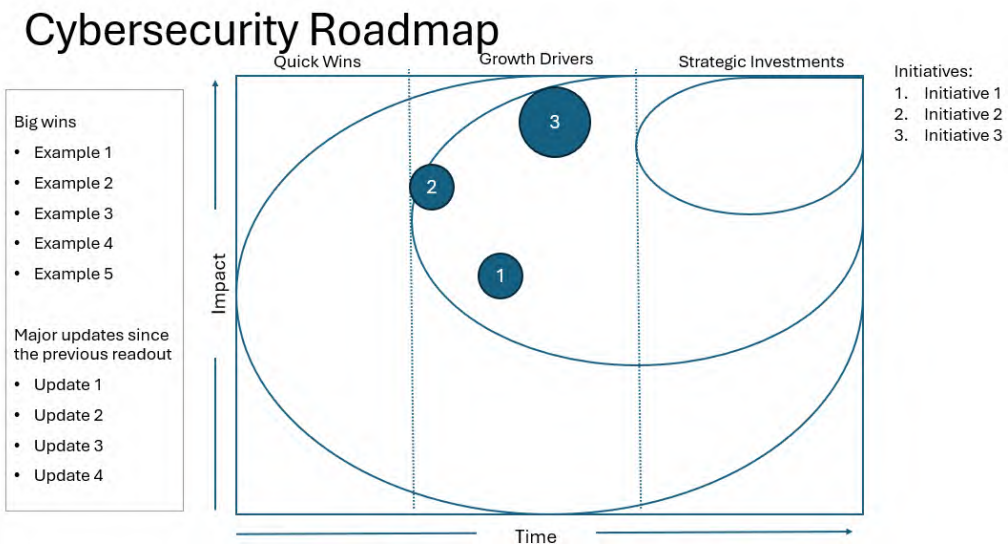


Figure 9.6 – Sample three-year security roadmap (Sun Diagram)

How you use this element should evolve based on where you are in your reporting cadence.

In your first update, orient leaders to the roadmap's major themes rather than walking through every initiative. Or you will run out of time and risk losing your audience in detail. For example, Year 1 may emphasize strengthening perimeter and foundational controls, Year 2 may shift toward detecting and managing threats that bypass those controls, and Year 3 may focus on resilience, automation, and optimization. Work will often progress across several areas at the same time, but a thematic view makes the intended sequence easier to understand.

Tip

This is also an opportunity to reinforce how the roadmap was built. Help the audience see that priorities are directly informed by the risks, maturity gaps, and compliance drivers. This strengthens confidence that resources are being allocated intentionally.

In subsequent updates, shift the conversation from strategy to progress. Highlight the work completed since the previous update and explain how it impacted the program. Address any material delay or change in direction before leaders need to ask about it. This provides a balanced view of progress and creates context for changes to the roadmap.

At the time this book is being written, security roadmaps are changing more frequently than reporting cycles, sometimes before you have an opportunity to present the next update. For example, supporting the organization's enterprise AI rollout may require resources originally planned for a tabletop exercise or the expansion of data tokenization.

Tip

Understanding and communicating trade-offs in writing has therefore become even more important. When an initiative is accelerated, explain why the priority changed and identify the work that may be delayed as a result. This shows leadership that the adjustment reflects a deliberate risk decision.

Over time, the roadmap becomes a record of the decisions that shaped the program, not only a plan for future work.

Sources to consider when framing the roadmap:

- The latest version of your security roadmap

The metrics

The earlier elements described the exposure and how the program is responding. This element answers another executive question: "*How healthy is the cybersecurity program?*" Metrics provide a structured way for leadership to understand whether critical capabilities are operating as intended and whether performance is moving in the right direction. *Chapter 11* explores how to select and design meaningful security metrics in greater depth; here, the focus is on how to incorporate those metrics into executive and board reporting.

Here is the tricky part: There is no single standard for how metrics should be used in executive sessions. Some leaders expect a brief walkthrough of key indicators. Others prefer to receive the metrics for reference and discuss them only when something requires attention. You should confirm the preferred approach early so you can use the meeting time effectively.

Present a balanced view of program performance. Although an all-green dashboard may look reassuring, it can create more questions than confidence when a significant incident occurs or additional investment is needed. Show both strengths and areas for improvement, using metrics that connect cybersecurity performance to business impact. Focus on indicators that tell a clear story about the health and direction of the program. Where possible, align those indicators with the top risks shown in your heatmap or prioritized risk view. This creates a clear connection between the organization's exposure and the evidence used to evaluate it. When a risk moves, leaders can see what data supports the change.

For example, if data loss appears among the organization's top risks, the number of incidents alone may not reveal the impact. One incident may be contained with no impact at all, while another may require notification to millions of clients whose data was accessed.

Because space is limited, limit the view to a set of high-value indicators, typically no more than 10–15. These should be consistent over time so that trends become visible and shifts in performance can be identified early. The set may still evolve as the program changes or your understanding of it improves.

In your first update, explain the rationale behind the metrics you selected. You are unlikely to have time to review every indicator individually. Instead, use a few examples to show how the metrics collectively provide insight into the program. Explain the thresholds where that context would help leaders interpret future movement.

In subsequent updates, focus on material changes. When you introduce a new indicator, explain what you learned about the program that made it useful. If you remove or replace a metric, clarify why another measure now provides a better view. This makes the evolution of the reporting framework visible rather than leaving leaders to wonder why a familiar indicator disappeared. In many cases, detailed metrics are included in the appendix, especially when earlier parts already provide context. This approach works well as long as the key signals are still visible in the main discussion. If there is a specific metric that reinforces a point you are making, weave it into your narrative rather than assuming you will get to discuss all metrics in detail.

With the reporting framework in place, attention now turns to leveraging it in an executive or board setting. The quality of the discussion depends not only on the materials, but also on the alignment built beforehand and how you lead the conversation once the meeting begins.

Preparing for executive and board sessions

Presenting to executive leadership and the board is one of the most visible responsibilities of a cybersecurity executive. These sessions shape how leaders understand the program and how much confidence they place in you as its leader.

Strong materials are only part of the equation. The outcome also depends on understanding the cadence and building alignment before the meeting.

This section focuses on the reporting cadence and the preparation required before you enter the room.

Understanding executive and board reporting cadence

In many organizations, cybersecurity is first presented to the C-suite or internal risk committee prior to each board presentation. This progression builds internal alignment, surfaces

questions early, and gives you an opportunity to refine your message before it reaches the boardroom.

The cadence of these updates varies depending on governance maturity and whether the company is public or privately held.

In publicly traded companies, the CISO often presents to the board's audit or risk committee at least twice a year, with more mature organizations expecting quarterly updates. A full-board presentation typically takes place annually.

In privately held companies, governance structures can vary significantly, and the cadence may be less formal. Even in those environments, regular executive-level updates are expected, with board engagement typically occurring at least once a year.

It is also helpful to understand the broader context around the meeting. If you are new to the organization, reviewing governance documents such as committee charters, annual priorities, or upcoming focus areas can provide insight into what topics may receive the most attention. Some organizations offer orientation sessions for new executives or board members. Joining these discussions can help you refine the messaging even further.

Aligning before the session

Preparation for executive and board sessions begins well before you enter the room. Experienced executives often say that the "meeting happens before the meeting." The formal session should build on prior conversations that already surfaced concerns and agreed on the message with your direct line of management and company executives. This preparation is not just about slides. It is about building a narrative, aligning stakeholders, and practicing your message. When done well, it allows you to walk into the room confident, focused, and prepared for the discussion.

Drafting the narrative

The first step is developing a coherent story. Begin with the message you want leaders to understand and the purpose of the discussion. Use the reporting framework introduced earlier in the chapter to decide which information supports that message and what can remain in the appendix.

If you are new to the organization, outline the proposed narrative and review it with your manager before building the deck. This is particularly valuable during your first one or two reporting cycles, when you are still learning what the audience expects and how leadership wants the message framed. It can save significant rework by identifying changes before they are incorporated into the slides. Once trust is established and the reporting structure becomes familiar, this early review will often become unnecessary.

AI may reduce the time required to create presentation materials, but it does not replace alignment on the story. A deck can now be produced much faster, which makes it even more important to confirm that the narrative reflects the organization's priorities before the slides give it form.

Reviewing and aligning

Once the narrative is aligned, develop the slides starting with the reporting elements suggested in this chapter. At this stage, it is also helpful to pressure-test the content yourself before sharing the materials more broadly. Look for areas where the message may feel unclear, overly technical, or open to misinterpretation. Any slide that requires a long technical explanation or could create an unintended impression should be refined early.

Review the deck with your manager and the stakeholders relevant to the content. As an example, legal and compliance should review sections that reflect regulatory interpretations or sensitive organizational positions. The second line of defense may be involved when the presentation includes formal risk conclusions or matters within its oversight.

Use these reviews to resolve differences in interpretation before the materials are finalized. If the update contains a significant change in exposure or direction, discuss it directly with the affected executives in advance. The boardroom should not be the first place a leader learns about an issue that affects their area.

Practicing your storytelling

With alignment in place, practice how you will communicate the update. It sharpens your narrative, builds self-confidence, and helps you anticipate where questions, skepticism, or concern may arise.

Rather than rehearsing the slides word for word, focus on the narrative. For each slide, ask yourself one simple question: "*What is the bottom line for each reporting element?*" If you cannot summarize the key message in one or two sentences, the audience will likely struggle to follow in a live setting. I write that bottom line down for each slide. I rarely need to look at it during the meeting, but the exercise forces me to clarify the message before I ever step into the room. It also serves as a simple checkpoint to make sure I communicate the one point I want leaders to remember before moving on.

Many people say they are too busy to practice. In my experience, practice is one of the highest-return investments you can make before an executive meeting. It is often the difference between presenting information and leading a confident discussion. As your experience grows, the amount of preparation time will naturally decrease. During your first year in an executive role, however, practice should be part of every major presentation.

Tip

Consider working with an executive or board coach, ideally outside your direct management chain, who has firsthand experience presenting to senior leaders or serving on boards. The goal is to receive candid feedback from someone who understands how executives consume information, rather than someone evaluating the technical accuracy of your content. Even a few conversations can provide useful feedback on how your message may land.

Case study: preparing for a first audit and risk committee update

A newly appointed CISO at a publicly traded financial services company in the United States was preparing for her first quarterly meeting with the board's audit and risk committee. She had been allocated 20 minutes, including questions, and the materials were due one week in advance.

Since the committee last met, the company had accelerated its enterprise AI rollout. Supporting the initiative required security resources originally assigned to expand data tokenization. Recent incidents at peer organizations had also increased leadership's interest in third-party risk.

Finding the focus

Because this was her first committee presentation, the CISO reviewed the committee charter and minutes from prior meetings. She also spoke with the committee liaison and learned that members were particularly interested in third-party exposure and the effect of the AI rollout on the security roadmap.

Once the narrative was aligned, the CISO developed the presentation using the reporting framework introduced earlier in the chapter. The threat landscape explained why third-party risk had increased, while the risk posture showed how that exposure affected the organization. The roadmap presented the decision to accelerate AI security work and delay part of the tokenization expansion.

Aligning the message

The CISO reviewed the materials with the CTO, CIO, and the General Counsel. She also involved the compliance team and the second line of defense. During the review, the second line asked whether delaying tokenization could affect an existing risk. The CISO added that context to the presentation and described the interim measures that would remain in place.

The CISO then rehearsed the presentation as a discussion rather than a slide-by-slide walkthrough. For each slide, she wrote down the bottom line and practiced communicating it naturally. She limited the prepared update to approximately 15 minutes, leaving the remaining time for questions and a clear close.

During the meeting, a committee member asked whether the company was increasing its data risk to support the AI rollout. The CISO acknowledged the trade-off and explained that the tokenization expansion had been delayed while the existing controls remained in place. She then moved to the roadmap slide and showed that visual impact.

Conclusion

As the meeting closed, the CISO reinforced the increased attention on third-party exposure. She also clarified that the enterprise AI rollout had changed the sequence of roadmap priorities and that management would continue to monitor the exposure created by delaying tokenization.

The committee left with a clear understanding of what had changed and how the security program was responding.

Preparation sets the foundation. Once the meeting begins, success depends on how you communicate in the moment—guiding the discussion, responding to questions, and adapting to your audience.

Showing up for the meetings

Executive and board sessions are discussions, not slide presentations. The materials create a point of reference, but the real value comes from the conversation they support. Your role is to help leaders understand the organization's exposure and guide a focused, high-value discussion.

How you show up in the room matters as much as what you present. Leaders are observing not only the content, but also how you think and how you respond under pressure. When done well, these interactions feel less like presentations and more like strategic conversations.

Once the meeting begins, your preparation becomes visible through the choices you make about where to spend time and how to respond when the discussion changes direction.

Leading the conversation

Most leaders review materials in advance, although you should not assume they have studied every slide. This ultimately means the session itself is rarely about walking through slides one by one.

Use the slides as reference points rather than a script. Lead with the conclusion, then provide the supporting context. If a question moves the conversation to a later topic, go to the relevant slide and return to the original sequence only if it still adds value. This allows the discussion to follow the audience's needs without losing the key message.

Managing time and focus

Time is limited at every level. Whether presenting to the C-suite or the board, you will often have only 15–20 minutes. Always remember that while a topic may be your favorite, it is just one part of a broader agenda.

Managing time in the room is just as important as managing content. Be mindful of the pace and keep an eye on the person managing the session. If time begins to run short, shift to reinforcing your most important points and bring the discussion to a confident close. As the meeting closes, reinforce three points:

1. The most important change in the organization's exposure
2. The progress leadership should recognize
3. Any decision or support needed from the audience

Respecting the time allocated signals professionalism, awareness, and maturity. If only one message can be reinforced, choose the one that leaders most need to remember.

Reading the room

Strong executive communication also relies on what you observe. Senior leaders often communicate as much through reactions, tone, and follow-up questions as they do through direct statements. Paying attention to these signals helps you understand where concern, confusion, or interest may be building.

Silence is one of the most common signals and rarely the most helpful one. While it can indicate agreement, it often means the point was unclear, the message did not resonate or did not feel relevant enough to prompt discussion. In a role where cybersecurity affects nearly every part of the organization, meaningful engagement is usually a healthier sign than quiet acceptance.

Participation patterns also provide useful insight. If several leaders ask similar questions, the issue likely needs clearer explanation. When someone who rarely speaks begins engaging, it often signals that the topic matters and deserves attention.

Tip

Virtual meetings make this harder. Body language is limited and silence becomes more ambiguous. In these settings, be deliberate about bringing leaders back into the conversation: pause, ask for perspectives, or briefly reconnect the topic to business impact.

Over time, learning to read these signals helps you adjust in the moment, clarify confusion early, and keep the discussion focused on what matters most.

Handling questions and dialogue

Executive and board meetings are rarely one-way presentations. Once you have established the key message, the discussion often shifts quickly to questions. Treat those questions as part of the meeting, not interruptions to it, and plan for at least 25% of your time to be dedicated to discussion.

Over time, you will begin to recognize patterns in the types of questions executives and board members ask. Most are variations of a few themes: *How exposed are we? What are we doing about it? Are we getting better?* These questions are less about technical detail and more about confidence in the direction of the program.

For board discussions, resources such as the **National Association of Corporate Directors (NACD)–Internet Security Alliance (ISA)** *Director's Handbook on Cyber-Risk Oversight* can also help you anticipate the questions directors may ask. The 2026 edition includes 15 boardroom tools covering topics such as incident response, emerging technologies, third-party risk, and cybersecurity metrics, several of which provide questions directors can use in discussions with management.

When responding:

- Listen to the complete question and clarify it when needed.
- Lead with a direct answer before providing supporting context.
- Connect the response to the organization's exposure or the action underway.
- Acknowledge uncertainty honestly when needed.

Avoid over-defending, over-explaining, or speculating under pressure. If you do not know the answer, say so clearly and commit to following up. Leaders are not expecting perfection, but they *are* expecting extreme ownership.

At times, questions may be emotionally charged or framed as "gotcha" moments. Stay calm, acknowledge the concern, and respond with facts and context. If the question requires more

detail than the meeting allows, offer to follow up rather than letting the conversation move too far from its objective. This allows you to acknowledge the concern without becoming defensive or dismissing the question.

How you respond in these moments shapes confidence in both you and the program. Executives are looking for sound judgment more than technical depth. Staying composed, answering directly, and acknowledging uncertainty when needed demonstrates that you understand the issue and are managing it with appropriate attention.

Closing with the message to remember

Executives rarely remember every element of an update. What stays with them is the message they hear as the discussion comes to a close. Reserve the final few minutes of the meeting to bring the conversation back to what matters most rather than trying to squeeze in one more slide.

Your closing should reflect the discussion that actually took place. Revisit the central message you identified during preparation, then adjust it based on the questions or concerns raised in the room. Summarize what has changed, clarify the implication for the organization, and make the next step explicit. If you need a decision or support from the audience, state it directly. If no action is required, say that as well and explain what you will continue to monitor or when leadership should expect another update.

Assaf Keren captures this balance well in *Lessons from the Frontlines: Insights from a Cybersecurity Career* through a framework he calls "State Reality, Inspire Hope." The principle is particularly useful when closing an executive discussion; be direct about the reality of the situation, then give leaders confidence that there is a credible path forward. Inspiring hope does not mean minimizing the risk or offering false reassurance. It means making the response and the next step clear.

For example, in the case study earlier in this chapter, the CISO might close by saying: "The key changes since our last update are increased third-party exposure and the decision to accelerate AI security work. The tokenization expansion has been delayed, with existing controls remaining in place. No decision is required from the committee today. We will continue to monitor both areas and report back at the next meeting."

Avoid introducing new information during the close. The objective is to leave leaders with a clear understanding of where things stand and what happens next. If executives remember only one thing from the update, it should be the message you reinforce before the meeting ends.

Notes from the field with Renana

Case study: developing executive presence

Early in my consulting career, I had my first interaction with a C-suite audience. I was scheduled to facilitate a full-day tabletop exercise with the executive team of a Fortune 100 technology company. The weeks leading up to the exercise were filled with interviews and documentation reviews in order to create a realistic scenario.

About an hour before the session started, I met with the partner leading the engagement. It was the first time he reviewed the materials. After flipping through the slides, he looked at me and said, "I really hope you know what you're doing."

Honestly, I did not. No one had coached me on what it takes to engage with a C-suite or board audience of a Fortune 100. My military background had given me experience speaking with senior leaders, but this felt different. These were executives responsible for a global organization, and I had no real way of knowing whether what we had prepared would actually be worthy of their time.

Fortunately, it was. The exercise generated an executive discussion with the client, and that one session led to many more. Over the years, a single exercise turned into hundreds of executive simulations around the world. What stayed with me was the realization that some leaders seemed to have the magic "executive presence." They knew how to communicate with senior leaders in a way that was clear, relevant, and actionable.

At the time, I was not sure how to develop that skill myself. In the years that followed, I spent countless hours presenting at security conferences and had regular interactions with C-suite leaders and boards of Fortune 500 companies. I prepared deliberately, often spending hours refining the message and considering how it might be received. The slides mattered, but I gradually learned that preparation was really about developing command of the narrative.

Along the way, I made many of the same mistakes that most security leaders make when they first enter these settings. Sometimes I was too technical. At times I became defensive when challenged. Occasionally I delivered a presentation that made perfect sense to me but failed to resonate with the audience. Some sessions ended with clear alignment and action, while others did not.

Those experiences taught me that success in those rooms is not about demonstrating that you have the most technical knowledge. It is about helping leaders understand what matters and giving them the context they need to act.

Strong mentors accelerated that learning. They challenged my thinking and gave me direct feedback about how I showed up. Through those conversations, I began to understand that

executive presence was not a polished presentation style or an innate quality reserved for certain people. It came from preparation and the ability to adapt when the discussion did not go as planned.

Many of the practices in this chapter come directly from those experiences. They reflect years of preparation, feedback, mistakes, and conversations that helped shape how I communicate with senior leaders today.

If there is one thing I would share with anyone stepping into these rooms for the first time, it is this: executive presence is built long before the meeting starts. Find someone. That person may be a trusted leader or an experienced executive coach. Candid feedback can help you develop a skill that is difficult to evaluate on your own.

I still think about the partner's words before that first exercise: "I really hope you know what you're doing." At the time, I heard them as a question about whether I could lead the session. Years later, I understand the broader lesson. Knowing what you are doing in an executive room does not mean having every answer. It means bringing clarity when the stakes are high and helping leaders determine what should happen next.

Summary

In this chapter, we explored how security leaders can communicate effectively with executives and boards. We examined how to translate technical risk into business impact, establish a consistent reporting framework, and select the reporting elements that best support each discussion. We also looked at how to prepare for executive and board sessions, lead the conversation, respond to questions, and close with a clear message.

In *Chapter 10*, we will explore how to cultivate a security-first culture by designing effective awareness programs, promoting shared responsibility, and engaging employees as an active line of defense.

Chapter checklist

- **Translate security risk into business impact.** Lead with what the issue means for the organization, quantify the context, and make the decision or action you need from leadership clear.
- **Establish a consistent reporting framework.** Keep the overall structure recognizable from one update to the next while selecting and emphasizing reporting elements based on the audience and what has changed.

