CYBER DEFENSE MAGAZINE

eMAGAZINE

JANUARY 2025

In This Edition

AI and Elections

The SME Cybersecurity Paradox: Why Smaller Businesses Are Prime Targets

Ten Cloud-Agnostic Cybersecurity Tips for Protecting Your Data Across Platforms

...and much more...

MORE INSIDE!

`

CONTENTS

@MILIEFSKY

From the

Publisher…

Cybersecurity in 2024 was a wake-up call because it exposed just how vulnerable our interconnected world really is. From the healthcare sector being crippled by ransomware to sophisticated nation-state attacks exploiting zero-day vulnerabilities, the message is clear: no one is safe, and complacency is dangerous.

APIs, supply chains, and human error became glaring weak points, reminding us that our defenses need to be proactive, not reactive. The rise of AI-driven attacks and deepfakes showed us that cybercriminals are evolving — and fast. If organizations don't adopt zero trust, continuous monitoring, and AI-driven threat detection, they're just sitting ducks.

2024 taught us that in cybersecurity, waiting to react is a recipe for disaster. It's time to harden our defenses and stay a step ahead — because the threats aren't slowing down.

If you haven't adopted a proactive, zero-trust, AI-assisted security posture, you're at risk. The threats are evolving — so should your defenses.

To the infosec solution providers: Entering the Global InfoSec Awards for 2025 is your chance to showcase your cybersecurity innovation to the world. These awards highlight cutting-edge solutions and offer industry validation, setting you apart from the competition. Winning brings credibility, media exposure, and new opportunities. Don't stay in the shadows — let the world see how you're leading the charge in cybersecurity.

https://cyberdefenseawards.com/

Stay vigilant. Stay secure. And remember — cybercriminals never sleep, so neither can your cybersecurity strategy.

Warmest regards,

Gary S. Miliefsky

Gary S. Miliefsky, fmDHS, CISSP®
CEO/Publisher/Radio/TV Host

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR-IN-CHIEF
Yan Ross, JD
yan.ross@cyberdefensemagazine.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451

https://www.cyberdefensemagazine.com

PUBLISHER

Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
https://www.cyberdefensemagazine.com/about-our-founder/

13 YEARS ★★★★★ ANNIVERSARY

13 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense Magazine is your go-to-source for Information Security. We're a proud division of Cyber Defense Media Group

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS

PROFESSIONALS WIRE WEBINARS

CYBERDEFENSECONFERENCES

Welcome to CDM’s January 2025 Issue

From the Editor-in-Chief

Entering the new year, we can reliably report that our base of authors and topics continues to expand along with our readership. Our many subjects reflect a forward-looking appreciation for the speed and breadth of developments in cybersecurity technology and practice.

The deep analysis provided by our contributing authors helps us understand and share with our readers the responses to the growing challenges to cybersecurity presented by cyber criminals, state-actors, and others who seek to interfere with the smooth operation of elements of critical infrastructure.

The technical side includes focus on AI, quantum computing, supply chain issues, and ransomware developments. Featured areas of concern include such critical infrastructure sectors as finance, health care, automotive applications, and defense endeavors.

Our authors address the needs of CISOs and other cyber security professionals, and provide valuable information to a growing group of vendors and suppliers and clientele of the entire range of cyber risk management providers.

We always strive to be the best and most actionable set of resources for the CISO community in publishing Cyber Defense Magazine and broadening the activities of Cyber Defense Media Group.