- **Align the message before the meeting.** Identify the key takeaway, review the narrative with your manager and relevant stakeholders, and resolve material differences or surprises before the formal session.
- **Prepare for the discussion.** Practice the narrative rather than memorizing the slides, pressure-test difficult questions, and reserve enough time for executive and board dialogue.
- **Lead and close the meeting intentionally.** Read the room, answer questions directly, connect the discussion back to business impact, and close by reinforcing the message leaders most need to remember and any next step or support required.

Additional resources

- Executive slides: `https://bit.ly/CISOBook31`
- NACD Director's Handbook: `https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/2026-cyber-risk-oversight/`

10

Championing Change: Cultivating a Security-First Culture

Most security leaders are good at protecting the organization. However, far fewer are good at getting the organization to think about risk the way they do.

This distinction is what separates a security function from a security-first culture. When risk becomes part of how the organization thinks, and not just how the security team operates, decisions are made differently. Simply put, security stops being a gatekeeper and becomes second nature.

Building a security-first culture that is embedded across every level is one of the hardest things you will do as a cybersecurity executive. It is also one of the most impactful things you can do. It is a lengthy process that does not happen through a single program or announcement. It happens through multiple layers combining people, education, and leadership behaviors, reinforced consistently over time.

This chapter focuses on how to embed security as a shared responsibility across your organization. Specifically, this chapter covers:

- Scaling security beyond the security team
- Designing security education programs
- Influencing C-suite and board security culture

By the end of this chapter, you will have the tools to distribute security ownership across your organization, including an annual calendar of education activities and a clearer idea of how to engage upper management.

Scaling security beyond the security team

No security organization, regardless of size or budget, can directly participate in every decision across an enterprise. Security teams are expected to support many ongoing initiatives, including product development, architecture reviews, risk management, and compliance requirements, all while responding to the latest security incident. Even well-established programs quickly encounter the same reality: the security team cannot be everywhere.

A common mistake many new executives make is assuming the solution is to add more security staff. In today's world, especially with budget constraints and the introduction of AI, the solution requires a different mindset, one that extends security thinking beyond the security organization itself. When employees across the business begin applying security lenses to their work, security considerations organically appear in conversations where the security team may not always be present, such as sprint planning, architecture discussions, and vendor evaluations. Instead of security being introduced later in the process, it becomes part of how teams approach risk and make decisions.

As you consider how to generate even greater impact in your first year, programs that extend security influence beyond the security team can amplify your reach. Two common approaches that support this model are Security Champions and **Business Information Security Officers (BISOs)**. The following diagram illustrates how these roles integrate with the central security organization: BISOs are embedded at the business unit level, and Security Champions are embedded within individual teams.

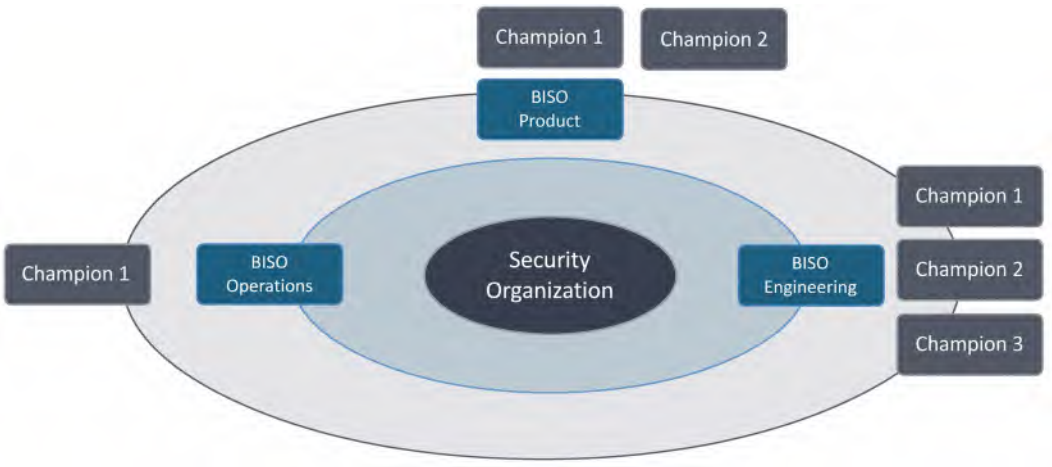


Figure 10.1 – Extending security influence through BISO and Security Champion programs

In the next sections, we will explore each approach, what role they serve, and how to set them up or uplevel existing programs.

Establishing a security champions program

A Security Champions Program embeds security-minded individuals within business and technology teams, extending the influence of the security organization beyond its own team.

Rather than serving as security experts, champions act as trusted advocates who help introduce security considerations into everyday engineering and product decisions. They typically volunteer for this role and take it on in addition to their primary responsibilities. This approach allows organizations to scale security influence without significantly increasing headcount while driving stronger adoption of secure practices through colleagues they already know and trust.

Champions are not expected to be experts across every security domain. Instead, they promote security priorities most relevant to their teams and act as a bridge between engineering and the security organization. Because they participate in day-to-day development activities, they can identify potential issues before they become costly to address. For example, if an organization is focused on reducing application security vulnerabilities, champions can encourage secure coding practices, promote the use of approved libraries, and raise potential concerns during design or code reviews. If the goal is to increase the adoption of encryption or data masking, champions can help teams understand where sensitive data exists and how the protections should be applied. By focusing champions on the organization's most important priorities, security teams can drive meaningful improvements without requiring champions to become full-time security professionals.

Introducing or uplifting the program

Security Champions programs can take different forms depending on the maturity of the organization and its needs. Some operate as informal networks of volunteers, while others use defined cohorts with structured training, recurring meetings, and clear responsibilities. Regardless of where you start, define the program's purpose, expectations, operating cadence, and responsibilities upfront. Champions should understand what success looks like and what is expected of them. It is important to note that Champions continue reporting through their existing management chain. The Security Champions program does not change reporting relationships.

If a Security Champions program does not yet exist, start small by identifying a limited number of engineers or product managers who already show an interest in security and invite them to participate as early champions. Look for individuals who consistently ask security questions during design reviews, report potential security risks, or have previously volunteered to support security initiatives. Their curiosity, credibility with peers, and willingness to

influence others are often strong indicators of success. Provide light guidance through short briefings, regular security updates, and access to the security team for questions.

For example, an organization launching its first Security Champions Program might begin with 10 engineers across several product teams who have already demonstrated an interest in security. The security team could provide an initial orientation on the program's priorities and expectations, followed by a monthly meeting to discuss recent incidents, upcoming initiatives, and issues champions are seeing within their teams. Champions would remain within their existing reporting lines while serving as a connection point to security. Over time, the organization could evaluate the program based on whether security issues are surfaced earlier, secure practices are adopted more consistently, and recurring issues decline within participating teams.

If a Security Champions program already exists, focus on strengthening its structure and impact. This may include establishing a regular cadence of champion meetings, providing deeper training opportunities, and recognizing champion contributions. As the program matures, shift the role of champions from recipients of security updates to active contributors. For example, involve champions in evaluating new security tools, reviewing proposed development standards, piloting process changes before broader rollout, or providing feedback on how security requirements affect engineering teams.

A successful program is measured by its influence rather than the number of champions. Depending on the program's objectives, signs of success may include earlier identification of security issues, increased adoption of secure development practices, greater participation in security initiatives, or fewer recurring issues within the teams supported by champions.

Sustaining engagement and developing future talent

Many champions take on this role in addition to their primary responsibilities. As a result, recognition plays an important role in sustaining engagement. Organizations can acknowledge champion contributions by highlighting their achievements in internal forums, recognizing their efforts during engineering meetings, or offering investment in further cybersecurity learning.

Another way to sustain engagement is to create a visible path for champions to continue developing their skills. For example, some organizations use an online secure-coding dojo where engineers can progress through internal certification levels, from white and yellow belts through green, blue, brown, and black belts. When incorporated into a Security Champions Program, this type of progression can create healthy competition while giving participants a clear incentive to continue building their security skills. The recognition associated with advancing to the next level can also make participation more visible within engineering teams.

The same opportunities that keep champions engaged can also help develop future security talent. If the program generates strong interest, consider introducing a rotation model that allows additional employees to participate over time. Rotations distribute the workload and expose more employees to security practices. In some cases, the champions program could also become a way to identify individuals who may be interested in pursuing security roles in the future, creating a natural talent pipeline into the security organization.

While a Security Champions Program is an effective way to scale security influence through embedded volunteers, there are limits to what can be achieved without formal accountability and dedicated ownership. As business complexity, regulatory obligations, and risk exposure increase, organizations may need a more formal model. The BISO role builds on many of the same principles while providing dedicated accountability and a more strategic partnership with business leaders.

Implementing a BISO model

BISOs extend the influence of the security organization by partnering closely with specific business units. Rather than operating solely from a centralized security team, BISOs work with product, engineering, and other leaders to ensure security considerations are incorporated into strategic decisions.

Because BISOs participate in planning discussions, roadmap reviews, and major initiatives, they can introduce security perspectives earlier in the decision-making process. Equally important, BISOs bring feedback from the business back to the security organization. This feedback helps security leaders understand priorities, operational constraints, and areas where security controls may need to evolve.

For example, when a business unit plans a new product launch or adopts new technologies, a BISO can help identify security and regulatory considerations early. At the same time, the BISO may surface feedback from engineering teams about friction in secure development processes or tooling. This allows the security organization to refine guidance, improve developer experience, and align security controls more closely with how teams actually build and operate systems.

While Security Champions typically operate at the team level within engineering or product groups, BISOs operate at the business-unit level, working directly with leadership to align security priorities with broader business objectives. Together, these roles help extend security influence across both technical teams and organizational leadership.

Introducing or uplifting the BISO model

Like Security Champions programs, BISO models vary depending on the organization's maturity and structure. Some organizations establish dedicated BISO roles embedded within major business units, while others assign existing security leaders to support specific divisions alongside their primary responsibilities.

If a BISO model does not yet exist, start by identifying the business units that represent the highest level of organizational risk rather than attempting to support every function equally. Your enterprise risk assessment, regulatory obligations, critical business services, and strategic initiatives should help determine where dedicated business alignment will provide the greatest value.

Select individuals who can translate between business and security rather than focusing solely on technical expertise. Strong BISOs understand security, communicate with executives, build trusted relationships, and influence decisions without direct authority. Provide BISOs with onboarding that introduces the organization's business strategy, operating model, risk appetite, governance processes, and security program. Because BISOs spend much of their time working with business leaders, understanding the business is just as important as understanding security.

For example, an organization beginning its BISO program may initially assign dedicated BISOs to the payments, cloud infrastructure, and customer platforms because they represent the organization's highest concentration of operational and regulatory risk. As the program matures, additional business units can be incorporated.

If the organization already has a BISO structure in place, focus on strengthening consistency, accountability, and outcomes. Establish a regular engagement cadence with business leaders, clarify responsibilities across the first and second lines of defense, and ensure BISOs participate in strategic planning rather than only responding to security requests. Regardless of the structure, align expectations for the role.

If the BISO responsibility is performed alongside another full-time position, the level of engagement will naturally be more limited. Organizations that establish dedicated BISO roles should define clear objectives and success metrics to measure their impact. For example, rather than measuring the number of meetings a BISO attends, evaluate how the business they support is improving.

As discussed in *Chapter 2*, Business Security Scorecards provide an effective way to measure this progress. Improvements in vulnerability remediation, risk acceptance, and audit performance provide a clearer indication of impact than activity-based metrics alone. As the program matures, involve BISOs earlier in strategic initiatives, acquisitions, major technology transformations, and product planning. This positions security as a business partner rather than a late-stage reviewer.

Sustaining strategic business partnerships

Building strong relationships with business leaders takes time and requires consistent engagement. The best BISOs do not limit interactions to quarterly reviews or risk discussions; they become trusted advisors who understand the business, anticipate upcoming initiatives, and bring security into conversations early.

For example, if a business unit is planning to expand into a new market, accelerate AI adoption, launch a new product, or acquire another company, the BISO should communicate those developments back to the security organization as early as possible. This allows security teams to anticipate new risks, adjust priorities, and support the business before key decisions are made.

Over time, these relationships become increasingly proactive. Rather than waiting to be invited, business leaders begin seeking the BISO's perspective when evaluating strategic initiatives, making technology investments, or assessing business risk. That shift, from reacting to requests to being included in important business discussions, is one of the best indicators that the partnership is progressing.

Table 10.1 summarizes how Security Champions and BISO programs differ in scope, responsibilities, and how they extend the reach of the security team. Together, these programs expand the influence of the security team across the organization.

Characteristic	**Security Champions**	**Business Information Security Officers**
Primary Purpose	Embed security into engineering and product teams	Align security strategy with business priorities
Typical Participants	Engineers, developers, architects, product managers	Dedicated security professionals
Primary Stakeholders	Engineering and product teams	Business executives and business unit leaders

Characteristic	Security Champions	Business Information Security Officers
Scope of Influence	Team or project level	Business unit or enterprise level
Time Commitment	Volunteer role alongside primary responsibilities	Dedicated or formally assigned responsibility
Primary Focus	Secure development and day-to-day practices	Supporting high-risk or business-critical functions
What Success Looks Like	Scaling security across technical teams	Integrating security into business decisions and priorities

Table 10.1 – Comparing Security Champions and BISO programs

Extending reach alone is not enough. Employees should also understand how to apply security in their day-to-day work. This is where structured education becomes essential to the program's success.

Designing security education programs

Security controls play a critical role in protecting an organization, but they cannot address all risks. It only takes one misconfigured server, an unpatched vulnerability, or a single phishing email to create significant exposure. Many cybersecurity leaders come from technical security roles where education efforts were primarily directed within their own teams. As a security executive, this scope expands. Security education becomes an organization-wide effort that helps bring employees along the journey and enables them to play an active role in protecting the company. In our opinion, it is one of the most rewarding parts of the job when an employee reaches out to report "something suspicious" and prevents a major incident because of a simple email or call.

Designing an effective security education program requires more than sending occasional reminders or tracking compliance with your annual training module. It should include three main elements: awareness, training, and testing. Together, they create a continuous learning cycle that helps employees recognize and respond to threats.

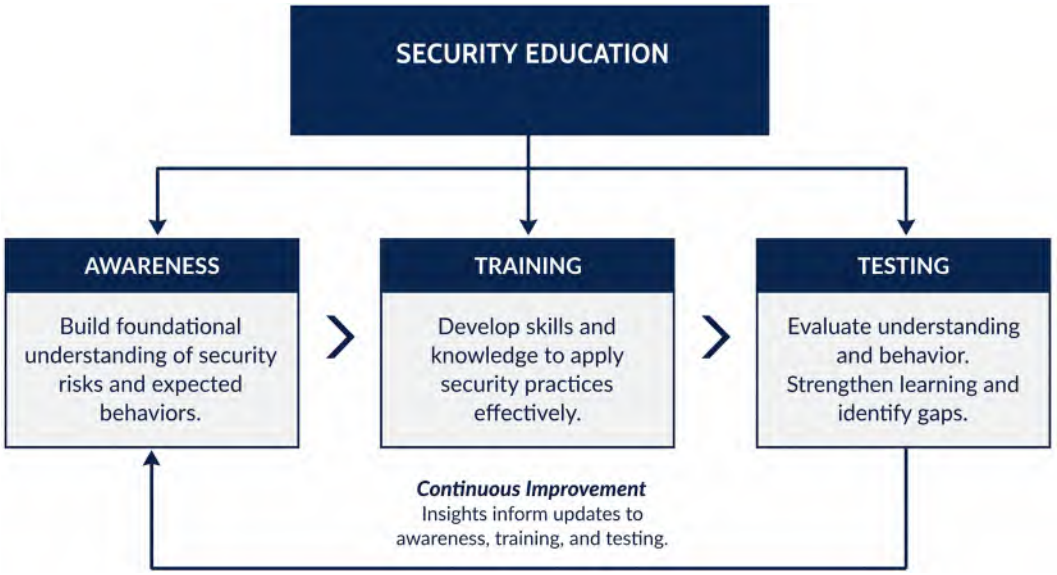


Figure 10.2 – Key components of a security education program

In this section, we will explore how to design each of these elements and conclude with a practical awareness program calendar that brings the different activities together throughout the year.

Establishing continuous security awareness

Many organizations have an awareness program because they are required to meet compliance or regulatory requirements, typically as an annual training module or a policy acknowledgment. While this approach satisfies compliance expectations, it rarely changes behavior.

A strong awareness program balances recurring risks with emerging threats. Some topics, such as **business email compromise (BEC)**, credential phishing, ransomware, and tax-season impersonation scams, should be reinforced regularly because employees are likely to encounter them year after year. Other topics require timely communication as new attack techniques or industry incidents emerge. A once-a-year compliance module cannot keep pace with this change. Instead, awareness should operate as a continuous program that reinforces known risks while adapting its messaging throughout the year.

Continuous awareness relies on repeated, timely touchpoints rather than a single annual event. These interactions should include a small number of practical behaviors, such as recognizing suspicious activity, pausing before acting, and knowing when and how to report a concern. The specific communication channels may vary across the organization and are

discussed later in this section. Over time, these repeated interactions help shift awareness from a compliance exercise to an organizational habit.

Defining the core components of awareness

A solid security awareness program typically combines several complementary components that help employees understand security expectations and develop basic cybersecurity skills. Understanding the role of each component helps security leaders design programs that strengthen the organization's overall security posture while also meeting compliance requirements. *Table 10.2* provides an overview of the components of the awareness program:

Program Component	**Purpose**	**Characteristics**	**Examples**
Compliance Modules	Ensures employees understand regulatory obligations, internal policies, and required security practices	Often mandatory and typically delivered through structured modules during onboarding and on a recurring basis; topics change relatively infrequently and focus on organizational policies and regulatory requirements	Acceptable use policies, data protection responsibilities, privacy obligations, incident reporting, and periodic policy acknowledgments
Security Education: Recurring Threats	Builds cybersecurity awareness around common threats employees encounter regularly	Recurring awareness campaigns and ongoing messaging throughout the year	BEC, credential phishing, ransomware awareness, password hygiene, seasonal scams such as tax-related fraud

Program Component	Purpose	Characteristics	Examples
Security Education: Emerging Threats	Keeps employees informed about new attack techniques as the threat landscape evolves	Updated periodically as attackers introduce new methods or as the security team observes new patterns	New phishing techniques, deepfake impersonation attempts, newly discovered vulnerabilities, or attack patterns reported across the industry

Table 10.2 – Primary components of an awareness program

Delivering through diverse communication channels

Security awareness programs rely on multiple communication channels to bring security awareness across the organization. While formal training plays an important role, many of the most effective awareness moments occur through everyday interactions such as short reminders in collaboration tools, discussions during team meetings, or organization-wide campaigns that highlight emerging risks.

Table 10.3 outlines common communication channels security teams use for security awareness and when each channel is most effective.

Communication Channel	Purpose	When to Use
Collaboration Platforms (Slack, Teams)	Deliver short, timely reminders and alerts directly in employees' daily workflow	When responding to active phishing campaigns, to share quick security tips in real time
Internal Newsletters or Security Bulletins	Provide broader updates on security topics and key awareness themes	Monthly or quarterly updates highlighting emerging threats, lessons learned from incidents, or awareness campaigns

Communication Channel	Purpose	When to Use
Intranet or Knowledge Portals	Serve as a centralized location for security resources and reference materials	When employees need step-by-step guidance, reporting instructions, policy references, or access to awareness materials
Company Meetings or Town Halls	Deliver security messages at the leadership level and demonstrate organizational commitment to security	When sharing major security updates, discussing lessons learned from incidents, or recognizing employees who contributed to security efforts
Team Meetings/ In-Person Engagements	Deliver targeted security guidance tailored to the risks faced by specific teams	When addressing role-specific threats, for example, meeting with HR to discuss remote employee risks or with finance to review impersonation and payment fraud scenarios
Webinars or Live Training Sessions	Provide deeper learning on specific security topics while allowing employees to ask questions	When introducing new security initiatives, discussing emerging threats, or providing focused training to particular business units
Lunch and Learn/ Brown Bag Sessions	Create informal opportunities for employees to learn about security topics in an open, conversational setting	When introducing new topics, discussing recent incidents, or encouraging employees to engage directly with the security team
New Employee Onboarding	Introduce employees to security expectations and reporting processes at the start of their employment	During orientation sessions to explain security policies, reporting procedures, and common threats employees may encounter

Communication Channel	Purpose	When to Use
Dedicated Security Awareness Events	Focus organizational attention on key security topics through coordinated activities	When running organization-wide initiatives such as Cybersecurity Awareness Month, phishing awareness campaigns, or themed security weeks
Digital Signage/ Office Screens	Passive reminders placed in common office areas	When displaying security tips, reporting instructions, or campaign messaging on screens in offices, cafeterias, or common spaces

Table 10.3 – Communication channels

If you are building an awareness program from scratch, start with two or three communication channels that best fit your organization's culture and focus on executing them consistently. As the program matures, additional channels can be introduced to expand reach.

Delivering meaningful security training

While awareness programs help keep security visible across the organization, training provides the structured instruction employees need to apply secure practices in their daily work.

A comprehensive training program focuses on practical guidance that employees can apply in real-world situations. It also recognizes that not all employees face the same risks, and therefore training should be structured to address the needs of different roles within the organization.

Distinguishing security awareness from security training

Security awareness and security training are often used interchangeably but serve different purposes within a cybersecurity program.

- Awareness focuses on maintaining visibility of security risks across the organization. It reinforces key messages through ongoing communication such as security tips,

newsletters, campaigns, or reminders tied to emerging threats. The goal is to keep security top of mind.

- Training focuses on developing specific knowledge and skills. It is more structured and designed to ensure employees understand how to perform certain actions safely.

For example, awareness messaging may remind employees to remain cautious when opening email attachments. Training teaches employees how to identify phishing indicators and what steps to take when they encounter suspicious messages.

Structuring training for different employee populations

Not all employees face the same risks. A mature security training program recognizes these differences and tailors instruction accordingly:

- Most organizations begin with baseline training that applies to all employees. It establishes a common foundation so that every employee understands the organization's basic security expectations and knows how to respond when something appears suspicious. These sessions are delivered through structured learning modules or interactive lessons and are often completed during onboarding and refreshed periodically.
- Beyond baseline training, many organizations introduce role-based training that focuses on risks specific to particular teams or functions. *Table 10.4* provides some examples:

Population	**Sample Training Focus**
Finance	BEC, payment fraud, invoice manipulation
Engineering/Developers	Secure coding practices, vulnerability management, dependency security
Executives	Targeted phishing and impersonation attacks, travel security risks
Human Resources	Protection of employee data and risks associated with remote workforces

Table 10.4 – Sample training focus

Organizations may also identify high-risk populations, or groups that attackers frequently target, such as frontline teams, help desks, executive assistants, and C-suite members, and provide additional training tailored to their exposure. For example, most major email security

providers offer specific "top target" reports that rank users based on the frequency, severity, and sophistication of the phishing emails they receive. Aligning training with employees' responsibilities helps ensure the content remains relevant and practical rather than becoming a generic compliance exercise.

Reinforcing learning through testing

Security testing tends to divide opinions: Some leaders see it as essential, while others feel it creates frustration or unnecessary noise. In practice, its value depends on how it is implemented.

If testing is introduced too early or without context, it can feel like a "gotcha" moment. In such cases, employees do not understand what they did wrong, and the exercise creates more resistance than learning. When testing follows awareness and training, it becomes a natural next step and an opportunity to apply what people have already learned.

In this section, we focus on three complementary approaches to security testing: phishing simulations, tabletop exercises, and live exercises. We then explore how gamification can increase participation and how exercise findings should be documented and managed.

Using phishing simulations as a learning tool

Phishing simulations are among the most debated tools in security awareness. Supporters view them as a practical way to practice learning and identify where additional education is needed, while critics argue that they can feel punitive, damage trust, or focus too heavily on click rates rather than behavior change. Their value therefore depends less on the technology, which is now widely available through email security platforms, specialized vendors, and AI-enabled tools, and more on how the exercise is designed, communicated, and followed by timely feedback.

Best practice is to aim for one or two cross-company simulations each year, with specific simulations for target audiences as needed. Keep in mind that this tool becomes ineffective when organizations lean toward overuse. There are organizations that send thousands of phishing emails every month without investing in awareness. At that point, you are not improving behavior; you are setting employees up to fail.

Cadence and intent are both important. If you are going to run phishing simulations, make sure they connect to something employees have already learned. For example, if you just ran a campaign on credential phishing, follow it with a simulation that tests that specific pattern. Then measure the relevant metrics such as reporting rates, time to report, and how quickly employees recognize something is off.

Tip

Be careful when impersonating known brands, partners, or regulators. You may have employees reach out to them to inquire about the email, resulting in impact to the broader relationship. I learned this firsthand when we used a well-known financial regulator in a phishing simulation. Several employees contacted the regulator directly, creating more friction than I had anticipated. The experience highlighted the importance of assessing potential external consequences and coordinating with the appropriate internal stakeholders before using a real organization's identity.

Using tabletop exercises to improve decision-making

Tabletop exercises are where you start to drive more engagement. These are discussion-based scenarios where you bring together cross-functional teams or executives to walk through an incident. While there are technical aspects, the focus is decision-making based on available information.

It is recommended to run one tabletop exercise in your first year. However, if the overall maturity level of the program is low or you cannot schedule the exercise until late in the year, it may be more valuable to move it into your second year. In most cases, begin with a technical exercise, which tests how incident responders investigate, contain, and recover from a simulated event using established tools and procedures. Follow with a management exercise, which focuses on how executives and business leaders make decisions, coordinate across functions, communicate with stakeholders, and manage the broader organizational impact of an incident.

If you have never facilitated an exercise before and do not have the budget to bring an external facilitator, consider starting with the **Cybersecurity and Infrastructure Security Agency (CISA)** library. They provide canned scenarios that can be easily modified to meet your exact needs. Another option would be using your sector's **Information Sharing and Analysis Center (ISAC),** such as **Financial Services Information Sharing and Analysis Center (FS-ISAC)** or **Healthcare Information Sharing and Analysis Center (H-ISAC)**.
Their tabletop materials are generally included in the membership.

Preparation is what makes or breaks these sessions. You want the scenario to feel realistic enough to engage people, but not so detailed that you get stuck debating whether every step is technically feasible. Be mentally prepared to have someone say, "*This wouldn't happen here.*" Do not get pulled into that debate. Instead, bring the conversation back to what matters, such as "*What decisions would we need to make?*" or "*Where do we have gaps?*"

A good tabletop does not prove that your plan is perfect. It helps you see where it is not. For example, in a ransomware scenario, leadership may need to decide whether to shut down systems, how to communicate with customers, and when to involve regulators. Those decisions are often even more complex than the technical response.

Conducting live exercises to validate readiness

Live exercises are a different level entirely. This is where you move beyond discussion by requiring teams to respond to an authorized, controlled attack conducted within the organization's real network. Instead of explaining how they would respond to ransomware, participants investigate exercise-generated alerts, coordinate across functions, contain the simulated threat, and make decisions in real time using the organization's existing tools and processes.

These exercises may incorporate the Red Team, Purple Team, or other adversary-simulation capabilities discussed in *Chapter 6*. The objective here is broader than testing an individual control: it is to observe how detection, response, and coordination work together when teams must respond in real time.

Note

A word of caution: people are usually uncomfortable with this step since live exercises carry substantially more operational risk than discussion-based tabletops. An error in the scenario or execution could disrupt production, affect critical services, or cause simulation tools and payloads to behave in unintended ways. For this reason, live exercises are usually better suited for your second year, after the organization has completed several tabletops, clarified decision-making authority, and addressed findings from earlier exercises. Before proceeding, establish a tightly controlled scope, identify systems that are off-limits, define rollback procedures, obtain the appropriate approvals, and give designated leaders the authority to stop the exercise immediately if conditions become unsafe.

The difference between discussing risk and experiencing it is significant. In a live exercise, you quickly see whether your detection works, whether teams know what to do, and how well coordination holds up under pressure. For example, you might simulate a compromised account or lateral movement and ask the security team to investigate and contain it while IT and business teams support the response.

> **Note**
>
> Organizations that run live exercises tend to have a clearer understanding of their actual readiness. It is one of the strongest signals that a program is moving toward a higher level of maturity. Executed at the right time, the exercise will serve as a validation of all the work you have done to date.

Regardless of what type of testing you perform, whether just one or all three, if testing uncovers gaps, treat it as a positive outcome and communicate it this way. These exercises are designed to surface weaknesses in a controlled environment. You should use those insights to improve processes, training, and coordination before the next exercise.

Using gamification as part of testing

Some organizations have found that incorporating elements of gamification can improve engagement in security programs. It introduces interactive challenges, rewards, and friendly competition that encourage employees to participate.

For example, one Fortune 500 technology company created an internal security program where employees earned points and badges for reporting phishing emails, completing security challenges, and identifying potential risks. Leaderboards highlighted top contributors, and they were celebrated on a quarterly basis.

Similar programs often include the following elements:

- Interactive simulations where employees practice identifying suspicious activity
- Micro-learning challenges that break security education into short tasks
- Real-time feedback explaining which indicators were missed
- Recognition and rewards such as badges, points, or leaderboard rankings

By rewarding positive behaviors rather than punishing mistakes, gamification can help transform security awareness into an engaging and continuous learning experience.

Managing exercise documentation and legal privilege

Tabletop and live exercises may expose significant gaps in technical readiness, executive decision-making, regulatory response, or cross-functional coordination. Before the exercise, work with your legal team to determine how it should be structured, documented, and shared. When the exercise is conducted under attorney-client privilege, organizations typically engage an external facilitator through counsel to run the session and prepare the detailed findings. Privilege is not automatic simply because counsel or an external party is involved, so the legal

team should define the engagement, reporting relationship, and handling of materials in advance.

You may still need to demonstrate to regulators, auditors, customers, or the board that an annual exercise was completed. Consider maintaining a one-pager including the date, scenario, scope, participants, and assigned follow-up actions, while placing detailed findings and remediation priorities in a separate, access-restricted report. This allows the organization to demonstrate completion and accountability without broadly distributing sensitive observations about control gaps or response weaknesses.

Tip

The structure will depend on the jurisdiction and circumstances. Make these decisions with counsel before the exercise rather than after sensitive findings have already been documented and circulated.

Building a security education calendar

Once the key elements of the education program are defined (awareness, training, and testing), the next step is coordinating them into a structured annual plan. A calendar helps security teams maintain a consistent rhythm of engagement across the organization and provides a simple way to align these efforts and communicate upcoming activities to internal partners such as HR, IT, and corporate communications.

Many organizations also use **Cybersecurity Awareness Month** in October as a focal point within the calendar. Because employees are often exposed to external messaging during this time, it provides a natural opportunity to amplify internal activities such as awareness campaigns, training refreshers, or interactive challenges.

Note

While Cybersecurity Awareness Month can generate strong engagement, it should complement a year-round program.

The following example illustrates how awareness, training, and testing activities can be coordinated across a typical year. *Table 10.5* focuses on the types of activities that may occur during each period; the specific delivery methods may vary depending on the organization's culture and communication practices:

Month	Awareness Activities	Training	Testing
January	New Year security reminders	Annual compliance training modules	—
February	Phishing awareness messages	—	Phishing simulation
March	Credential security campaign	Role-based training (engineering)	Tabletop ransomware
April	Data protection reminders	—	Targeted phishing simulation
May	Privacy and data handling awareness	Privacy compliance training	—
June	Travel and remote work security reminders	—	—
July	Mid-year security tips campaign	Executive security briefing	—
August	Secure collaboration and file sharing awareness	—	Targeted simulation
September	Pre–Cybersecurity Awareness Month communications	—	Phishing simulation
October	Cybersecurity Awareness Month campaign	Refresher training sessions	Gamified phishing challenge
November	Holiday shopping and scam awareness	—	Targeted phishing simulation

Month	Awareness Activities	Training	Testing
December	Year-end security reminders	Optional refresher modules	—

Table 10.5 – Sample security calendar

Establishing a calendar such as the one suggested in the preceding table helps security leaders coordinate efforts across teams, maintain visibility of security topics throughout the year, and create a predictable cadence that employees can recognize and engage with.

You should coordinate the activities listed in the preceding table with the broader Technology organization to avoid a situation where your events conflict with theirs, and vice versa. It is one of the easiest ways to drive alignment and greater participation. For example, if your developer training event conflicts with a sprint planning meeting, you can guess which one they are going to attend.

Lasting culture change requires visible support from leadership. The next step is ensuring that executives and the board model and promote these behaviors.

Influencing C-suite and board security culture

When executives and board members consistently include security in their discussions and decisions, they signal that security is a business priority rather than solely a security-team responsibility. In this section, the focus shifts from how to communicate with leadership, covered in *Chapter 9*, to how ongoing executive engagement can help shape the organization's security culture.

Early in your tenure, executives form their perception of how you operate. Your communication style can help build credibility and position you as a strategic partner. In this section, we will focus on two key approaches to influencing executive and board security culture: proactive communication during emerging events and structured, ongoing engagement.

Responding to emerging threats through proactive communication

Executives are constantly exposed to security incidents in the news. When a major breach occurs, they often ask themselves: *"How does this apply to us?"*

Please, do **not** wait for that question to come to you. Building on the executive communication principles introduced in *Chapter 9*, a concise emerging-event update can answer five practical questions:

- What happened? (2–3 sentences)
- What were the results or impact? (1–2 sentences)
- Do we have exposure? (confirmed exposure, no exposure identified, or assessment underway)
- What are we doing about it? (containment, mitigation, or assessment actions, as applicable)
- How often will status updates be provided? (daily, weekly)

This simple format enables executives to understand the situation and engage in informed conversations. For example, following a widely publicized ransomware attack in your industry, you could proactively send a short update confirming whether your organization is exposed and outlining any measures already in place.

In some cases, these moments can also be used to highlight gaps. For instance, perhaps the organization was not impacted but could have been. In other words, you were lucky, but you do not want to rely on luck in the future. Consider using this context to explain what additional controls or investments are needed to reduce future risk.

Many new security leaders assume that "*C-suite doesn't care about these things*." This could not be further from the truth. They do care and often have not experienced proactive engagement from security before. From our experience, it is one of the easiest opportunities to act on in your first year.

Note

Some executives may initially question why the update is needed, especially if they are not used to proactive security updates. Others may even ask to opt out of the updates; do not treat this as a sign of failure. Continue to communicate with those who are willing to listen, even if it translates into a reduced audience. Over time, you may be able to win them back.

Establishing ongoing engagement

Ad hoc updates address immediate concerns. As an executive looking to influence culture, you also need consistent and structured engagement with leadership.

In many organizations, cybersecurity engagement with the C-suite or the board is limited to an annual update. This frequency may meet regulatory expectations or check the box, but it is rarely sufficient. To strengthen engagement, consider incorporating the following practices:

- **External experts**: Bring external experts, such as law enforcement, outside counsel, or consulting partners, to provide an education session. They can bring broader industry context and help leadership better understand the value of security investments. External perspectives can validate the direction of your program. Choose the speaker carefully, because the audience will often associate the quality of the session with your judgment and the credibility of the security organization. Before the session, brief the speaker on the audience, objectives, key messages, and appropriate level of detail so the session supports your broader goals.

> **Tip**
>
> Separately, review the planned content with your direct management team before presenting it to the C-suite or board. Confirm what will be covered, what will remain outside the scope, and where sensitive questions may arise. This preparation helps avoid surprises and gives your leadership team the context they need to support the discussion.

- **Executive tabletop exercises:** Similar to the testing approaches discussed earlier in this chapter, executive tabletop exercises allow executives to practice decision-making during a simulated incident. These sessions focus on business impact, including communication, legal considerations, and operational trade-offs. It is your opportunity to demonstrate that you have prepared the company for the scenario through collaboration with others. Ideally, the executive exercise is the final step after conducting a series of technical exercises.

Before scheduling an executive tabletop exercise, consult your legal team to determine whether attorney-client privilege should apply and how the exercise should be facilitated and documented. Refer to the section *Managing exercise documentation and legal privilege* earlier in this chapter for additional guidance.

In conclusion, executive engagement is about increasing awareness and enabling better decisions. When leaders are equipped with the right context, structure, and practice, they are more likely to prioritize security needs. You will know the culture is taking hold when you see the following behaviors:

- Executives proactively ask security-related questions during discussions.
- Leadership references security considerations in business decisions.

- Board members engage in conversations beyond compliance-driven updates.
- Security is discussed in terms of business impact, not technical detail.

Executive engagement, combined with Security Champions, BISOs, and security education programs, enables a security-first culture where security is a shared responsibility across the organization.

Notes from the field with Renana

Case study: making security everyone's business

Most companies will tell you cybersecurity is a priority. They may cite budget allocations, dedicated headcounts, or the latest tools they have deployed. It all sounds compelling on paper. The data, however, tells a different story.

When you walk into an organization and find thousands of unpatched vulnerabilities sitting unaddressed, a backlog of overdue audit findings with no clear owner, no KRIs in place to signal where the organization stands, and a thirty-minute C-suite update happening once a year, you are looking at a culture where security is not really a priority. It is a talking point.

No matter what organization you join, no matter what you inherit, the culture becomes your responsibility the moment you step into the role. Early on, I believed that security was something I could carry personally. I put in the long nights. I held the one-on-ones. I built presentations. And while those efforts had real value, their reach was limited to the rooms I could physically be in and the conversations I could directly have. That approach does not scale, not at a mid-sized company, and certainly not inside a Fortune 500.

One of the most important shifts I made as a security executive was letting go of the idea that security belonged to the cybersecurity team. Security is a shared responsibility across every function, every team, and every employee. There is no program, no tool, and no headcount large enough to substitute for that. The mission of a cybersecurity leader goes beyond protecting the organization to helping the employees understand that they are part of the protection.

The programs outlined in this chapter often take months, and sometimes years, to see measurable impact. They are not quick wins. Each one represents a layer, another strand woven into the fabric of how the organization thinks and acts.

I did not have a playbook when I started investing in culture. I built these programs over time, through trial and error, learning from what worked and adjusting what did not. Through that, a few principles have stayed with me.

Start small. You do not need a large budget or a perfect plan to begin. In today's environment, with the tools available through AI and modern platforms, the barrier to entry is lower than it has ever been. What matters is getting started.

Be consistent. Whether you begin with an awareness campaign, a phishing simulation program, a Business Information Security Officer model, or a series of honest conversations with leadership, showing up consistently over time is what creates change. Sustained effort matters more than any single initiative.

Watch for behavior, not just metrics. When people across the organization begin making cybersecurity a priority on their own, without being prompted or without a policy requiring it, the culture is shifting. That is the signal that the work is landing.

You will know it is working when signals start to emerge. For instance, security comes up organically in management meetings, not because someone put it on the agenda, but because leaders are asking about it. Developers adopt security tooling not because it is mandated, but because they trust it and understand why it matters. The data begins to reflect it too: risk trends downward, remediation improves, and adoption increases.

I saw this firsthand. Watching the signals emerge—the conversations, the behaviors, the data—was one of the most rewarding experiences of my career. It did not happen all at once, but it started with believing it was possible.

The work of building a security culture can feel slow and, at times, invisible. You will put energy into programs that take years to pay off. You will have conversations where you are not sure anything landed. You will look at the data and wonder if the needle is moving.

Little by little, you will bring others on the journey with you. And when you look back, you will see that the most important thing you built was not a program or a framework; it was a security-first culture where everyone felt a shared sense of responsibility.

Summary

In this chapter, we explored how to build a security-first culture by extending ownership across the organization. We examined how Security Champions and Business Information Security Officers can expand the security team's influence. We also discussed how continuous awareness, training, and testing can improve employee readiness, and how consistent engagement with C-suite and the board can make security a regular part of business discussions. Culture develops through sustained effort, and one of the clearest signs of progress is when employees and leaders begin considering security as part of their everyday decisions.

In *Chapter 11*, we will examine how to measure and communicate the impact of this work through meaningful metrics that help stakeholders understand where the program is improving and where additional attention is needed.

Chapter checklist

- **Launch or uplevel Security Champions or BISO programs.** Define clear ownership, expectations, operating cadences, and measures of success appropriate to each model.
- **Build a 12-month security education calendar.** Coordinate awareness, training (including Cybersecurity Awareness Month), and testing activities throughout the year.
- **Communicate proactively with executives.** Send timely briefings on relevant industry incidents to help leadership understand their potential impact on the organization.
- **Schedule a tabletop exercise appropriate to the program's maturity.** Begin with a technical exercise before advancing to an executive session as the organization becomes ready.

Additional resources

- Sample security education calendar: `https://bit.ly/CISOBook26`
- CISA tabletop materials: `https://bit.ly/CISOBook27`

11

Proving Your Impact: Measuring Success and Demonstrating Value

Throughout this book, we have focused on helping you build the foundation of an effective security program. You have worked to improve the organization's security posture and, eventually, like every leader, will face the same question from executive leadership, the board, or even yourself: How do we know if we are making a difference?

Security executives are expected to demonstrate progress, justify investments, communicate business value, and show that the security program is progressing over time. This is not demonstrated solely by the number of security tools deployed, the number of vulnerabilities remediated, or the volume of alerts investigated. While those activities are important, they are only part of the story. Earlier in the book, we discussed aligning security with business objectives, understanding organizational priorities, managing risk, and establishing governance. Measuring success builds upon those foundations. Without understanding the business, it is difficult to select meaningful metrics. Without a clear strategy, measurements become disconnected from organizational goals. Without governance, metrics lose credibility because there is no consistent way to validate progress or hold risk owners accountable.

This chapter addresses those questions. More importantly, it is about selecting measurements that influence decisions rather than simply filling dashboards.

Metrics should help prioritize investments, identify opportunities for improvement, strengthen conversations with stakeholders, and demonstrate that security is creating measurable value for the organization.