Wishing you all success in your cybersecurity endeavors,

Yan Ross

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemagazine.com

SPONSORS

NIGHTDRAGON

*"**NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

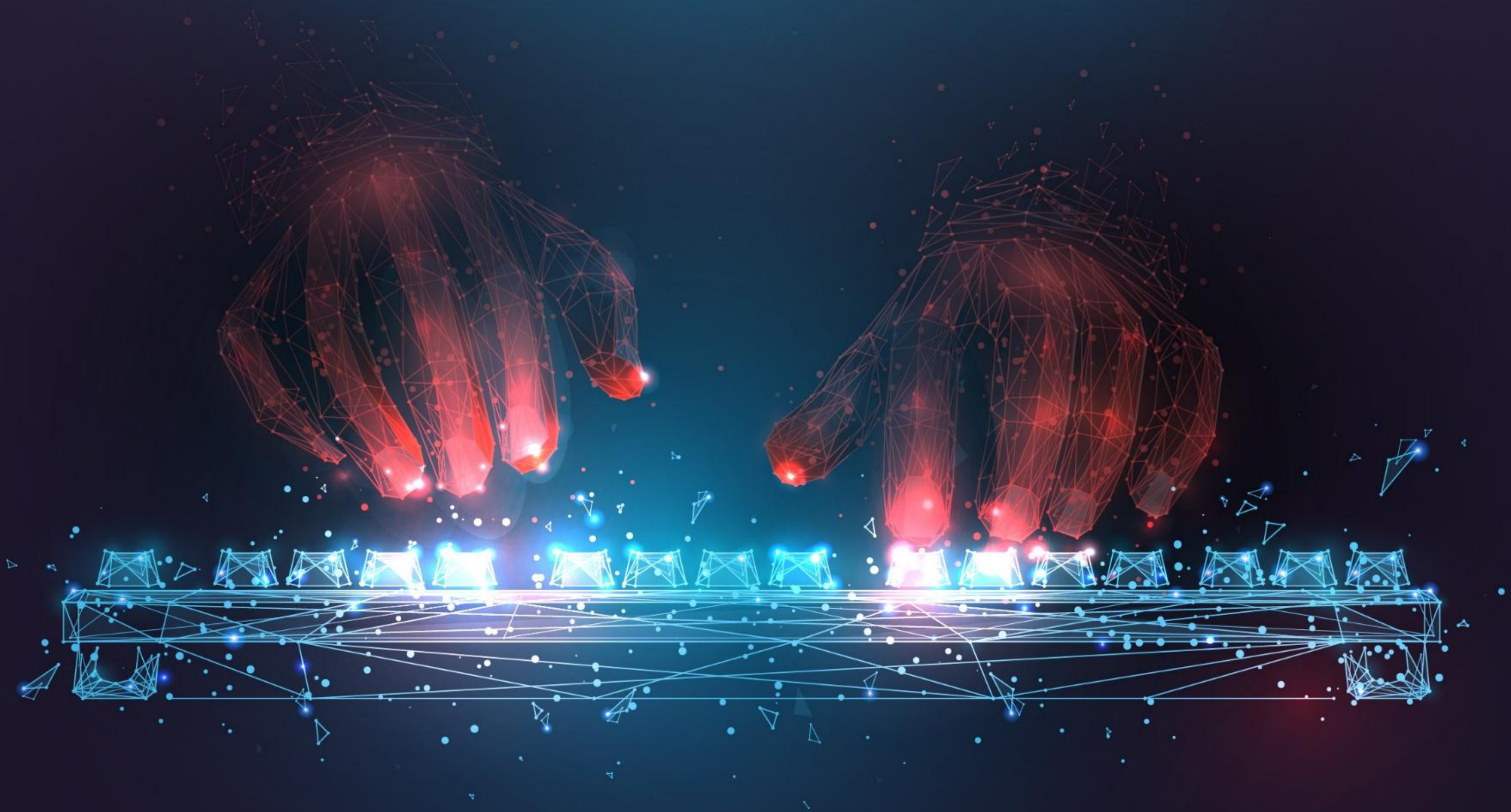
WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

Don't risk it, secure your data today.



Ransomware disproportionately impacts small and medium sized businesses. NSA's no-cost cybersecurity services can help protect DOD contractor networks from threats.