In this chapter, we will explore the following topics:

- Defining meaningful security metrics that align with business objectives
- Demonstrating the **return on investment (ROI)** of security initiatives
- Measuring security program maturity and operational effectiveness
- Communicating security outcomes to technical and non-technical audiences

Defining meaningful security metrics that align with business objectives

Security Information and Event Management (SIEM) platforms generate millions of events each day. Vulnerability scanners identify thousands of vulnerabilities. Endpoint protection platforms continuously look for suspicious activity. Identity systems record countless authentication events. Dashboards multiply, reports become longer, and before long everyone is looking at hundreds of metrics.

But ironically, despite having more data than ever before, many organizations struggle to answer one very simple question: *Is our security program becoming more effective?* You could quickly lose credibility as a security executive by overwhelming leadership with numbers that do not tell a story.

The answer is rarely found by adding another dashboard or collecting another metric. Instead, it comes from selecting measurements that tell a meaningful story about the organization's ability to manage cyber risk while enabling the business to achieve its objectives.

Security metrics should never exist in isolation. Every metric you report should help explain how security contributes to business success.

Earlier in your career, success may have been measured by operational accomplishments such as how many vulnerabilities you remediated, how many incidents you investigated, or how quickly your team deployed a new security control. Those activities remain important, but executive leadership evaluates success differently.

This is one of the biggest mindset shifts many new security executives must make. The questions shift from operational to strategic, for example:

- How resilient is the organization against DDoS attacks?
- How long will it take to recover from a ransomware attack?
- How secure is the usage of AI?

One mistake you should avoid is selecting metrics based on the capabilities of your security tools rather than the priorities of the business. Security tools are excellent at generating data such as blocked malware, phishing attempts, firewall events, privileged account usage, and

hundreds of other technical measurements. The problem is that most of these metrics do not answer the questions that executives are asking.

Imagine presenting the following statement to your CEO: "*We blocked 8.7 million phishing emails this quarter*." It sounds impressive, right? But what should the CEO do with that information? Is eight million good? Is it bad? Is the number increasing because attackers are targeting the company more aggressively, or because the email security platform became better at detecting malicious messages? Without context, the metric becomes little more than an interesting statistic.

Now let's change the way we present the information: "*We have seen an 11X increase in the number of phishing attacks. Out of them, less than 1% were delivered to employee mailboxes. This quarter, 42% of all employees reported at least one phishing email. This suggests our awareness program and email protection investments are improving our stance against phishing attacks.*"

Notice that this last statement tells a story. It connects security activities with business outcomes. It explains not only what happened but why it matters. *Table 11.1* shows additional examples of what to measure and why it matters:

Instead of measuring	**Measure**	**Why it's important**
Number of vulnerabilities	Percentage of critical business systems meeting remediation objectives	Demonstrates whether the organization's most important assets are being protected within agreed risk tolerances, rather than simply counting findings
Number of security awareness training sessions completed	Reduction in successful phishing attempts Improvement in employee reporting rates Decrease in credential compromise	Measures whether security awareness is changing employee behavior and reducing organizational risk instead of tracking training attendance alone

Instead of measuring	Measure	Why it's important
Number of endpoint agents deployed	Percentage of critical assets continuously monitored by security controls	Focuses on security coverage of the organization's crown jewels, ensuring visibility where it matters most rather than measuring deployment volume

Table 11.1 – Measuring what matters

Operational teams need different metrics to run the security program. The objective is to ensure that the metrics presented to leadership explain business value rather than technical activity.

Every metric should answer a business question, and a simple exercise that you can do as you review the metric in the dashboard is to ask yourself: What business question does this metric answer?

Table 11.2 has examples of business questions and possible metrics that you can use:

Business question	Possible metrics	Rationale
Can we detect attacks quickly?	**Mean time to detect (MTTD)** Percentage of high-severity alerts investigated within the SLA Percentage of monitored critical assets	Early detection reduces attacker dwell time and limits the potential business impact of a security incident. These metrics measure the organization's ability to identify malicious activity before it escalates into a significant breach.
Can we recover from major disruptions?	**Recovery time objective (RTO)** achievement Disaster recovery exercise success rate Critical application recovery readiness	Cyber resilience is measured not only by preventing attacks but also by the organization's ability to restore critical business operations quickly. These metrics demonstrate operational preparedness and business continuity capabilities.

Business question	Possible metrics	Rationale
Are we reducing business risk?	Reduction in critical risks over time Percentage of risks with approved remediation plans Residual risk trend	Executive leadership needs visibility into whether the organization's overall risk exposure is improving. These metrics demonstrate progress in managing, mitigating, or accepting risks through a structured governance process.
Are our security investments improving security?	Attack surface reduction	Security investments should produce measurable outcomes. These metrics help demonstrate whether investments are reducing organizational exposure and strengthening the effectiveness of the security program rather than simply adding new technologies.

Table 11.2 – Business questions and metrics

Executive dashboards bring these measurements together. They should show whether controls are becoming more effective, whether performance is improving compared with the previous quarter, and whether the business's most critical assets are protected.

Operational metrics vs. executive metrics

Earlier in this section, we emphasized that executive metrics should focus on business outcomes rather than technical activity. That does not mean operational metrics are less important. In fact, operational metrics are what enable security teams to manage the day-to-day health of the security program. The difference is not whether one set of metrics is more valuable than the other; it is that they serve different audiences and support different decisions. Operational metrics help security teams answer questions such as:

- Are endpoint agents healthy and reporting?
- Are critical vulnerabilities being remediated within SLA?
- Is the **security operations center (SOC)** investigating alerts within expected timeframes?

- Are backup jobs completing successfully?
- Are identity governance processes operating correctly?

These metrics are reviewed daily or weekly because they help teams detect operational issues before they become business problems. Executive metrics, on the other hand, answer broader questions:

- Is cyber risk increasing or decreasing?
- Are we becoming more resilient?
- Are our security investments delivering measurable value?
- Are we meeting our regulatory obligations?
- Are our highest business risks being reduced?

A useful way to think about the relationship is that operational metrics drive execution, while executive metrics drive decisions. An executive dashboard should never replace operational dashboards, and operational dashboards should never be presented directly to the board. One informs daily operations; the other informs strategic decision-making. The most mature organizations maintain both and ensure that executive metrics are supported by operational measurements beneath them.

Automating metrics and dashboards

One of the easiest ways to lose confidence in your metrics is by relying on manual data collection. Spreadsheets copied from multiple systems every month are time-consuming, difficult to validate, and almost impossible to scale as the organization grows.

Whenever possible, automate both the collection and presentation of your security metrics. Modern security platforms, GRC solutions, SIEMs, cloud security platforms, vulnerability management tools, and identity systems all expose APIs that allow metrics to be collected continuously and displayed in near real time.

Automation also enables another capability that is often overlooked: monitoring the health of the security program itself.

For example, imagine that endpoint protection is deployed to all production cloud images. If a deployment error causes endpoint coverage to drop from 98% to 50% overnight, how long would it take your organization to notice?

If the answer is "during next month's executive report," then the metric has failed in its purpose. Automated thresholds and alerts should be established for critical operational metrics such as these. When coverage falls below an acceptable level, vulnerability remediation exceeds established SLAs, or backup success rates decline, the appropriate teams should be notified immediately.

Note

Metrics should not simply describe yesterday's performance; they should help identify today's operational problems before they become tomorrow's incidents.

Aligning metrics with their owners

One important lesson that many new security executives learn is that cybersecurity does not own every metric reported on a security dashboard.

Consider disaster recovery exercises. Their success directly affects cyber resilience, yet ownership often resides with the infrastructure, business continuity, or IT operations teams rather than the security organization. Likewise, identity metrics may be owned jointly with Identity Engineering, while application security metrics may depend heavily on engineering teams. For this reason, every executive metric should have a clearly identified business owner.

The owner is responsible for maintaining the control, validating the accuracy of the measurement, explaining significant changes, and presenting remediation plans when performance falls below expectations. This approach creates shared accountability across the organization and reinforces one of the themes discussed earlier in this book: *security enables governance*. However, accountability for many security outcomes is distributed across the business.

I strongly encourage clearly defining every metric. Document every metric before it appears on an executive dashboard. This may seem unnecessary when the metric is first created, but several years later, people often forget exactly how it was calculated.

Every metric should include a written definition that specifies:

- What the metric measures and how that impacts the business
- The data source
- How frequently it is updated
- Who owns it
- The numerator
- The denominator
- Any assumptions or exclusions

For example, suppose your dashboard reports **Endpoint Protection Coverage: 96%**. At first glance, the number seems straightforward. But what does the remaining 4% represent? Does the denominator include only managed Windows devices, or does it also include Linux servers, macOS endpoints, cloud images, test environments, and disconnected systems?

Without clear documentation, two different teams may calculate the same metric differently, leading to inconsistent reporting and confusion during executive reviews or audits.

> **Note**
>
> Well-defined metrics remain meaningful long after the people who originally created them have moved to different roles.

Once these metrics are aligned, use them to demonstrate the value of security investments and explain how security ROI differs from that of other departments.

Demonstrating the return on investment (ROI) of security initiatives

Unlike revenue-generating departments such as sales or product, security rarely produces direct financial returns. A successful phishing campaign that never happened does not appear on a financial statement and neither does an attacker who failed to compromise privileged credentials because of your identity strategy. To put it more directly, customers rarely renew contracts because your endpoint detection platform stopped malware execution the night before.

Security is, by nature, an investment in resilience. Its value mostly lies in the incidents that were prevented, the business disruptions that never materialized, and the reputational damage that was successfully avoided. This creates one of the greatest leadership challenges in cybersecurity: demonstrating value when success is often invisible.

The mistake many security leaders make is trying to prove their value solely through technical accomplishments. They highlight the number of alerts investigated, vulnerabilities remediated, or attacks blocked. While these accomplishments matter operationally, they rarely answer the question executives are actually asking, which is whether security made a meaningful difference.

One lesson I learned early in my leadership career is that different executives define value differently. While the CEO may care about business resilience and customer confidence, the CIO may prioritize operational stability. Meanwhile, your security team may view success as deploying a new capability or reducing incident response times. None of these perspectives are wrong; they simply represent different ways of evaluating the same investment.

Note

Throughout *Chapter 1*, we emphasized understanding how the organization generates revenue and what business outcomes matter most. That same principle applies here. The return on a security investment should always be evaluated within the context of the business objectives it supports.

Historically, security leaders have justified investments by discussing breach prevention, for example, by opening the conversation with the statement: "*We need this solution because it reduces the likelihood of a ransomware attack.*"

While technically accurate, this approach has limitations. First, it relies on hypothetical scenarios. Nobody can prove with certainty that a specific investment prevented a future attack. Second, it often positions security as a cost center that only consumes budget to avoid unlikely events. A more effective approach is expanding the conversation beyond risk avoidance. Modern security programs create value in multiple ways, such as:

- Reducing operational inefficiencies
- Simplifying compliance activities
- Accelerating incident response
- Increasing customer confidence
- Improving business resilience
- Enabling faster cloud adoption
- Reducing manual effort through automation
- Improving decision-making by providing better visibility into organizational risk

With the rationale in mind that technology is not the outcome, business value is, review *Table 11.3*, which translates security technology into business value:

Security investment	**Business objective**	**How to demonstrate value**
Identity modernization	Reduce identity-related risk while improving workforce productivity	Fewer compromised accounts, faster onboarding/offboarding, reduced help desk calls, stronger compliance posture
Cloud security program	Enable secure cloud adoption	Faster cloud deployments, fewer high-risk misconfigurations, improved regulatory readiness
Security awareness program	Reduce human-related risk	Lower phishing success rates, increased employee reporting, fewer credential compromise incidents
Incident response modernization	Improve operational resilience	Reduced mean time to detect and respond to incidents, reduced business disruption, faster recovery from incidents
Vulnerability management program	Reduce organizational exposure	Higher remediation rates for critical assets, reduced attack surface, improved risk posture
Third-party risk program	Strengthen supply chain resilience	Increased supplier assessments, reduced vendor-related risk, better contract compliance

Table 11.3 – Security investment and business objectives

Security technologies create technical capabilities, but executives invest in business outcomes. When presenting the value of a security initiative, always translate technical improvements into measurable business impact.

Quantifying risk reduction

Measuring risk reduction is considerably more challenging than measuring operational efficiency, but it remains an important part of the conversation. The objective is not to pretend that cyber risk can be predicted with absolute mathematical precision. Rather, the goal is to use the best available evidence to estimate risk, acknowledge uncertainty, and demonstrate whether the organization's overall exposure is moving in the right direction.

In *Chapter 8*, we discussed maintaining a risk register, documenting risk ownership, and establishing governance processes. Those same artifacts become valuable inputs when discussing ROI.

Organizations that want to take risk quantification further can use established approaches such as **Factor Analysis of Information Risk (FAIR)**. FAIR provides a structured model for analyzing cyber risk by considering the probable frequency of a loss event and the probable magnitude of the resulting loss. Rather than simply describing a risk as high, medium, or low, FAIR can help translate a risk scenario into probabilistic and, when appropriate, financial terms. For example, instead of reporting that credential compromise represents a "high risk," an organization could estimate the probability of a material loss occurring over the next twelve months and the potential range of financial impact. FAIR also recognizes different forms of loss, including productivity loss, response costs, replacement costs, fines and judgments, reputational damage, and loss of competitive advantage.

This can be particularly useful when evaluating security investments. Suppose you are considering a $2 million privileged access management initiative. Rather than relying only on technical improvements to justify the investment, a FAIR-based analysis can help estimate how the proposed controls may change the frequency or magnitude of relevant loss scenarios. You are not claiming that the organization will save exactly a particular amount of money. Risk is inherently uncertain, and FAIR explicitly treats it probabilistically. Instead, you are giving leadership a structured way to compare the cost of the investment with the expected reduction in financial exposure. This can make conversations about cybersecurity investment much more consistent with the way executives already evaluate other forms of enterprise risk.

For example, after implementing a privileged access management initiative, you may observe:

- Fewer privileged accounts
- Elimination of shared administrative credentials
- Increased MFA coverage
- Reduced attack paths
- Lower residual risk for identity-related scenarios

None of these measurements individually prove financial return. Collectively, however, they demonstrate a measurable reduction in organizational exposure. Boards increasingly understand this language because it connects investments directly to enterprise risk management rather than isolated technical improvements.

Demonstrating value through business enablement

Security is frequently perceived as the department that slows down projects. Mature security organizations accelerate innovation because they provide predictable governance, reusable security patterns, and standardized controls.

Consider a cloud adoption initiative without established security standards. In such a case, every new workload requires lengthy security reviews as engineering teams wait for approvals, and projects slow down and frustration grows.

Now imagine that your organization has implemented secure landing zones, infrastructure-as-code templates, standardized identity controls, automated policy validation, and continuous compliance monitoring. Instead of reviewing every deployment individually, developers inherit secure configurations by default. As a result, deployment cycles accelerate and security reviews become more predictable. The return on investment is no longer measured solely by improved security; it is measured by faster business execution. This type of ROI is often more compelling to executive leadership than discussing threat detection percentages.

Therefore, as you prepare to demonstrate value, focus on telling a story rather than just showing raw numbers. Before showing charts, percentages, or financial calculations, explain the business problem. Describe the challenge the organization faced, explain the investment that was made, and show how the investment changed operational behavior. To translate that, let's use a fictitious scenario.

Suppose an organization is struggling to remediate critical vulnerabilities across thousands of servers. Ownership has been inconsistent, reporting fragmented, and remediation has frequently exceeded established service-level objectives.

Over the past 12 months, the security team implemented centralized vulnerability governance, automated ownership assignment, executive dashboards, and regular risk reviews with business stakeholders. The result was presented to leadership as follows: "*More than 95% of our most important business systems met agreed timelines for remediating critical vulnerabilities.*"

Notice that the story explains the outcome before introducing the metric, and the number reinforces the narrative; it does not replace it.

Also remember that demonstrating ROI is not an activity reserved for budget season; it should be embedded into every significant security initiative. Before requesting funding, define how success will be measured. Establish baseline measurements before implementation, then track

progress against those objectives as the project advances. Once the initiative is complete, compare the results to the original goals and communicate both the achievements and the lessons learned.

By using this approach, you create a continuous cycle of planning, measurement, and improvement while building credibility with executive leadership. Over time, leaders begin to recognize that the security organization consistently delivers measurable business outcomes rather than simply requesting additional investment. Next, you also need to ensure that you are measuring the security program's maturity and operational effectiveness.

Connecting maturity to metrics

It is important to distinguish between **performance metrics** and **maturity measurements** because they answer different but related questions. A performance metric tells you what is happening. A maturity assessment helps explain how consistently and sustainably the organization is capable of producing that result. You need both perspectives to understand whether the security program is truly improving.

For example, suppose 95% of critical vulnerabilities are currently being remediated within the organization's established service-level objectives. That is a strong performance metric, but by itself it does not tell you whether the underlying vulnerability management program is mature. The result may depend on engineers manually reviewing spreadsheets every week, repeatedly contacting system owners, and escalating overdue vulnerabilities through informal relationships. The organization is achieving the desired outcome, but the process may be difficult to sustain or scale.

A more mature vulnerability management capability might produce the same 95% result through automated asset discovery, risk-based prioritization, clearly assigned ownership, automated remediation workflows, documented exception processes, and dashboards that continuously monitor performance. The KPI may be identical, but the organization's ability to consistently produce that outcome is very different.

Assess the people, processes, governance, and technology behind each result to determine whether the capability can sustain it.

You do not need to create a complicated maturity model during your first year. Start with a small number of security domains that are most important to the organization's risk profile and assess each one against a consistent set of criteria. Depending on the organization, those domains might include identity security, vulnerability management, incident response, cloud security, data protection, application security, third-party risk, and security governance.

For each domain, evaluate a few practical dimensions:

- **Process:** Is the activity performed consistently and documented, or does success depend on individual knowledge and manual effort?
- **Ownership:** Are responsibilities clearly assigned, and are accountable owners identified?
- **Governance:** Are expectations, exceptions, risks, and remediation decisions formally reviewed and documented?
- **Technology and automation:** Are appropriate tools and automation supporting the process, or does it depend heavily on manual activities?
- **Measurement:** Are KPIs defined, consistently collected, and used to identify areas requiring improvement?
- **Continuous improvement:** Are lessons from incidents, assessments, audits, and metrics used to improve the capability over time?

You can then use a simple maturity scale to establish a common language. For example, **Level 1** may represent an ad hoc capability that depends largely on individual effort; **Level 2** may indicate that basic processes and ownership exist; **Level 3** may represent documented and consistently implemented processes; **Level 4** may indicate that the capability is measured, automated where appropriate, and actively governed; and **Level 5** may represent a capability that is continuously optimized based on metrics, risk, and lessons learned. The specific labels matter less than applying the criteria consistently.

Consider incident response as an example. An organization at an early maturity level may have skilled analysts who successfully handle incidents but rely heavily on individual experience and informal processes. As the capability matures, incident classifications become standardized, roles and escalation paths are documented, playbooks are regularly exercised, response metrics are automatically collected, and lessons learned from incidents drive improvements to controls and procedures.

You are no longer measuring only whether incidents were resolved; you are measuring whether the organization has developed a repeatable and sustainable capability for responding to them.

The same approach can be applied across the security program. You might determine that identity security is operating at the maturity level appropriate for the organization's risk, while cloud security requires significant improvement and third-party risk requires only incremental investment. Document the current maturity, define the **target maturity**, identify the most important gaps between the two, and connect those gaps to specific initiatives and metrics.

This last step is critical. A maturity assessment should not become another scorecard that gets presented once a year and then forgotten. If cloud security needs to move from Level 2 to Level 3, define what must actually change to make that happen. Perhaps asset ownership needs to become consistent, security policies need to be automatically enforced, or coverage of critical cloud workloads needs to increase from 70% to 95%. Those become measurable objectives that can be tracked through the metrics already discussed in this chapter.

In this way, maturity and metrics reinforce each other. Maturity establishes where the capability is today and where it needs to go; metrics provide the evidence that it is actually moving in that direction. Together, they allow you to demonstrate not only that individual security numbers are improving, but that the security program itself is becoming more disciplined, repeatable, measurable, and resilient.

Measuring maturity and operational effectiveness gives you the evidence to understand whether the security program is improving, but measurement alone is not enough. The value of those metrics depends on your ability to explain what they mean, why they matter, and what actions they should drive. A security analyst, a business leader, a CEO, and a board member may all look at the same security outcome through very different lenses. In the next section, we will explore how to communicate security outcomes effectively to technical and non-technical audiences, translating metrics and security achievements into messages that are relevant, understandable, and actionable for each stakeholder.

Communicating security outcomes to technical and non-technical audiences

Apply the executive communication principles from *Chapter 9* to the results measured here. Explain what improved, why the change matters to the business, and whether the evidence supports a decision or further action.

Translating technical achievements into business outcomes

Earlier in this chapter, we discussed the importance of measuring business outcomes instead of technical activities. The same principle applies to communication. Suppose your security team recently implemented MFA across the enterprise; the technical accomplishment might sound like this: "*We deployed phishing-resistant MFA to 98% of privileged accounts*."

That statement is accurate, and for a technical audience, it may be sufficient. However, for an executive audience, you might instead say this: "*The organization significantly reduced the likelihood of credential-based attacks against our highest-value accounts while also strengthening compliance with regulatory identity requirements*."

The technology remained exactly the same, but the outcome became the focus. This simple shift transforms security from a collection of technologies into a business capability.

Tip

Over time, you will discover that every stakeholder views cybersecurity through a different lens, and you need to tailor your message according to the audience.

Similarly, if the time required to establish the scope of high-severity incidents decreased by 48%, explain the operational improvement through a story: "*Earlier this year, our analysts often spent several hours identifying the scope of high-severity incidents because relevant security information was scattered across multiple systems. Following the implementation of centralized detection and automated investigation workflows, analysts can now identify affected systems much more quickly, reducing the time required to begin containment and minimizing potential business disruption.*"

The metric becomes more meaningful because the audience understands why it changed. In summary, whenever possible, present metrics within a narrative.

Note

Nothing lands better than a story.

Summary

Measuring security success is not about filling dashboards with more numbers but selecting metrics that help the organization understand whether security is reducing risk, improving resilience, enabling the business, and creating measurable value. As a security executive, you need to move beyond activity-based reporting and focus on measurements that answer the questions leadership actually cares about: "*Are we safer, are we more prepared, are we improving, and are our investments making a difference?*"

This chapter reinforced that meaningful metrics start with the business, not the technology. The best metrics connect technical activity to outcomes such as reduced exposure, faster detection, improved recovery readiness, stronger control coverage, better compliance, and increased confidence in the protection of critical assets.

You also learned that demonstrating ROI in security requires a broader view of value. Security investments may not always produce direct revenue, but they can reduce operational inefficiencies, improve response times, simplify compliance, increase customer confidence, strengthen resilience, and accelerate business initiatives such as cloud adoption. As the cybersecurity executive, it is your job to convey all of this to tell a clear story: identify the

business problem, explain the investment, show what changed, and use the metric to reinforce the outcome rather than replace the narrative.

Finally, this chapter emphasized that maturity and communication are both leadership disciplines. Security maturity should be proportional to business risk and should not be treated as a race to the highest score in every domain. Just as importantly, security outcomes must be communicated differently to different audiences. When you measure the right things and communicate them effectively, security becomes more than a function that protects the organization; it becomes a trusted business capability that helps leaders make better decisions.

Metrics, maturity assessments, and effective communication help demonstrate the progress of the security program, but sustaining that progress requires something equally important: sustaining the leader behind it. Cybersecurity leadership comes with constant pressure, difficult decisions, competing priorities, and the reality that the work is never truly finished. In *Chapter 12*, we will explore the human side of cybersecurity leadership, including how to manage sustained pressure, establish healthy boundaries, recognize the warning signs of burnout, build personal resilience, and create leadership practices that allow you and your team to perform effectively over the long term.

Additional resources

- NIST SP 800-55 Volume 1 – Measurement Guide for Information Security: Identifying and Selecting Measures: `https://bit.ly/CISOBook28`
- NIST Cybersecurity Measurement Program: `https://bit.ly/CISOBook29`

12

The Resilient Leader: Sustaining Leadership and Managing Burnout

By the time you reach this chapter, you have spent most of your first year looking outward—learning the business, building relationships, and shaping the security program. This chapter turns that same attention toward a resource the operating model also depends on: your ability to continue leading effectively over time.

The security executive role can be deeply rewarding, but it also tends to be relentless. There is always another vulnerability, audit request, board meeting, regulatory development, vendor problem, or incident that does not care what day or time it is. As your credibility grows, more people ask for your opinion, your calendar fills, and more decisions reach you. Even with strong discipline and support, periods of exhaustion or even burnout are likely to occur.

Sustainable leadership is therefore not about achieving balance or eliminating pressure. It is about recognizing when the demands of the role have become difficult to sustain, understanding how that pressure affects your judgment and the people around you, and making changes as needed. The goal is to build the capacity to move through demanding periods, recover, and continue leading effectively.

Earlier chapters discussed delegation, developing talent, building relationships, governance, and operational discipline. Those practices also contribute to resilience. A leader with trusted deputies, clear escalation paths, and reliable coverage carries a different burden from one who has become the center of every decision. This chapter connects those ideas and applies them to the sustainability of both the leader and the organization.

In this chapter, we will focus on:

- Recognizing the impact of security leadership on your well-being
- Protecting your capacity to lead
- Maintaining perspective beyond the role
- Building resilience into the operating model

Recognizing the impact of security leadership on your well-being

Cybersecurity leadership combines forms of pressure that do not normally appear together in the same role. You are accountable for risks you cannot eliminate, are expected to influence teams you do not control, and are often required to make decisions before all the facts are available. The consequences can include business disruption, regulatory scrutiny, customer impact, and public attention. That combination makes the role fundamentally different from managing a purely technical function.

The work also carries a difficult asymmetry. Successful security work often goes unnoticed. An attack is stopped, a risky configuration is corrected, or a vendor issue is discovered before customers are affected. But when something fails—a ransomware attack disrupts operations, customer data is exposed, or a critical service becomes unavailable—the visibility is immediate.

That imbalance can create the belief that you must personally inspect everything because one missed issue could become the issue everyone remembers.

The first year can intensify this pressure. You want to establish credibility, learn quickly, and show that you can handle the role. Long days, early mornings, evenings, and occasional weekends are a reality for many executives. The role will rarely fit neatly within traditional working hours. The risk arises when periods of heightened intensity become the standard rather than the exception.

Cybersecurity leadership has no natural finish line. New technologies, adversary techniques, acquisitions, suppliers, and regulations continually change the environment. If your definition of success is getting everything done, the role will always leave you feeling behind. A more sustainable definition is building an organization that can identify the right risks, make decisions, respond effectively, and continue improving without requiring your involvement in every detail.

However, even a sustainable operating model cannot eliminate periods of intense pressure. The challenge is distinguishing a demanding period from a pattern that is beginning to affect your energy, judgment, or behavior, often before the effects become visible to others.

Recognizing the early warning signs of burnout

Burnout rarely appears out of the blue. It often develops through small changes that gradually become normalized. You check messages earlier and later in the day. You begin consistently canceling one-on-ones and other regular touchpoints across your circles of influence whenever urgent issues arise. Strategic work moves to the weekend because the workday is consumed by meetings. On the calendar, you may still look productive, but the quality of your thinking begins to decline.

For leaders, acknowledging these changes (even privately) can be difficult. When others rely on you to remain steady, it is easy to explain away mounting strain as temporary or simply part of the role. You may also worry that admitting it to others will be interpreted as weakness or raise questions about whether you can handle the position, particularly if this is your first time operating at this level.

> **Note**
>
> Senior leadership can be lonely. There are fewer people with whom you can speak candidly about what the role is taking from you. That hesitation can delay action.

For a security executive, the earliest warning signs are often visible in how the organization operates. Ask yourself these questions:

- Is my energy returning when I step away, and am I sleeping well enough to recover?
- Has my patience or ability to regulate my reactions changed in ways others may already notice?
- Am I becoming more cynical, detached, or less connected to work that previously mattered to me?
- Has my ability to focus or make sound decisions changed, or do familiar responsibilities now require significantly more effort?
- Am I routinely pushing strategic work into evenings or weekends because meetings consume the workday?
- Are routine decisions repeatedly escalating to me, or am I reviewing work that a trusted leader should own?
- Can I step away for a day without creating uncertainty, or has the organization learned that nothing moves without me?

These questions are not a wellness scorecard. They are intended to reveal whether sustained pressure is beginning to affect you and whether the operating model has become too

dependent on your constant availability. *If your answers raise concerns, working harder or becoming more efficient is unlikely to address the underlying problem.*

Do not wait until you are approaching burnout to ask these questions. Schedule a recurring quarterly check-in on your calendar and revisit them after any sustained period of heightened pressure. Discuss your answers with a trusted advisor who has seen you operate over time. They may recognize changes you have overlooked or begun to accept as normal.

Using a structured check-in

Structured tools can provide another point of reference. The following resources can support reflection, but they are not a diagnosis or a substitute for professional care. If a pattern is persistent or is affecting your health or ability to function, seek appropriate support rather than treating it as another leadership problem to solve alone.

Assessment tools:

- The *World Health Organization-Five Well-Being Index (WHO-5)* is a brief self-report measure focused on the previous two weeks.
- The **Copenhagen Burnout Inventory (CBI)**, developed through the *Project on Burnout, Motivation, and Job Satisfaction (PUMA)* research project, examines personal, work-related, and client-related burnout.
- For security teams, **Cybermindz** offers the *Resilience Pulse and Resilience Index* to help organizations examine stress, energy, recovery, and burnout indicators across the workforce.

Additional support/guidance:

- The **NIST NICE** webinar *Mental Health in Focus: Managing Burnout and Finding Balance in Cybersecurity Work* offers a cybersecurity-specific discussion of warning signs, decision-making, and organizational support.
- The *HBR Guide to Beating Burnout* by **Harvard Business Review** provides broader practical guidance for individuals, teams, and organizations.

Whether you use the questions relating to burnout above or a structured tool, context matters. A demanding week does not necessarily indicate chronic overload. The next step is to determine whether the intensity is temporary or has become the normal way of operating.

Distinguishing temporary pressure from chronic overload

Shifting priorities and urgent demands are part of executive leadership. Before considering how to respond, it is worth taking a moment to compare a short-term burst of intensity with chronic overload. They may feel similar in the moment, but they require different leadership responses.

A **short-term burst** can be sustainable when it is tied to a defined outcome, other work is consciously deprioritized, and the intensity is followed by meaningful recovery. For example, suppose a vulnerability affecting customer-facing systems was actively exploited. This may require several days of concentrated leadership attention. Meetings may be canceled, and lower-priority work might be deferred. Clear decision authority and coverage arrangements will be established so that the same people are not carrying the full burden continuously. Once the immediate risk is addressed (the defined outcome in this case), the operating rhythm will reset and those involved will have space to recover.

Chronic overload looks different. It usually means the next critical issue arrives before the organization has had the chance to recover from the previous one. In this situation, new work may be added without an explicit decision about what will stop or move. The leader will continue to be the default point of escalation and strategic work might get repeatedly pushed into evenings and weekends. Recovery is postponed because there is always another reason to maintain the same pace, so the exceptional response gradually becomes the operating model.

AI further intensifies this pattern. AI-assisted development and security research have increased the speed at which vulnerabilities are created, identified, and reported. A vulnerability management program that once mobilized around an occasional critical issue may begin receiving critical findings every week. If each one triggers the same escalation path and executive involvement, the short-term surge model becomes permanent.

This distinction can be difficult to recognize from inside the situation. Each demanding week may have a reasonable explanation, making it easy to believe that the pressure will ease after the next deadline.

Look for patterns across several weeks rather than judging one difficult day in isolation. Ask someone you trust whether they have noticed a change in your energy or how you are showing up; the pattern may be easier to see from the outside.

A strong sense of responsibility can make it even harder to question the pace, particularly when slowing down feels like letting your team or the organization down.

Protecting your capacity to lead

Security leadership is a marathon, not a sprint, even when the role often feels like a series of sprints. You are here for the long run—to create lasting impact, not simply reach the next deadline or navigate the next crisis.

Many executives build their careers by being the person who can absorb pressure and remain steady when situations become difficult. That endurance is valuable, but it can also create the belief that the answer to sustained pressure is simply to endure more of it.

Before you can take care of everyone who depends on your leadership, you need to take care of yourself. This is not separate from your leadership responsibility; it is part of it. You may be able to keep working as your energy declines, but *sustaining effort is not the same as sustaining effectiveness*.

The shadow of the leader is long. How you show up under pressure shapes how your team believes they should show up. A leader who remains constantly available and treats recovery as optional can unintentionally establish that behavior as the standard. Managing your energy therefore protects more than your own effectiveness; it influences the culture around you.

Managing your energy

Investing in your energy is often hardest when you need it most. When the calendar becomes crowded and work feels urgent, the activities that restore you are usually the easiest to remove. Exercise can wait. Dinner with the family can be shortened. Sleep can be reduced, and vacation can be postponed. Each decision may appear reasonable in isolation, but together they remove the very sources of energy that help you sustain the role.

In *The Power of Full Engagement*, Jim Loehr and Tony Schwartz emphasize that sustained performance depends on managing energy and not simply time. Done consistently, this can become a leadership superpower: a relatively small investment can improve how you show up for many hours afterward. It might be an hour at the gym, dinner with your family, or the portable three-minute breathing-space practice described by Michael Chaskalson in *Mindfulness in Eight Weeks*. The activity and duration will vary, but the objective is the same: creating enough distance to return with greater clarity, patience, and perspective.

The **RSA Conference** article *Mindfulness in Cybersecurity: A Shield Against Stress and Burnout* offers additional examples of how practices such as mindful breathing, focused attention, and short breaks can be applied in a cybersecurity environment.

When I led Cyber Threat Management at PayPal, sustained pressure was part of the role. My team helped protect customers around the world, operated across time zones, and carried responsibilities that did not stop at the end of the business day.

During COVID, the boundaries between work and home narrowed even further. When demands increased, my instinct was to remove the activities described above from my calendar first. They felt negotiable because they did not carry the same visible urgency as an incident, executive request, or emerging threat.

However, over time, I learned that these commitments could not remain optional. Twice a week, I left home at a specific time to make it to yoga class, even when unfinished work and unanswered messages remained. The hour away did not eliminate the pressure, but its effect lasted well beyond the class. I returned with more energy and perspective, which changed how

I approached the work that was still waiting. What initially felt like time taken away from the job became an investment in how I performed it.

The same principle applies to sleep and vacation. Repeatedly shortening sleep to create more working hours may help you finish another task tonight, but it borrows capacity from the following day. Sustained sleep deprivation can make it harder to regulate your reactions, maintain attention, and exercise sound judgment. You may respond more sharply than intended, miss an important detail, or make an avoidable mistake.

Time away also needs to create meaningful distance from the role. Being physically away while continuously monitoring messages may preserve your availability, but it does little to restore your energy.

Tip

There will be situations when stepping away is not the right call. During an active incident or another consequential moment, the organization may need your continued involvement. Managing your energy is not a rigid rule that takes priority over the needs of the business. The distinction is whether remaining engaged is a temporary response to a genuine need or the default expectation you place on yourself. When you cannot step away in the moment, create space to recover as soon as circumstances allow.

The value of managing your energy becomes especially visible in the quality of your decisions. Fatigue does not simply change how you feel; it can change how you evaluate risk, respond to uncertainty, and exercise judgment.

Preserving decision quality

As a security executive, one of your most valuable contributions is your judgment. You will rarely have perfect information, unlimited resources, or enough time to evaluate every possibility. Your role is to understand the context, consider the trade-offs, and make the best decision you can with the information available.

When your capacity declines, nuance is often the first thing to disappear. You may settle on the first answer that comes to mind, postpone a difficult conversation because you lack the mental space to handle it thoughtfully, or treat every issue labeled critical with the same level of urgency. Two issues may carry the same severity rating and still create very different levels of business exposure. Preserving decision quality requires enough capacity to look beyond the label and understand what the situation means for the organization.

The frameworks introduced earlier in this book can help. In *Chapter 4*, we discussed using defined prioritization factors to build your security roadmap. Return to those factors when

new demands emerge rather than reassessing every request from the beginning. When urgent work is introduced, identify what will move or slow down as a result. Your roadmap should make existing commitments visible and give you a structured way to explain the trade-offs.

For example, an executive may ask the security organization to support a new business initiative immediately. The request may be important, but that does not mean it should simply be added to everything already underway. Applying your established prioritization factors can help you evaluate the business value, risk, timing, and resources required. You can then decide whether the initiative should take priority and communicate what will be deferred to create the necessary capacity.

Sustaining good decision-making across the security organization requires leaders who can exercise judgment without waiting for you. Your role is not to make every security decision yourself. It is to help your leaders understand how you approach difficult situations, give them clear decision authority, and trust them to act within those boundaries. This allows sound decisions to continue without making you the bottleneck, while keeping you available when an issue genuinely requires your involvement.

One of my mentors at EY, Patrick, taught me this lesson. Whenever I reached out to ask what I should do, he would often respond, "I trust your judgment." As a mid-level manager, I hated that answer. I wanted him to tell me what to do. What I did not understand at the time was that he was teaching me how to think through challenging situations and develop confidence in my own decisions.

I now use a similar approach with my team. I can see their frustration when they want a direct answer, and I ask them to make the decision. It can be difficult to watch someone struggle when you know you could resolve the issue more quickly yourself. Stepping in every time may solve the immediate problem, but it takes away an important opportunity for that person to grow. The judgment they develop through those moments will allow them to handle increasingly complex decisions on your behalf—and prepare them for the leaders they are becoming.

Note

It is important to note that *delegation needs to be supported by clear expectations*. Your leaders need to understand which decisions they own, when an issue should be escalated, and how much risk they are authorized to accept. They also need to know that you will support a reasonable decision, even when you might have approached it differently. If you routinely take decisions back or reverse them without explaining why, people will learn to wait for you instead of using their own judgment.

Even with clear priorities and capable leaders, some decisions require uninterrupted time to think. That space rarely appears on an executive calendar by accident.

Protecting your calendar

In *Chapter 1*, we discussed owning your calendar during the listening tour so you could create time to learn about the organization and build important relationships. This discipline remains important long after the listening tour ends. The purpose may change, but your calendar should continue to reflect the work that requires your attention and not simply the meetings other people ask you to attend.

Executive calendars rarely become overloaded all at once. The meeting load accumulates gradually: another operational review, vendor briefing, project update, or discussion where your presence may be helpful but not essential. The impact is easy to underestimate. A two-hour weekly meeting adds up to more than 100 hours over the course of a year. Across several recurring meetings, the time available for strategic thinking quickly disappears, pushing work that requires concentration into evenings and weekends.

Treat your time as a leadership resource and review it as carefully as you would review a budget. Each week, review your upcoming calendar with your administrative assistant. Identify meetings that can be shortened, attended less frequently, delegated to a direct report, or removed altogether. Delegating a meeting can also create a development opportunity by giving another leader greater exposure and experience representing the organization.

Once a quarter, take a broader look at your recurring meetings. Instead of asking whether you need to attend next week, consider whether the meeting still needs to exist in its current form. Meetings that were valuable six months ago may no longer serve the same purpose. You can also work with your chief of staff or administrative assistant to combine meetings with overlapping participants and objectives, preserving the necessary decisions and alignment while reducing the time required.

Some responsibilities require uninterrupted attention. Strategy, board preparation, difficult writing, and complex decisions are executive responsibilities, yet they are often treated as activities to complete between meetings. Reserve *focus time* several times a week and ask your administrative assistant to avoid scheduling over it unless urgent. Use that time to return to notes you have taken throughout the day, reflect, or complete work that requires deeper thought.

Tip

The practice does not need to be perfect. Sometimes focus time will need to become meeting time, and there may still be nights when you go back online to complete a specific task or join an evening call. Knowing that you have reserved capacity on your calendar can still provide peace of mind and give you greater control over when and how you address those demands.

Protecting your calendar does not mean becoming inaccessible. Your directs and key partners should have predictable ways to reach you and understand what warrants interrupting protected time. Making that distinction requires boundaries supported by people who can provide reliable coverage when you are unavailable.

Setting boundaries and coverage

Setting boundaries means protecting your time by defining when your personal involvement is genuinely necessary. In security leadership, a useful boundary is less about the hour on the clock and more about the reason you are being asked to engage. A potentially material incident, significant customer impact, a credible threat to critical operations, or an urgent regulatory matter may require your immediate involvement.

Make those expectations explicit. The incident severity definitions, escalation paths, and playbooks discussed in *Chapter 6* can help your team distinguish between a situation that requires your authority and one they are equipped to manage. Without that clarity, people may escalate too much because they are afraid of making the wrong decision or wait too long because they do not want to disturb you.

You also need to honor the boundaries you establish. If you ask the team to contact you only when defined thresholds are met but continue monitoring every message and inserting yourself into routine decisions, the boundary will have little effect. Your behavior teaches people whether they genuinely have authority or are simply expected to wait for you.

Additionally, when you take time away (during protected time in the workday, over an evening or weekend, or while on vacation), be specific about your availability. Let the team know when you will be completely unavailable and when you can still be reached. If you are available for urgent matters, identify the best way to contact you, such as by text, and how quickly they should expect a response. For instance, "Text me for a potentially material incident; use email for anything that can wait until I return" provides more useful direction than "Reach out if anything comes up."

Reliable coverage also requires coordinating planned absences. Before stepping away, confirm who is responsible, what that person can decide, and how others will know where authority has shifted. Make sure the designated leader has the context and organizational standing to act. Test the arrangement before depending on it by allowing your deputy to lead an operational review, manage an exercise, or make a consequential decision while you remain available in the background. Time away is a poor moment to discover that nobody knows who can approve a containment action or communicate with senior leadership.

The same clarity is needed with your manager and executive peers. Explain how critical issues will reach you, who will provide coverage, and how other matters will be handled while you are unavailable. Framing the conversation around continuity and decision-making demonstrates that the boundary is supported by a thoughtful operating model, not a lack of commitment.