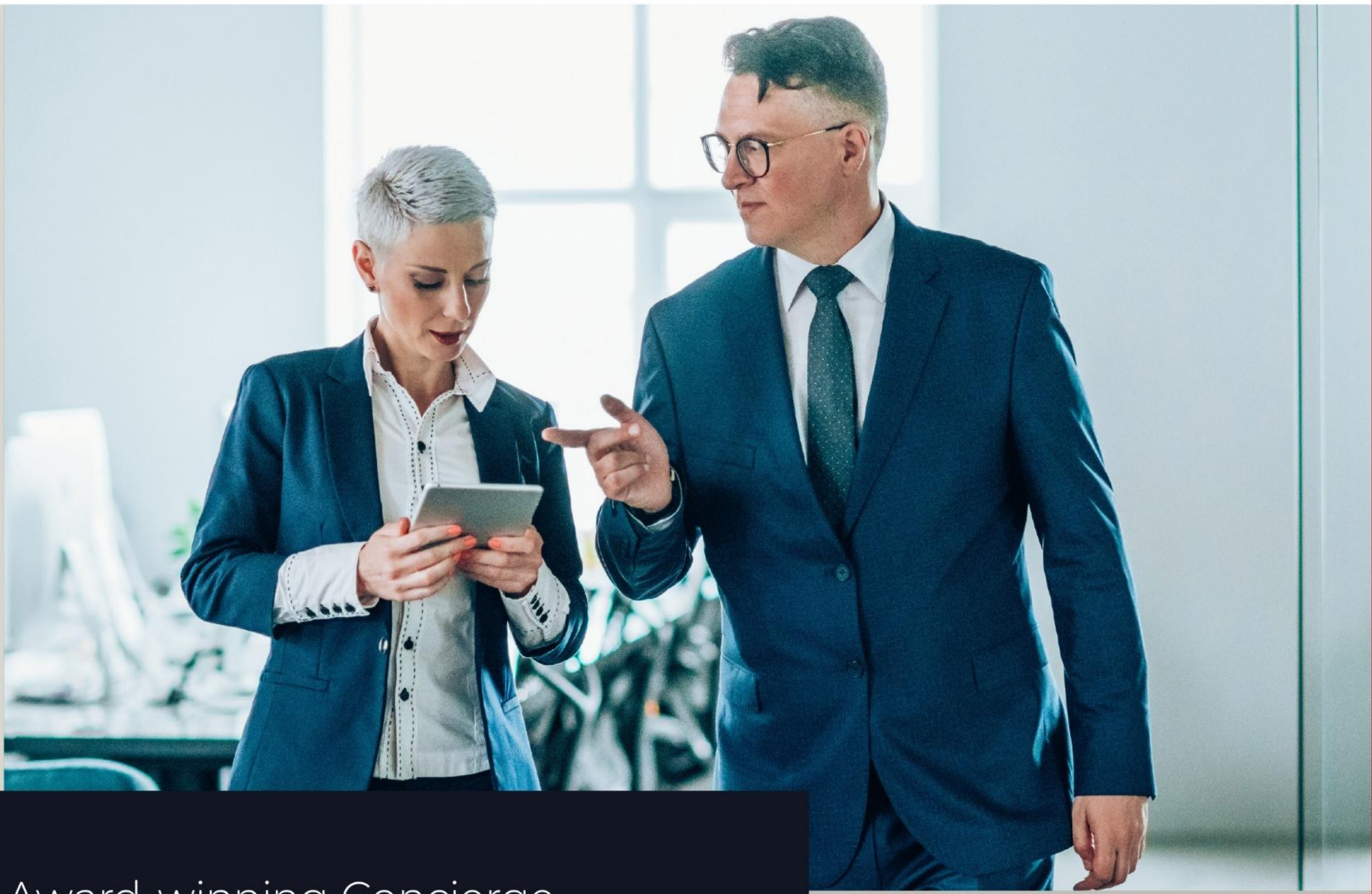
Available to any company with an active DOD contract or access to non-public DOD information.

GET STARTED TODAY

NSA.GOV/CCC

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

CYBERSECURITY COLLABORATION CENTER



CYE

Transform the way you manage cyber risk.