Make sure you and your deputy are not away at the same time. Consider vacations, holidays, and important personal commitments such as birthdays when looking ahead at the coverage calendar.

I used this approach with Dan, who was one of my direct reports at PayPal. We coordinated our vacations, holidays, and important personal dates so that one of us was available when the other stepped away. I followed the same practice with my manager, which generally meant that at least two of the three of us were available.

The arrangement improved continuity, but it also made the experience better for each of us. We could be more present during our time away because we trusted that someone familiar with the work was available.

Reliable coverage creates room to step away without making the organization fragile. Sustaining yourself over the longer term, however, also requires relationships and sources of support beyond the immediate demands of the role. We turn next to the relationships and practices that support leadership over time.

Maintaining perspective beyond the role

There is a limit to what you can address by managing your calendar and setting better boundaries. While these practices create room to think and recover, they do not necessarily provide perspective when the role begins to narrow your world.

Maintaining perspective requires support beyond the day-to-day operating practices discussed in the previous section. It depends on having people with whom you can speak candidly, continuing to learn without trying to follow every development, and looking beyond the next deadline or position. Together, these practices can help you remain grounded and adapt as your career and responsibilities evolve.

Building a personal support system

The relationships that help you operate within the organization are not always the same relationships that help you process the demands of the role. Some situations cannot be discussed openly with your team, and there will be times when you need an outside perspective.

In *Chapter 2*, we discussed the different roles that counselors, mentors, and sponsors can play in your career. As your responsibilities grow, build on that framework by creating a small personal **board of advisors**. A trusted peer can help you compare operating practices. A former manager or mentor can challenge your thinking when you are too close to a problem, while an executive coach can provide candid feedback. No single person needs to fill every role.

Professional networks and peer communities can provide another valuable source of support. I have been amazed by colleagues who were willing to go above and beyond when I reached out with a question. They shared how they had approached a similar challenge, introduced me to someone with relevant experience, or made time for a candid conversation. It can take time to find a professional community where you feel that level of trust and generosity, but the right one can become invaluable.

Include people who know you beyond your title. Friends and family may not understand every detail of the work, but they can recognize changes in your energy or behavior and remind you that the role is important without allowing it to become your entire identity.

> **Note**
>
> The people closest to you may notice that something has changed before you are ready to acknowledge it yourself.

Once you find the right relationships and communities, hold on to them. Invest in them before you need support. Check in when things are going well, ask how others are doing, and provide the same candor and help you hope to receive. At the same time, remain thoughtful about confidentiality. A trusted advisor can help you examine your approach without knowing every sensitive detail, while employee, legal, or incident matters should remain within the appropriate channels.

Tip

It can be surprisingly difficult to find 25 or 30 minutes on someone's calendar. Do not let that become the reason you lose touch. Pick up the phone and call someone you have not spoken with in a while—not a text, an actual call. Who knows? They may even pick up. You do not need a full meeting for every conversation. Seven minutes can be enough to reconnect, ask how someone is doing, or let them know you were thinking about them. That small investment can go a long way toward maintaining a relationship.

Trusted relationships help you maintain perspective. Sustaining your leadership also requires continuing to grow without turning the constant pace of change into another source of exhaustion.

Continuing to learn

Curiosity is one of the reasons many of us are drawn to cybersecurity. There is always a new technology, threat, regulation, or business model to understand. That constant change can make the work exciting, but it can also leave you feeling perpetually behind.

As your responsibilities grow, your definition of staying current needs to change. Technical fluency remains important, but you no longer need to become the deepest expert in every domain. Your effectiveness may depend just as much on understanding finance, governance, organizational design, communication, AI, privacy, geopolitics, and business strategy.

Remember, the objective is to know enough to ask informed questions, recognize when the environment has changed, and determine when deeper expertise is required.

The number of learning opportunities can quickly become overwhelming. You may receive invitations to conferences, industry events, vendor briefings, dinners, advisory sessions, webinars, and peer discussions. Many of them may be valuable, but you cannot attend everything. Each commitment carries a cost beyond the time shown on the invitation. An evening dinner may replace time with your family. A conference may require several days of travel and create additional work before and after the event.

Tip

An invitation is an opportunity, not an obligation. Choose the events that support your priorities, provide access to people or perspectives you would not otherwise encounter, or create space for a conversation that matters. Declining an invitation does not mean that the topic or relationship is unimportant. It means you are making a deliberate choice about where to invest limited time and energy.

Create a learning agenda connected to the role you have and the environment ahead. Choose a small number of themes for the year rather than collecting disconnected content. For example, if AI is changing your company's products and operating model, focus on the architecture, governance, and security implications most relevant to those changes. *You do not need to follow every new tool or announcement to provide effective leadership.*

Rely on your professional network to help separate meaningful developments from noise. Ask trusted peers which events were worth attending, what issues are affecting their programs, and which resources helped them understand a changing area. Sometimes a focused conversation with someone who has already examined an issue will provide more value than another day of presentations.

Learning can also happen through post-incident reviews, conversations with business leaders, and books outside cybersecurity. Select the formats that work for you and give yourself permission to ignore the rest. The goal is not to consume everything. It is to remain curious and intentional about what you need to learn next.

Continuing to learn helps you evolve with the role. Sustaining a long-term career also requires perspective about how organizations, responsibilities, and your own priorities may change over time.

Maintaining career resilience in times of change

There is another dimension of resilience that security executives do not always discuss openly: careers change. Organizations reorganize, strategies shift, leaders move on, and roles expand or disappear. Strong performance does not guarantee that every chapter will end on your preferred timeline.

Career resilience does not mean constantly preparing for your next job. It means recognizing that your title, reporting structure, and organization may change while the capabilities you have developed remain yours. Your judgment, communication skills, technical understanding, crisis leadership, and ability to develop people will travel with you.

Be clear about what matters to you and what you are no longer willing to compromise. A role may offer greater scope or compensation while demanding more than you are prepared to give in another area of your life. There may also be periods when you knowingly accept that trade-off. The important point is to make the choice deliberately and revisit it as your circumstances change.

For example, an organizational restructuring may significantly expand your responsibilities without adding resources or decision authority. Career resilience does not require you to accept the new conditions without question. Clarify what success now requires, identify the support that is missing, and determine whether the role remains aligned with your priorities. The right response may be to reshape the position, adjust your expectations, or eventually consider a different opportunity.

Keep a record of the outcomes you have created along the way. Document transformations completed, measurable improvements, incidents navigated, teams developed, risks reduced, and business initiatives enabled. These examples help you recognize the value you have built beyond a particular title and explain that value when your career takes an unexpected turn.

Note

Not every difficult period means it is time to leave, just as staying is not always evidence of resilience. Sometimes the right choice is to improve the operating model and give the situation time to change. At other times, resilience means recognizing that the role no longer works for you. Maintaining perspective allows you to distinguish between a difficult season and a situation that requires a more fundamental decision.

These choices help you sustain your own leadership over time. The next challenge is ensuring that the organization can sustain periods of pressure without depending on any one person—including you.

Building resilience into the operating model

The practices discussed so far can help you protect your own capacity, but they cannot compensate for an organization that depends on individual heroics. If important decisions stop, incidents stall, or stakeholders lose confidence whenever one person is unavailable, the operating model remains fragile.

A resilient security organization can absorb periods of intense pressure without relying on the same people to carry the full burden every time. Decision authority is understood, leadership depth exists, and the team can maintain continuity when someone steps away.

The real test is not how the organization performs when every leader is available and conditions are predictable. It is what happens when an incident begins during a vacation, a critical employee leaves, or several significant demands arrive at the same time. Building that resilience begins by treating delegation as more than a way to manage workload.

Delegating as a resilience control

Delegation is often discussed as a management skill. In a security organization, it is also a resilience control. Every critical responsibility that only one person can perform creates a single point of failure. That person may be you, but the same risk exists when a technical process, stakeholder relationship, or operational decision depends on one member of the team.

Look across the organization and identify the responsibilities that cannot stop when someone is unavailable. This may include leading an incident workstream, operating a critical security platform, briefing executives, coordinating with key partners, or making time-sensitive risk decisions. For each one, ask a simple question: *Who is second*?

However, naming a backup is not enough. Resilience is built through experience and not simply by assigning someone's name to a coverage plan. That person needs context, access, relationships, authority, and regular opportunities to operate. If they have never used the system, worked with the stakeholder, or exercised their judgment, they will still depend on the primary owner when the situation becomes difficult. Building that trust takes time.

Give your delegates visibility *before* you need them to act on your behalf. Include them in important meetings with legal, technology, business leaders, and other key partners. Let them present updates, lead exercises, and represent the security organization. This helps stakeholders become familiar with their judgment while allowing your delegates to understand how decisions are made across the company.

For example, if a potentially material incident occurs while you are away, you will likely make yourself available regardless of where you are. Delegation does not remove the CISO's accountability or replace the need for executive leadership during a consequential event. It ensures that the response does not depend on you personally directing every workstream or introducing the team to critical stakeholders for the first time during a crisis.

In this case, trusted delegates can lead technical and operational workstreams, coordinate with partners who already know them, and make decisions within established boundaries. That allows you to focus on enterprise trade-offs, executive communication, and the decisions that specifically require the authority of your role.

Build this depth through regular practice rather than emergency handoffs. Rotate ownership of operational reviews, important presentations, exercises, and stakeholder meetings. Allow another leader to take the lead while the primary owner remains available to provide context

and feedback. Periodically test whether the work can continue when the person who normally owns it steps back.

The objective is not to make every employee interchangeable. Specialized expertise and role-specific accountability will always exist. It is to identify where dependence on one individual could create meaningful risk and reduce that exposure before the organization is forced to test it during a difficult moment.

Reducing key-person dependencies strengthens the organization's ability to operate through disruption. During sustained periods of intensity, however, even well-prepared teams need a deliberate path back to a sustainable pace. Recovery therefore needs to be built into the operating model.

Making room for recovery in the operating model

The end of an intense period does not mean the team has recovered. An incident may be contained, a regulatory deadline met, or an important transformation completed while the people involved remain depleted. At the same time, the work deferred during that period is usually waiting for them.

Supporting recovery requires more than encouraging people to take care of themselves. It requires decisions about workload, coverage, and timing. Identify who carried the greatest burden, what work can wait, and how responsibilities will be redistributed. Otherwise, exhausted employees may return to a full calendar and an accumulated backlog.

For example, imagine that a team has spent a week responding to a significant incident. The event was contained on a Friday, but the responders are scheduled to return on Monday to their normal meetings, project commitments, and on-call responsibilities.

A more sustainable approach is to stagger time away, shift on-call coverage, move nonessential deadlines, and reduce meetings for those who carried the response. The security function continues operating, but individuals are not left to find space to recover on their own.

When reviewing a sustained period of intensity, consider the human impact alongside the technical and operational lessons discussed in *Chapter 6*. Examine how long people remained engaged, whether handoffs worked, where coverage became thin, and which responsibilities accumulated. Use those observations to improve staffing, rotations, and escalation practices before the next demanding period.

The right response may vary across the team. Someone who worked overnight may need immediate time off, while another person may need relief later after completing follow-up work. Some may prefer to leave early for several days; others may benefit more from taking a full day off. The objective is not to give everyone the same response. It is to understand how they were affected and create meaningful space for them to recover.

For many security teams, intensity has become part of the normal operating environment. Waiting for the work to slow down may mean that recovery never happens. It needs to become a deliberate and visible part of how the team operates.

The example you set matters. Tell the team when you are taking recovery time, whether that means leaving early or taking a day off, and make sure those who carried the workload have an opportunity to do the same. If encouragement alone is not enough, track whether team members actually take recovery time. If you tell people to recover while remaining visibly online and continuing at the same pace, they may conclude that recovery is supported in theory but not in practice.

Recovery is not a reward for extraordinary effort. It is part of managing the risk created by sustained fatigue and preserving the team's ability to perform after the immediate pressure has passed. The next challenge is addressing the daily workload, leadership expectations, and culture that shape the team between those demanding periods.

Sustaining team capacity

Protecting your own capacity cannot come at the expense of the team. If every meeting you decline, decision you delegate, or responsibility you release simply moves additional work to people who are already stretched, the pressure has shifted rather than improved.

Do not wait for someone to escalate that the workload has become unsustainable. High-performing leaders often continue absorbing new responsibilities because they do not want to disappoint you or appear unable to handle the role. By the time they raise the concern, the impact may already be visible in missed commitments, declining quality, or exhaustion.

Make capacity a recurring discussion in one-on-ones and leadership team meetings. Ask what has been added, what is taking longer than expected, which commitments are beginning to slip, and where routine work is regularly moving into evenings and weekends. Most importantly, ask what should stop. These conversations make it easier to address pressure before the individual feels that asking for help is the only remaining option.

Security organizations often add responsibilities faster than they retire them. A new tool creates another platform to manage. A regulatory requirement adds evidence collection and reporting. An acquisition introduces more systems, identities, and stakeholders. Over time, individually reasonable additions can create an unreasonable operating load.

In many organizations, securing additional headcount is increasingly difficult. That makes prioritization even more important. Before concluding that the team simply needs to absorb more, consider whether work can be eliminated, simplified, automated, consolidated, or supported differently. If none of those options creates enough capacity, make the trade-off visible. Leadership should understand which commitments, service levels, or timelines will be affected if additional resources are not available.

For example, when a new regulatory reporting requirement is introduced, do not simply add it to someone's existing responsibilities. Determine whether another report can stop, an overlapping activity can be consolidated, or part of the work can be automated. If the requirement must be added without more resources, identify which existing commitment will move and communicate that decision clearly.

Be intentional about the behavior you recognize. If visibility and praise go primarily to people who work all night or rescue poorly planned projects, the team will learn that heroics are the path to recognition. Also recognize those who prevent emergencies, simplify work, develop others, and create enough structure that the organization does not depend on a last-minute rescue.

A sustainable team will still experience pressure. The difference is whether the organization continually adds work without making choices or regularly revisits what matters, what can stop, and where support is needed. Sustainability is not a one-time design decision; it requires the same periodic attention you apply to risk, strategy, and performance.

Notes from the field with Renana

Case study: when the blueprint had to change

By the time I entered my second year in the CISO role, I had experienced burnout twice earlier in my career. Those experiences taught me to recognize the warning signs, and over time I became more disciplined about many of the practices described here. I protected time for family and exercise, created room to think, and paid closer attention when the pace became difficult to sustain. I believed I had learned how to manage it.

From the outside, writing a book can look like a series of polished milestones: the outline, the finished chapters, and the posts on LinkedIn that mark the journey. The reality behind those moments was very different. I wrote the outline when I was in my third trimester. Soon afterward, I welcomed a newborn, returned to work, navigated changes in the threat landscape, saw one of my direct reports resign, and took on the additional responsibilities of the CIO role. My instinct was familiar: absorb the additional demands and assume I would find a way to manage them.

For several months, I continued at the same pace. I had made commitments that mattered to me, and I knew that much depended on how I showed up. Sleep was scarce, yet I kept treating my capacity as though it had not changed. I recognized some of the warning signs but continued to explain them away. Because I knew the practices, I convinced myself that I could correct course without slowing down.

More than one friend asked how I was doing. I heard their concern, but I continued to describe the situation as temporary. During a call with my executive coach, Elissa, those separate

observations finally landed as one clear message. Taken together, they described a reality I could no longer rationalize: I was experiencing burnout for the third time in my career.

It took time away to understand that the answer was not to recover just enough to return to the same pattern. The blueprint itself needed to change—not only how I recovered, but how I decided what to take on in the first place.

In retrospect, I played a major role in what happened. This experience is why this chapter focuses on managing burnout rather than avoiding it. None of us leads perfectly, and even experienced leaders can return to familiar patterns when the demands accumulate. What matters is recognizing what is happening, accepting when the current approach is no longer working, and making the changes needed to move forward.

Despite the challenges, during this year I led significant transformation efforts across the business, learned a great deal about myself as a leader, and completed the book you are now holding. I am proud of what I accomplished during that period. The experience gave me a clearer blueprint for sustaining my energy while continuing to pursue the technology work that excites me.

Summary

In this chapter, we explored how to manage burnout and sustain your leadership through the pressure inherent in the security executive role. We examined how to recognize early warning signs, distinguish temporary intensity from chronic overload, and protect your capacity through energy management, calendar discipline, boundaries, and reliable coverage. We also considered how trusted relationships, selective learning, and periodic reassessment can help you maintain perspective over time.

Finally, we discussed how delegation, deliberate recovery, and regular capacity reviews can strengthen resilience across the organization. Resilience is not measured by how much pressure you can absorb; it is reflected in whether you and the organization can continue operating effectively when demands increase.

In *Chapter 13*, we will reflect on the progress made during the first year, recalibrate expectations, and prepare for the transition into year two.

Sustained leadership checklist

- Establish a regular self-check. Review changes in your energy, behavior, and decision quality before sustained pressure becomes your normal operating state.
- Protect time for recovery and focused thinking. Clarify how you can be reached when something genuinely requires your attention.

- Build a personal support system. Maintain trusted relationships and identify the few areas where continued learning matters most.
- Review team capacity. Address key-person dependencies and create recovery time after sustained periods of intensity.

Additional resources

- Jim Loehr and Tony Schwartz – The Power of Full Engagement: https://www.simonandschuster.com/books/The-Power-of-Full-Engagement/Jim-Loehr/9780743226752
- Michael Chaskalson – Mindfulness in Eight Weeks: https://www.harpercollins.com/products/mindfulness-in-eight-weeks-the-revolutionary-8-week-plan-to-clear-your-mind-and-calm-your-life-michael-chaskalson
- RSA Conference – Mindfulness in Cybersecurity: A Shield Against Stress and Burnout: https://www.rsaconference.com/library/blog/mindfulness-in-cybersecurity-a-shield-against-stress-and-burnout
- World Health Organization – The World Health Organization-Five Well-Being Index (WHO-5): https://www.who.int/publications/m/item/WHO-UCN-MSD-MHE-2024.01
- National Research Centre for the Working Environment – Copenhagen Burnout Inventory (CBI): https://nfa.dk/vaerktoejer/spoergeskemaer/spoergeskema-til-maaling-af-udbraendthed-cbi/copenhagen-burnout-inventory-cbi
- Cybermindz – Resilience Monitoring for Cyber Teams: https://www.cybermindz.org/what-we-do/resilience-monitoring
- NIST NICE – Mental Health in Focus: Managing Burnout and Finding Balance in Cybersecurity Work: https://www.nist.gov/video/mental-health-focus-managing-burnout-and-finding-balance-cybersecurity-work
- Harvard Business Review – HBR Guide to Beating Burnout: https://store.hbr.org/product/hbr-guide-to-beating-burnout/10406
- CISA – Cybersecurity Education and Career Development: https://www.cisa.gov/resources-tools/programs/cybersecurity-education-career-development

13

Conclusion: Beyond the First Year – A Journey of Continuous Evolution

Take a moment to look in the rearview mirror. Congratulations! You made it through your first year as a security executive. It was likely a year filled with highs, lows, difficult decisions, and more than a few unexpected turns.

You stepped into the role with ideas and aspirations. Over the course of the year, you built critical relationships and trust, established credibility, assessed the organization, defined a security vision and strategic pillars, prioritized risk, secured support, and began strengthening the organization across multiple security domains. Along the way, you learned the business, navigated competing priorities, responded to challenges, and adapted your approach as new information emerged.

The first year was never about solving everything. It was about building the foundation required to lead effectively over the long term. In this final chapter, we will focus on closing out your first year and preparing for what comes next. Specifically, we will cover:

- Wrapping up your first year
- Preparing for your second year

Wrapping up your first year

Before rushing into next year's roadmap, pause and reflect. One of the most common mistakes leaders make is moving directly from one initiative to the next without evaluating the current

state. We will use a three-step process—reflection, documentation, and recalibration—as shown in *Figure 13.1*:



Figure 13.1 – Reflection framework

The process starts by looking back at the year to understand what changed, what you learned, and what should shape your priorities going forward.

Reflecting on your progress

Much like a personal year-end reflection or New Year's resolution exercise, this process is about evaluating where you started, what goals you set, what progress you made, and where gaps still remain. The difference is that, as a security executive, this reflection extends beyond personal growth to include your impact on the security program, your people, and the business itself.

Some priorities were likely achieved faster than expected. Others may have evolved entirely as your understanding of the organization matured. Your goal is not to prove that every initiative was completed exactly as planned. Instead, you should aim to honestly evaluate progress, understand why priorities shifted, and intentionally decide what deserves your focus moving forward.

As with the assessment exercises discussed in *Chapter 1*, it is helpful to structure this reflection intentionally. Schedule a day (or half a day) to step out of the chaos of the day-to-day to ask and answer the following questions:

Reflection Question	**Why It Matters**
Where did the organization make the most meaningful progress?	Identifies initiatives that materially improved security posture

Reflection Question	Why It Matters
Which initiatives were delayed or deprioritized?	Demonstrates how priorities evolved as your understanding of the business and threat landscape matured
What assumptions from your first 90 days proved incorrect?	Highlights growth in your understanding of the organization and improves future decision-making
Which risks were reduced, and which were elevated?	Evaluates whether investments and initiatives moved the needle in the areas that matter most
What new risks or exposures emerged during the year?	Reinforces that security programs must continuously adapt to changes in the business and threat landscape
Which relationships became critical to your success?	Identifies partnerships that enabled progress and should continue to be strengthened
Where did the organization struggle operationally?	Surfaces gaps in execution, staffing, governance, or cross-functional alignment
Which failures or setbacks produced the most important lessons, and how broadly were those lessons shared?	Reveals whether the organization has a learning culture that surfaces issues quickly, shares lessons across teams, and reduces the likelihood of repeating the same failures

Table 13.1 – Reflection questions

The questions above are intended to help you move beyond a simple "what went well and what didn't" exercise. They provide a structured way to evaluate the maturity of the program and the organization's changing risk landscape.

Documenting your thoughts

This is also the time to proactively prepare a year-end or beginning-of-year briefing using the templates and communication frameworks discussed throughout the book. The goal is to capture where the program stands today and what should carry forward into year two. At a minimum, capture the following points:

- **What changed**: The most meaningful accomplishments and areas where progress fell short

- **What moved**: Material changes in risk, maturity, or other indicators you have been reporting throughout the year
- **What changed course**: Priorities that were accelerated, delayed, or deprioritized, and why
- **What you learned**: Assumptions that changed and lessons that should influence future decisions
- **What carries forward**: Unresolved risks, dependencies, and priorities that require continued attention in year two

Tip

Using consistent templates over time helps your audience become familiar with the structure and flow of your updates, allowing conversations to focus less on navigating the presentation and more on the content, risks, and decisions.

Recalibrating expectations and priorities

Once you have documented your perspective, the final step is to recalibrate. Validate and socialize your findings with key stakeholders and revisit the stakeholder relationship map introduced in *Chapter 2*, as it has likely changed since your early days. Their feedback can help identify blind spots, challenge assumptions, and provide additional context you may still be missing.

Use those conversations to determine what should carry forward into year two, what needs to change, and where additional alignment is required. The objective is to enter your second year with a shared understanding of where the program stands and what requires attention next.

Preparing for your second year

One of the more difficult realities of leadership is that by the end of the first year, you may actually have more issues than when you started. Many leaders find this discouraging. After all the investment, effort, and change, how is it possible that the organization still appears to have so many unresolved problems?

The answer is often simple: maturity creates visibility. As organizations improve tooling, governance, telemetry, and operational rigor, they uncover risks and weaknesses that previously existed unnoticed. In many cases, the environment did not become less secure, but the organization gained a clearer understanding of its true exposure.

I have seen annual risk assessment scores decline despite significant program improvements. In one example, the scope of the assessment expanded beyond the enterprise network to

include development and **quality assurance (QA)** environments, uncovering additional gaps that had never previously been measured. In another case, controls believed to be operating effectively were later found to be out of alignment with prior regulatory requirements.

These moments can feel frustrating, especially after a year of hard work and meaningful progress. However, they are often signs of a maturing program rather than a failing one.

This is also one of the defining moments of your leadership journey. The message you deliver (and how you deliver it) will significantly influence how stakeholders perceive both the program and your leadership going into year two. If you communicate uncertainty without direction, stakeholders may begin to associate the growing list of issues with leadership failure rather than increased organizational visibility. Your role is to help stakeholders understand the difference.

Knowing this moment is likely to come, begin preparing the organization for it well before year-end. Around months nine or ten of your tenure, start introducing the idea that stronger visibility and higher standards often reveal additional risk. *Figure 13.2* illustrates this pattern, based on the *Don't Fire Me Chart* described by Phil Venables in his blog post on career longevity in cybersecurity.

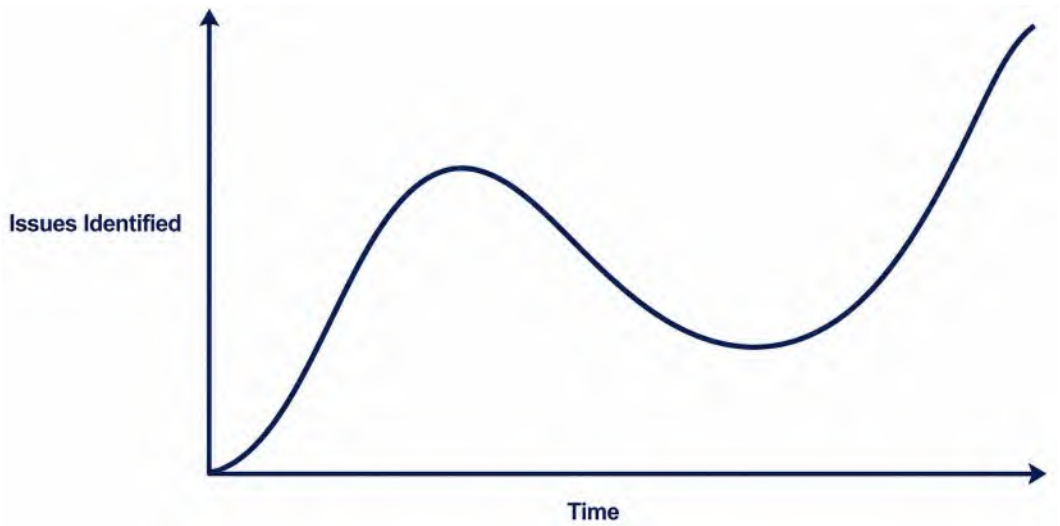


Figure 13.2 – Risk visibility over time

The strength of the diagram lies in its simplicity. It captures a reality many security leaders experience but struggle to explain clearly: as visibility and program maturity improve, the organization may temporarily feel less secure because it now understands risks that were previously hidden.

Just as importantly, the model translates a complex security concept into language that resonates with non-technical executives and board members. It helps shift the conversation away from "*Why do we suddenly have more problems?*" toward "*How are we improving our understanding and management of risk over time?*" The important distinction is whether the increase reflects better visibility into existing risk or a genuine deterioration in the environment. That is the context leadership needs to interpret the trend correctly and determine whether additional action is required. Providing that context can shape the trust, support, and momentum you carry into your second year.

> **Tip**
>
> The *Don't Fire Me Chart* is a memorable name, but you do not need to use that terminology with executives or the board. Consider presenting the underlying concept with a more neutral title, such as *Risk Visibility Over Time*, unless you know the informal name will resonate with your audience.

Year two will not necessarily become easier. The threat landscape will continue to evolve. Business priorities will shift. New technologies, regulations, acquisitions, and organizational changes will introduce new complexity. The difference is that you are no longer starting from zero. You now have context, relationships, operational experience, and proven methods to navigate the organization through uncertainty. And now, you are ready for what comes next.

Chapter checklist

- **Reflect on your first year**. Evaluate where the program made meaningful progress, where priorities shifted, and what you learned along the way.
- **Document where the program stands**. Capture the most important changes, remaining risks, and priorities that should carry forward.
- **Recalibrate with key stakeholders**. Validate your perspective, reset expectations where needed, and align on the areas that require continued attention.
- **Prepare the organization for year two**. Help leaders understand that greater maturity may reveal additional risk and provide the context they need to interpret those changes appropriately.

Additional resources

- Career Longevity & The Don't Fire Me Chart: `https://www.philvenables.com/post/career-longevity-the-don-t-fire-me-chart-1`

14

Unlock Your Exclusive Benefits

Your copy of this book includes the following exclusive benefits:







Follow the guide below to unlock them. The process takes only a few minutes and needs to be completed once.

Unlock this Book's Free Benefits in 3 Easy Steps

Step 1

Keep your purchase invoice ready for *Step 3*. If you have a physical copy, scan it using your phone and save it as a PDF, JPG, or PNG.

For more help on finding your invoice, visit `https://www.packtpub.com/en-us/unlock?step=1`.

Note: If you bought this book directly from Packt, no invoice is required. After *Step 2*, you can access your exclusive content right away.

Step 2

Scan the QR code or go to packtpub.com/unlock.



On the page that opens (similar to *Figure 14.1* on desktop), search for this book by name and select the correct edition.

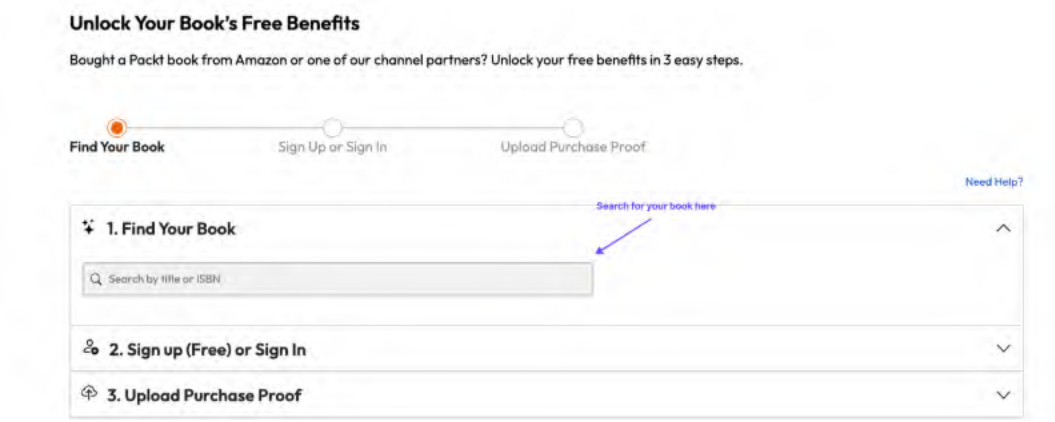


Figure 14.1 – Packt unlock landing page on desktop

Step 3

After selecting your book, sign in to your Packt account or create one for free. Then upload your invoice (PDF, PNG, or JPG, up to 10 MB). Follow the on-screen instructions to finish the process.

Need Help

If you get stuck and need help, visit `https://www.packtpub.com/unlock-benefits/help` for a detailed FAQ on how to find your invoices and more. This QR code will take you to the help page.

Note: If you are still facing issues, reach out to `customercare@packt.com`.

Appendix

Security Executive Onboarding Questionnaire

Starting a new security leadership role requires learning far more than can reasonably be covered in a handful of introductory meetings. The questions in *Chapter 1* focus on the areas we believe are most important during your initial assessment. This appendix provides a more comprehensive set of questions and information requests you can use as your understanding of the organization develops.

This questionnaire is designed for security executives at different levels of responsibility, including CISOs, deputy CISOs, heads of security, and leaders responsible for major security functions. Not every question will apply to every role or organization. Use it as a reference rather than a checklist: select the areas most relevant to your scope, adapt the questions to your environment, and prioritize deeper exploration based on what you learn during your listening tour.

Some areas will require more than a standard introductory meeting. When a topic is particularly important to your responsibilities or initial assessment, consider scheduling a dedicated two- to four-hour deep-dive session with the relevant team during your first 60 days. These sessions create space to understand how the capability operates today, review supporting documentation, and explore areas that warrant further attention.

Using this appendix

You do not need to answer every question before forming your initial point of view. Start with the questions most relevant to your role, risk profile, and current business priorities. Request supporting documents where they will help validate what you hear, and revisit the remaining areas as your context improves. Where your role does not include direct access to a particular

audience or artifact, such as board materials, work through your manager or the appropriate executive sponsor.

Understanding the business

These questions help you understand the organization's strategy, operating model, priorities, and the business initiatives that security is expected to support.

- What are the company's core values and leadership principles?
- How is the executive leadership team structured, and which business lines or functions does each leader own?
- How are technology and security teams organized, including the major functions and leadership responsibilities within each?
- What are the organization's top business, growth, or transformation strategies?
- What are the current business-line, technology, and product strategies?
- Which major projects, programs, or products is the security organization expected to enable?
- Which board meetings, leadership offsites, planning sessions, or team activities should you be aware of or plan around?
- What legal entities, subsidiaries, or significant operating entities sit within the broader organization?

Understanding governance and key stakeholders

Use this section to understand the governance structures, recurring forums, executive expectations, regulatory relationships, and open issues that shape your role.

- Review information-security materials presented to the board or relevant board committees during the past 24 months, where your role permits access.
- Review relevant technology materials presented to the board or board committees during the past 24 months.
- What is the upcoming board and committee schedule, and where are security or technology topics expected on the agenda?
- Which governance committees does your role participate in, and what is the cadence of each?
- Which recurring technology, risk, legal, product, or business meetings should you attend?

- Who are the key first-, second-, and third-line stakeholders for your role, including partners in the HR, finance, legal, communications, sourcing, risk, and internal audit departments?
- Who are the key regulatory contacts relevant to the security program?
- Where are the organization's major offices, data centers, vaults, or other critical facilities?
- Which corporate audits or regulatory examinations are in progress or planned, and who coordinates the associated materials and presentations?
- What security issues are currently open? What are the target closure timelines and tracking routines?
- What significant regulatory, audit, or second-line issues were closed during the past five years, and what themes emerged?
- What are the current objectives, key results, or goals for the security organization?
- Which major projects, programs, or backlog items is the security organization sponsoring or driving?
- Who leads the Project Management Office, Product Management Office, or equivalent delivery/governance functions?

Understanding the organization and talent

These questions help you understand the structure of the security organization, leadership capability, talent practices, location strategy, and development opportunities.

- What leadership-development programs are available across the organization?
- Review the current organizational charts for technology, security, and any functions directly within your scope.
- Where appropriate and permitted, review a current workforce roster showing role, location, reporting line, tenure, and relevant performance history.
- What is the organization's location and hybrid-work strategy?
- What leadership offsites, team-building activities, exercises, or recurring leadership routines are planned?
- Review recent performance evaluations for your direct reports or leadership team, where appropriate.

- Which universities, military-transition programs, apprenticeships, professional groups, or other channels are used to build the talent pipeline?
- What documented career paths, learning paths, development programs, and upskilling opportunities exist for security and technology employees?

Understanding financials and vendors

Use these questions to understand the resources available to execute the security program, the economics of the organization, and major supplier commitments.

- What are the current-year and next-year operating and capital budgets within your scope?
- Are there cost-reduction, efficiency, or savings commitments already in place? What actions have been identified to meet them?
- What is the manager-to-individual-contributor ratio, and are there material outliers?
- How many managers have very small teams, and what is driving those structures?
- How many employees report to managers in a different location or city?
- How many management layers exist within the organization?
- What has monthly budget-forecast accuracy looked like over the past 12 months?
- Review the major suppliers and vendors within your scope, including product or service, purpose, cost, contract owner, and renewal date.
- For on-premises environments, what depreciation schedules are used for hardware and what amortization schedules are used for software?
- How are SaaS, PaaS, and IaaS consumption and cloud spend tracked? Is there a FinOps process or system you can access?

Understanding risk, controls, and compliance

These questions help you understand how the organization defines, measures, accepts, tracks, and governs security risk and how controls connect to regulatory and industry requirements.

- What are the organization's top information-security risks, and which are owned by security versus governed or overseen by security?
- What known policy exceptions, control exceptions, or formal risk acceptances are currently open?
- What risk model is used, and how are risk ratings determined?
- Is there an operational-risk taxonomy, and how does cybersecurity map into it?

- Is there a **risk and control self-assessment (RCSA)** process? If so, review recent ratings and understand how they connect to other risk repositories.
- Where are security risks and treatment plans tracked?
- Are there documented risk-appetite statements for business lines or major risk areas?
- Review the most recent external enterprise-wide information-security risk or control assessment.
- Which frameworks, regulations, or standards have been formally assessed, such as NIST CSF, **Gramm–Leach–Bliley Act (GLBA)**, GDPR, or other requirements relevant to the organization?
- Is there an integrated requirements library that maps regulatory and standards obligations into a common control set?
- How do external requirements map into policies, standards, procedures, and technical baselines?
- What is the security control architecture, and how many documented controls exist?
- How are controls tested for design and operating effectiveness?
- What portion of control testing is automated?
- Which control certifications or external attestations has the organization obtained, such as **System and Organization Controls (SOC)** reports or ISO certifications?
- Is there a security dashboard that shows control gaps, overdue vulnerabilities, threats, incidents, or other material risks?

Understanding architecture and infrastructure

This section focuses on the technical environment that the security program protects and depends on, including internet-facing infrastructure, remote access, applications, cloud environments, assets, and development pipelines.

- Where are the organization's internet data centers or major internet ingress and egress points located?
- What internet bandwidth is associated with each major site?
- What carrier- or cloud-based DDoS protection is in place, and what volumetric protection levels are supported?
- What on-premises DDoS protection is in place, if any?
- What Layer 7 DDoS protection is in place, such as cloud **web application firewall (WAF)** or equivalent services?

- Where are other critical information-processing facilities, data vaults, or data bunkers located?
- What public IP address ranges does the organization own or operate?
- How are **Border Gateway Protocol (BGP)** advertisement changes monitored, and who is alerted when changes occur?
- Review the inventory of registered internet domain names.
- Is there a domain-brand monitoring and takedown service? What service levels apply?
- Where are remote-access or VPN concentrators located, and what proportion use strong authentication?
- Is external **Remote Desktop Protocol (RDP)** access permitted anywhere in the environment?
- Where is internet- or extranet-facing virtual desktop access used, and what authentication controls apply?
- Is there a complete inventory of external connections, including extranets, business-to-business VPNs, and other connectivity?
- Approximately how many workstations are in use, and what is the distribution by device type and operating system?
- Approximately how many servers or compute instances are in use, and what is the operating-system distribution?
- How many business applications exist? Which are on-premises versus cloud-based, and which are SaaS, **platform as a service (PaaS)** and **infrastructure as a service (IaaS)**?
- Which applications are modernized, which carry material technical debt, and which depend on unsupported components?
- Which applications are considered critical to the business?
- Review high-level public cloud architecture diagrams and major cloud landing zone designs.
- Review CI/CD pipeline diagrams and the security controls integrated into development and deployment processes.

Understanding resilience, business continuity, and crisis management

Use these questions to understand how the organization prepares for disruption, recovers critical services, protects backups, tests recovery capabilities, and coordinates crisis response.

- How is business criticality determined for operations, processes, services, applications, suppliers, people, and data?
- How are technology assets tiered from a recovery standpoint?
- How often are recovery-time objectives for technology assets tested?
- How often are business recovery plans tested?
- Is integrated disaster recovery or business continuity testing performed with critical suppliers, clients, or customers?
- Do resilience exercises include destructive-malware or ransomware scenarios?
- Do resilience exercises include DDoS scenarios?
- What percentage of applications, technology assets, or recovery plans typically fail DR or BCP tests?
- Review the backup architecture, including immutable disk, snapshots, vaulting, tape, or other recovery mechanisms.
- Review backup-replication architecture and any data vault or bunker designs.
- Are all online backups immutable? If not, which are not, and what is their business criticality?
- What DDoS scrubbing capability exists, and what portion of internet-facing applications is covered?
- Are tabletop exercises conducted with security and technology teams? Who coordinates them, and how are lessons institutionalized?
- Are executive tabletop exercises conducted with senior business leaders? Who coordinates them?
- Review recent and planned tabletop exercises.
- Review business-continuity and crisis-management processes, escalation criteria, scenario runbooks, and after-action reporting.
- Review major incidents or crises from the past three years.
- Consider scheduling a dedicated deep dive on disaster recovery, business continuity, incident response, and crisis management during your first 45 to 60 days.

Conducting security program deep dives

Initial conversations rarely provide enough depth to understand every security capability. As you identify areas that are particularly important to your scope, risk profile, or early priorities, schedule dedicated deep dives with the teams responsible for those capabilities. You do not need to complete every deep dive during your first 60 days; prioritize the areas that matter most based on what you learn during the initial assessment.

Establishing the security program baseline

Before or alongside the deep dives, gather a baseline view of the current program:

- What security products and supplier solutions are used across major control and process areas? Review the vendor, product, purpose, and cost where available.
- Where are the current information-security policies, standards, and technical baselines maintained?
- How does the security function support or add value to fraud-management teams?
- Is there a dedicated innovation team, or is innovation expected across functions?
- What enterprise-wide capabilities exist for PKI, encryption, secrets management, tokenization, data redaction, and application authentication?
- Are external internet-based security-rating services used to monitor the organization's posture? How does the organization compare with peers?
- Are external scoring services used to monitor critical suppliers?
- How frequently are phishing simulations performed, and what did the most recent enterprise-wide results show?
- Does the organization carry cyber insurance? What are the coverage limits, premiums, ownership, and key requirements?
- Review recent internet-perimeter penetration tests and red team assessments.
- Review recent enterprise-wide or business-specific information security program assessments.
- Review open internet-facing vulnerabilities, including severity and age.
- Confirm whether remote-access VPNs, virtual desktops, and other remote-access pathways use strong authentication, and identify any external RDP exposure.

Ransomware readiness

- Is there a documented ransomware or destructive malware kill chain with preventive, detective, response, and recovery controls mapped to each stage?

Security strategy and risk assessment

- What are the known strategic security gaps, risks, and active treatment plans?
- Review the most recent NIST CSF or equivalent framework assessment.
- Review recent external risk and control assessments.
- Review the current one-year and three-year security strategy or equivalent planning horizons.