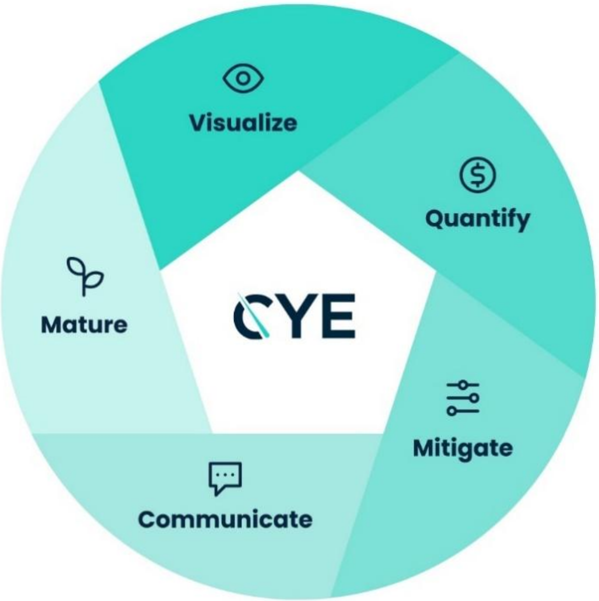
CYE's optimized cyber risk quantification solution enables you to:

Visualize

Predict probable attack routes by leveraging AI and data science with our SaaS platform.

Mature

Embrace transformation and unlock your organization's full potential with confidence.



Quantify

Determine the potential financial consequences of cyber risk in dollars, as well as the cost of remediation.

Communicate

Clarify and present your cyber risk in business terms to executives, security teams, and partners.

Mitigate

Focus your resources on addressing the most critical threats that truly pose risk to your business assets.

> "The investment in CYE's tools and services has helped us receive the financial support over the past couple of years that we didn't have several years ago."

John Padilla, Associate VP of IT SONICWALL

The Benefits of Working with CYE

96%

of customers' business-critical attack routes are blocked within six months

88%

Reduction in remediation time following a cyber incident.

87%

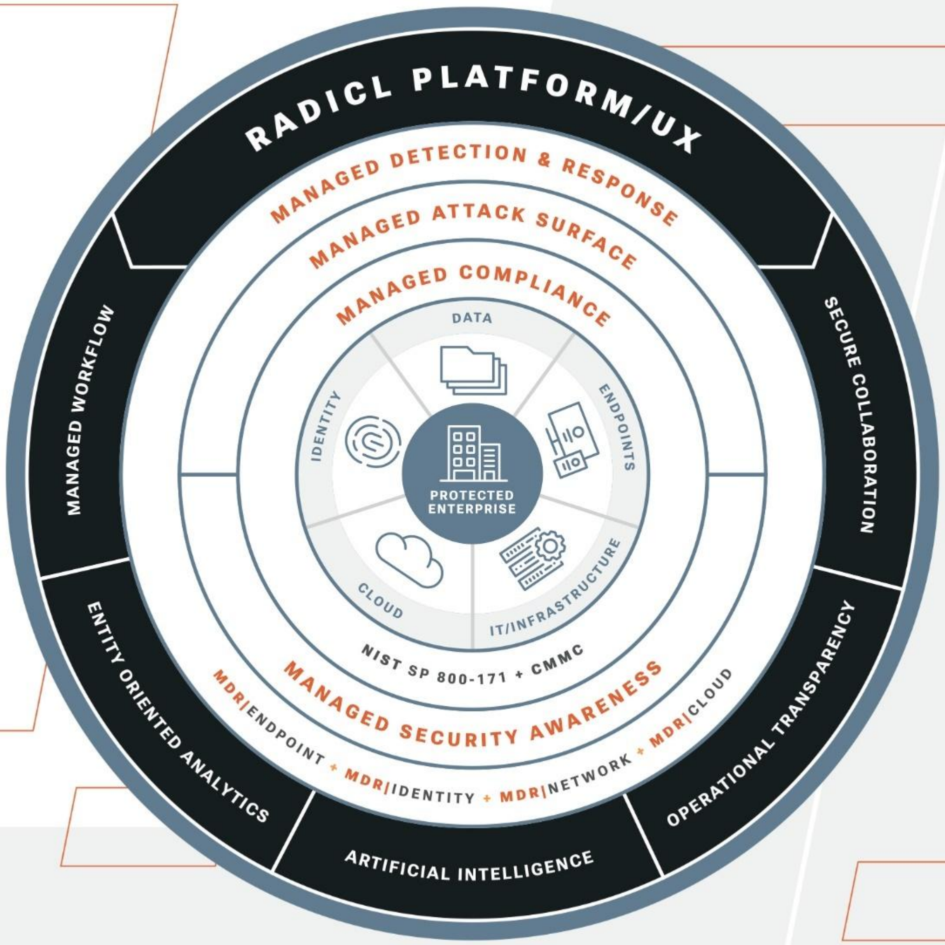
of customers improve ROI on their security budget.