Vulnerability and patch management

- What vulnerability-management service levels, objectives, or remediation timelines are defined? How does Technology perform against them?
- Which internet-facing vulnerabilities remain open, and how old are they?
- What other material vulnerabilities are currently open?
- What is the scanning coverage and frequency across environments?
- Are authenticated vulnerability scans performed?
- Is there an off-network patching capability?
- How are vulnerabilities in images, containers, Kubernetes, and software dependencies managed?
- Is there a repave or rehydrate process for rolling out new golden images? Which environments use it, and how quickly can systems be refreshed?
- Is there a program for retiring prohibited, legacy, or unpatchable technology?
- How is vulnerability management integrated with technology-modernization work?
- As applications are modernized and made modular, how are risks managed when components of the same application run across different environments or clouds?

Penetration testing and offensive security

- Review the penetration-testing program, including red, blue, and purple team activities.
- Review recent reports, open findings, remediation status, and how results feed into risk and engineering priorities.

Monitoring, detection, and security operations

- How are security operations centers and related monitoring functions organized?
- What is the depth and coverage of telemetry across endpoints, networks, cloud, identity, applications, and data?

- How are alerts leveled, triaged, escalated, and retained?
- What packet-level or forensic recording capabilities exist, and what are the retention periods?
- How are threat hunting, data science, AI/**machine learning (ML)**, and automation used within security operations?
- Is MITRE ATT&CK or an equivalent framework used to assess detection coverage?
- Are adversary-emulation exercises conducted?
- What process identifies manual work or operational toil that can be automated through SOAR, RPA, or other automation?
- Is there a formal security automation center of excellence or equivalent capability?

Cloud security

- What are the major external workloads or services using IaaS, PaaS, and SaaS?
- What are the major internal implementations of IaaS, PaaS, and SaaS?
- Review the major cloud-service architectures across providers such as AWS, Azure, Google Cloud, or others in use.
- Is there a high-level architecture or placemat showing cloud components and the security services applied to each?
- What does the service-edge or **secure access service edge (SASE)** architecture look like, and which supplier products support it?
- How fully are security tooling and services integrated into CI/CD pipelines?
- How is the security backlog managed within product and development processes?
- Are security and other non-functional requirements integrated into engineering backlogs?
- What telemetry and observability are available from public-cloud environments?
- How is configuration drift identified and resolved in public-cloud services and workloads? Is **cloud security posture management (CSPM)** used?
- How is configuration drift identified and resolved in SaaS services? Is **SaaS security posture management (SSPM)** used?
- How is data-location or data-posture drift monitored? Is **data security posture management (DSPM)** used?

- What development methodologies and agile practices are in use, and how is security integrated into them?
- Are customer journeys documented, and is security included when those backlogs are prioritized?

Incident response and recovery

- Review the most impactful cyber incidents from recent years and the lessons that followed.
- How is the incident response function organized, and how does it integrate with security operations, crisis management, disaster recovery, and business continuity functions?
- Review operational runbooks, escalation criteria, exercise cadence, after-action reviews, and major remediation commitments.

Threat intelligence

- How is threat intelligence collected, analyzed, and distributed?
- Which suppliers, ISACs, government agencies, and intelligence feeds are used?
- Are industry-standard protocols such as **Structured Threat Information Expression (STIX)/Trusted Automated Exchange of Intelligence Information (TAXII)** used for receiving or sharing indicators and courses of action?
- Where relevant, who holds government clearances and how frequently are classified or restricted briefings received?
- Who or what are the top threat actors or attack types of concern to the organization?
- How are threat-actor groups, tactics, techniques, procedures, and infrastructure tracked?
- How much automated response to external threat intelligence is in production?
- Does the intelligence function produce broader intelligence beyond cyber threat intelligence, such as market, regulatory, emerging technology, or customer intelligence?
- How does situation reporting work, and what recurring intelligence products are produced?

Identity and access management

- Review the IAM architecture and major products.
- Which IAM controls are centralized versus decentralized?
- How are privileged access and service accounts managed?

- How are credentials, secrets, and vaulting handled?
- How are user joiner, mover, and leaver processes managed?
- How are access reviews performed?
- How are encryption keys, PKI, **hardware security modules (HSMs)**, and secrets managed?
- Review the directory architecture and any privileged or hardened directory designs.

Customer identity and authentication

- Review the architecture and products supporting customer identity and authentication.
- How is identity proofing performed?
- What authentication capabilities are available?
- How are high-risk transactions identified, and when is step-up authentication required?
- How do customer-authentication systems integrate with fraud, customer contact, and other enterprise platforms?

Governance, risk, and control

- Review the architecture of systems used to manage policies, standards, baselines, controls, risks, risk acceptances, and open issues.
- How are internal and external findings linked to risk, control, and remediation records?

Network security

- Review the high-level network architecture and major security controls, including firewalls, routing and switching, IDS/IPS, proxies, remote access, VPNs, taps, packet capture, SD-WAN, and SASE.
- Identify areas of legacy architecture, material single points of failure, or major modernization work.

Endpoint security

- Review the endpoint environment, including physical and virtual workstations, laptops, desktops, refresh intervals, and patch management infrastructure.
- Review anti-malware, **endpoint detection and response (EDR)/extended detection and response (XDR)**, host-protection, systems-visibility, security-baseline, and configuration-validation capabilities.

Application security

- Review the application-security program, including **static application security testing (SAST), dynamic application security testing (DAST)**, **interactive application security testing (IAST)**, **runtime application self-protection (RASP)**, WAF, container security, microservices, and API security.
- Is there an API gateway strategy, and what security controls are embedded within it?
- Are API posture-governance tools or equivalent controls in use?
- How are application-security findings integrated into development workflows and remediation backlogs?

Third-party risk management

- Review the third-party risk-management program, including how suppliers are tiered, assessed, monitored, and escalated.
- Identify the most critical suppliers, their current risk ratings, and known material gaps.

Insider threat and data protection

- Review the insider-threat program, including governance, investigative processes, and typical use cases.
- Review data loss prevention, user and entity behavior analytics, monitoring use cases, and common incident patterns.

External engagement and partnerships

- How does the security organization manage relationships with industry groups, government agencies, strategic partners, customers, and other external stakeholders?
- Which external relationships are most important during incidents, regulatory events, or major program changes?

Business change and security enablement

- How does the organization assess security risk when business processes, products, technologies, or operating models change?
- How does security provide enablement and guidance early enough to influence design decisions?
- Is there a formal DevSecOps or equivalent secure-change process?

Artificial intelligence and machine learning governance

- How are AI, ML, and **large language model (LLM)** use cases governed and enabled?
- How are security, privacy, data, third-party, and model risks evaluated before and after deployment?

Getting oriented to the organization

A few practical onboarding questions can reduce friction and help you become productive more quickly.

- Where is the corporate directory or equivalent employee directory?
- Is there a corporate glossary of acronyms, business terms, and internal system names?
- Who manages corporate travel and executive travel support?
- Is there a formal innovation process, technology lab, incubator, or equivalent function? Who leads it?



packtpub.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

At www.packtpub.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Other Books You May Enjoy

If you enjoyed this book, you may be interested in these other books by Packt:



Cybersecurity Strategy for the AI-Driven Era

Tim Rains

ISBN: 9781806028573

- Identify common enterprise intrusion paths and reduce initial compromise
- Distinguish credible threat intelligence from industry noise
- Improve vulnerability management while reducing risk and cost
- Assess malware, ransomware, and internet-based attack techniques
- Secure APIs and reduce exposure from trusted enterprise tools
- Evaluate Zero Trust and attack-centric security strategies
- Apply cloud, resilience, and AI capabilities to improve security outcomes
- How governments request data and how enterprises manage access, risk, and oversight



A Day in the Life of a CISO

David J. Gee

ISBN: 9781806110698

- Adapt security strategies to manage emerging threats, including AI-driven risks
- Build and execute cyber strategies while balancing business needs and budget constraints
- Discover effective leadership and communication techniques critical for CISOs
- Implement talent development strategies for building a resilient cybersecurity team
- Learn from real-world incidents, including how to recover after breaches
- Explore career development pathways for cybersecurity professionals, including alternative and non-traditional paths to CISO roles

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packt.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Share your thoughts

Now you've finished *The Cybersecurity Executive's First Year Playbook*, we'd love to hear your thoughts! Scan the QR code below to go straight to the Amazon review page for this book and share your feedback or leave a review on the site that you purchased it from.



https://packt.link/r/1806679337

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Index

A

AI development lifecycle (AIDLC) **186**

Alignment Matrix **79 – 81**

account takeover (ATO) **250**

attorney-client privilege (ACP) **137**

auto-remediation **174**

B

Bring Your Own Device (BYOD) **20**

Business Information Security Officer (BISO) model
- defining 280
- implementing 279
- strategic business partnerships, sustaining 281

Business Information Security Officers (BISOs) **276**

budget request template
- accelerated investment 127
- minimum viable investment 126
- recommended investment 126
- using 125, 126

business context **8**
- general knowledge 9
- operational dependencies 10
- regulatory and compliance landscape 10, 11
- revenue 9, 10

business email compromise (BEC) **283**

C

C-Suite and board security culture
- influencing 295
- ongoing engagement 296, 297
- threats response, through proactive communication 295, 296

C-suite **61, 62**
- 10- minute security update framework 62 – 64

CTEM framework
- applying 170
- discovery 171, 172
- mobilization 172 – 174
- prioritization 171 – 173
- scoping 171, 172
- validation 171 – 173

Capability Maturity Model Integration (CMMI) **11**

Capital Expense (CapEx) **24**

Cascade Pyramid **79, 80**

Chief Finance Officer (CFO) **143**

Chief Legal Officer (CLO) **143**

Continuous Threat Exposure Management (CTEM)
- used, for moving vulnerabilities to exposure 170

Copenhagen Burnout Inventory (CBI) **322**

Cybermindz **322**

Cybersecurity and Infrastructure Security Agency (CISA) **290**

centralized SOC **180**

chief compliance officer (CCO) **233**

compliance **232 – 236**
- governance committees 236 – 238

continuous security awareness **283**
- core components, defining 284, 285
- diverse communication channels, delivering 285, 286

continuous threat exposure management (CTEM) **168**

contractual protections
- additional security 130, 131
- using 128

couselor **47**

credible security budget request
- ask navigation 127, 128
- budget request template, using 125, 126
- building 120
- funding 122
- groundwork 121, 122
- making 120

credible security budget request, funding
- budget 123
- initiatives 122
- risk 122
- timing 123 – 125

critical data
- classifying 200 – 202
- data classification models, for models 203
- ownership and accountability for 204, 205

critical risks **228**

cross-functional group **142**

crown jewels **190**
- identity and data, protecting 191 – 193

D

Data Loss Prevention (DLP) **99, 103**

Distributed Denial of Service (DDoS) **9, 52**

data protection strategies
- across data life cycle 205
- backup and recovery 209, 210
- data stages 206 – 208
- encryption and key management 208

dependencies sequencing
- foundational prerequisites, identifying 107
- hidden enabler projects 108
- risk-based urgency, evaluating 108, 109

distributed SOC **180**

documentation and information validation **33**
- common mistakes, avoiding 33, 34
- documentation templates, using 34
- legal liability, checking 35
- observations, validating 35

E

executive and board sessions
- alignment 265
- cadence, reporting 264
- case study 267, 268
- meeting 268 – 271
- narrative, drafting 265, 266
- preparing 264
- reviewing & aligning 266
- storytelling practice 266

external stakeholders
- consulting firms 25
- external audit 25
- meeting 25
- vendors 26

F

Factor Analysis of Information Risk (FAIR) **311**

Financial Services (FS)-ISAC or Healthcare (H-ISAC) **290**

Financial Services Information Sharing and Analysis Center (FS-ISAC) **251**

federally funded research and development centers (FFRDCs) **181**

fourth-party vendor risk **213**

G

Gantt chart **109**

General Data Protection Regulation (GDPR) **10**

Governance, Risk, and Compliance (GRC)
policy development checklist 226
security policies and standards, developing 222 – 225
governance, risk, and compliance (GRC) 219
as leadership function 220 – 222
group coaching 151

H

Health Information Sharing and Analysis Center (H-ISAC) 251
harvest now, decrypt later (HNDL) 200
high risks 228
high-performing team
building 143, 144
expectations, setting with recruitment 144 – 146
hiring 144
interview process 146, 147
references, using 148, 149
talent recognition 149, 150
high-performing team, talent recognition
appreciation 151
coaching 151
training strategy, using 150
human identities 195

I

IT and product leaders
aligning, around shared business outcomes 50 – 52
collaborating with 50
competing priorities 50
Information Sharing and Analysis Center (ISAC) 180, 290
Information Sharing and Analysis Organization (ISAO) 180
incident response (IR)
capabilities, maturing 160
current IR plan, accessing 163
excellence, building 158 – 160
industry standards, using 163 – 167
incident response capabilities
incident response cadence (proactive), establishing 161, 162
role evolution, during incidents (reactive) 160
internal stakeholders
business leaders 21
finance and procurement 24
Human Resources (HR) 22
legal 21
meeting 21
physical security 23
risk and internal audit 23
third-Party risk management 24

J

just-in-time (JIT) 191, 195

K

Key Results (KRs) 158
key performance indicators (KPIs) 77, 78
key risk indicators (KRIs) 77, 78

L

legacy risk
managing 105
listening tour
conducting 11, 12
direct meeting 17
general questions 14, 15
internal stakeholders, meeting 21
quick meeting 16
technology leaders meeting 18
time and structure, creating 12, 13
long-term trust
building 64
lower risks 228

M

MITRE ATT&CK framework
using 182
materiality 140

case study 142
cross-functional group, assessing 142, 143
executive leadership and board, notifying 141

maturity measurements
connecting 313 – 315

mean time to detect (MTTD) **51**

mean time to respond (MTTR) **51**

mentor **47**

mobile device management (MDM) **215**

multi-factor authentication (MFA) **194, 223, 315**

N

Network Access Control (NAC) **30**

New York State Department of Financial Services (NYDFS) **10**

non-functional requirements (NFRs) **186**

non-human identities **195**

O

Objective and Key Results (OKRs) **157**

Operating Expense (OpEx) **24**

one-on-one coaching **151**

operational TI **175**

organizational culture
Cross-Functional collaboration, reviewing 32
evaluating 31
leadership alignment, assessing 31, 32
risk appetite and ownership, identifying 32

P

Prioritization Quadrant Model **95, 96**

personally identifiable information (PII) **134**

perspective role
career resilience, maintaining 332, 333
continuing 331, 332
maintaining 329
personal support system, building 330, 331

phased implementation
dependencies, sequencing across initiatives 106
planning 106
roadmap 109
roadmap performance, reviewing 112, 113
roadmap progress, measuring 111

post-quantum cryptography (PQC) **208**

priorities, for security initiatives
common mistakes, avoiding 90, 91
establishing 90
prioritization matrix, building 91
visualizing 95

prioritization matrix
building 91
prioritization factors, applying 93, 94
prioritization factors, identifying 91 – 93

privacy incidents
case study 139
escalating 139, 140
materiality, assessing 140
navigating 133
pitfalls 138, 139
preparing 133
privileges 137
responsibility, shifting from technical response 135, 136
security, recognizing 134, 135

privilege creep **197**

privileged access **211**

privileged access management (PAM) **194**

privileged human identities **195**

proactive vulnerability **168**

procurement levers
- core security leaders 129, 130
- partnering 131, 132
- using 128

program planning **68**
- common pitfalls 69, 70
- tactical to strategic thinking 68

protected health information (PHI) **134**

R

Reduce Mean Time to Detect (MTTD) **158**

Reduce Mean Time to Respond (MTTR) **158**

recovery point objectives (RPO) **209**

recovery time objectives (RTO) **209**

reflection framework **341, 342**
- expectations and priorities, recalibrating 344
- progress, reflecting 342, 343
- thoughts, documenting 343

reinforcing learning
- exercise documentation and legal privileges, managing 292
- gamification, using as testing 292
- live exercises, conducting to validate readiness 291
- phishing simulations, using 289
- tabletop exercises, using to improve decision-making 290
- through testing 289

reporting framework
- Ad-Hoc Structure 248
- building 247
- compliance posture 259, 260
- industry or peer security incidents 252, 253
- maturity assessment 256 – 259
- metrics 263, 264
- risk posture 253 – 256
- roadmap 261 – 263
- threat landscape 249 – 251

resilience
- building, into operating model 333
- case study 337, 338
- control, delegating 334, 335
- recovery, making 335, 336
- team capacity, sustaining 336, 337

return on investment (ROI) **120**

return on investment (ROI) of security initiatives
- demonstrating 308 – 310
- risk reduction, quantifying 311, 312
- value, demonstrating through business enablement 312

risk considerations **226**
- elf-identified risks 230
- risk appetite 227
- risk management KPIs 232
- risk register, as system of accountability 228
- risk tolerance 227
- roles and responsibilities 230, 231

risk visibility **344 – 346**

robotic process automation (RPA) **195**

role-based access control (RBAC) **195, 198**

S

SOC
- centralized SOC 180
- distributed SOC 180
- maturing 180, 181
- maturing, from reactive to predictive 182, 183
- virtual/hybrid SOC 180

Security Information and Event Management (SIEM) **302**

Security Plan Flowchart **79 – 81**

Security Scorecard **52 – 55**

Security Simplification case studies
- platform to best-in-class 103, 104

platform to platform 102, 103
Security simplification case studies **102**
Sun Diagram Model **96, 97**
security architecture
as strategic enabler 183 – 186
security awareness
versus security training 287
security champions program **277**
defining 277
future talent, developing 278
security education programs
calendar, building 293 – 295
continuous security awareness 283
designing 282
security training, delivering 287
security leadership
boundaries and coverage, setting 328, 329
calendar, protecting 327, 328
decision quality, preserving 325 – 327
energy, managing 324
protecting 323
security leadership impact
burnout warning signs, recognizing 321, 322
recognizing 320
structured check-in, using 322
security metrics
aligning 307
automating 306
defining, with business objectives 302 – 304
operational metrics, versus executive metrics 305, 306
security outcomes
communicating, to technical and nontechnical audiences 315
technical achievements, translating into business outcomes 316
security perimeter
human identity 195, 196
identity sprawl 197
identity, using as 195
non-human identity 195, 196
privilege creep 197
security philosophy
defining 70
guiding principles, establishing 70 – 72
risk-innovation-compliance balance 72
security, aligning with business objectives 72, 73
security plan **78**
cascading 83
cross-functional partners 84
executives and board 84
one-page security plan 82
overview, creating 83
security teams 83
security plan visual format **79**
Alignment Matrix 81
Cascade Pyramid 80
Security Plan Flowchart 81
security posture
assessments and audit reports 29, 30
asset inventory 28
identifying 27
policies and governance 29
risk landscape analysis 30, 31
security metrics 27
threat exposure management 28
tool and control coverage 28
security program
integration, across business units 158
Objective and Key Results (OKRs), defining 157, 158
operational backbone, building 156
security risk
translating, into business impact 245, 246
security roadmap visualization **109**
Gantt chart timeline 109
swimlane timeline 110
security strategic agility

emerging risks and technologies, leveraging 85
maintaining 85
review rhythm, building 86

security team
security, scaling 277

security technology stack optimization **97, 98**
future state, designing 101, 102
tool mapping 100, 101
tools, evaluating 98, 99

security training
for employee populations 288
reinforcing learning, through testing 289
versus security awareness 287

security vision
initiatives, documenting 76, 77
metrics, selecting to track progress 77
reflecting on 74
setting 73
strategy and initiatives 73, 74
translating, into into long-term strategic pillars 76
vision statement, creating 75

self-identified risks **230**

shadowing **151**

software dependencies **212**

sponsor **47**

stakeholder relationships
cadences, determining 58, 59
making time, for connection 60
managing 55
partnership mindset, building 56
stakeholder map, creating 56 – 58

strategic TI **175, 176**

supply chain
access risks 214, 215
identity risks 213 – 215

swimlane timeline **110**

T

Team Assessment Tool **40, 41**
champions, identifying 43, 44
explorations 45, 46
skills and role alignment, evaluating 42, 43

Three Lines of Defense model
first line of defense 231
second line of defense 231
third line of defense 231

tactical TI **175**

tactics, techniques, and procedures (TTPs) **175, 182**

target maturity **314**

team empowerment
success, amplifying through recognition 49
support roles 46 – 48
through development and recognition 46

technical debt
managing 105

technology leaders meeting **18**
architecture 19
infrastructure 20
software development 18, 19

temporary pressure
from chronic overload 322

third-party risks
identifying 210 – 212

threat exposure management **28**
security incidents 29

threat intelligence (TI)
integrating, into decision making 174, 175
intelligence-led defense, building 176, 177, 180
operational TI 175
strategic TI 175, 176
tactical TI 175

threat landscape **249 – 251**

traditional vulnerability management
limitations 169

U

U.S. Securities and Exchange Commission (SEC) **10**

V

Virtual Desktop Infrastructure (VDI) **20**

virtual/hybrid SOC **180**

W

World Health Organization-Five Well-Being Index (WHO-5) **322**