Visit us at cyesec.com

RADICL™

We Protect American SMBs From Advanced Cyberthreats

If you want to maximally reduce your cyber incident risk, get RADICL!



- ✓ Endpoints Protected
- ✓ Identities Secured
- ✓ Vulnerabilities Reduced
- ✓ Incident Response 24 x 7
- ✓ CMMC / NIST 800-171 Assured

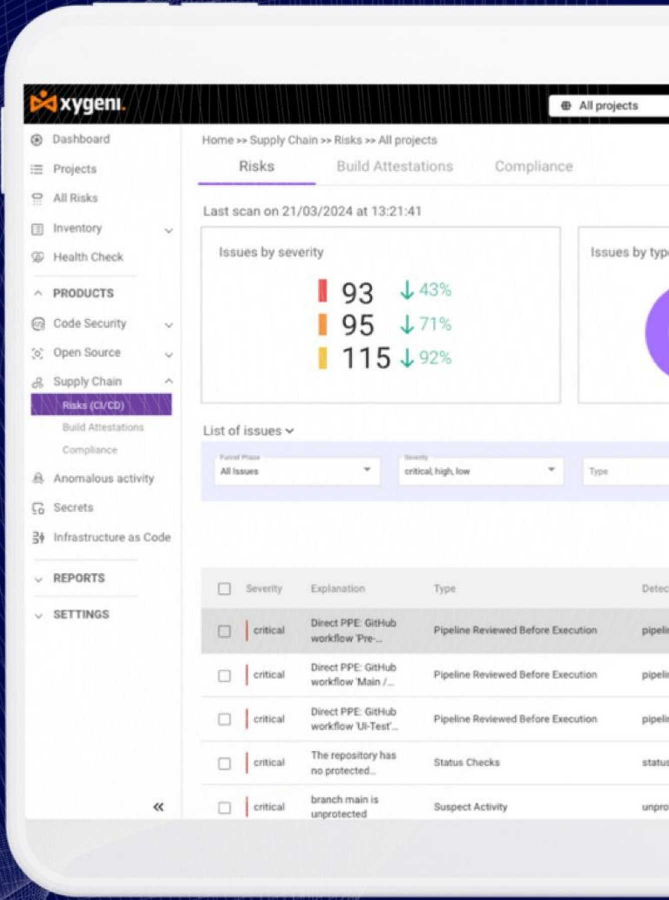
> "Companies developing, holding, or delivering technology, information or operations of interest to nation state cyberthreats are being actively targeted by extremely advanced threat actors. These companies make up America's Defense Industrial Base (DIB) and Critical Infrastructure (CI) and are under constant attack. For the sake of national security, they must be better protected. These same companies, along with others in verticals like finance, legal, and healthcare are also in the crosshairs of motivated and advanced cybercriminals. RADICL was born to bring these "high value target" companies a radically different class of cyberthreat protection - protection previously only available to the largest of enterprises and government entities. If you desire the best protection possible, we'd love to talk to you."

Chris Petersen, CEO of RADICL

GIVING SMBS LONG-OVERDUE ACCESS TO ENTERPRISE-GRADE CYBERSECURITY PROTECTION.

VPN
Tasks
Scenarios
Plugins
Assets
Reports
Task Schedule
On Demand
Start Time
11/29/2023 20:14:48
End Time
11/29/2023 21:48:16
Task Description
Estimated next execution time
Task Progress Information
# of jobs created
# of jobs completed
9250
9250
Action Type
Discover
Scan
Exploit
Score (Out of 100 scale,the higher score means more secure.)
20
Attack Surface %
Vulnerability %
Risks %
VUL Coverage %
HTTPS %
Active Assets %
95
# of Vulnerabilities
High
Medium
Low
Info
34
21
13
27
20%
Conversion Rate
Shell
Database
6%
2
Active Site
Total
Inactive
6
Execution Summary
1
Active IP
Total
Inactive
Execution Time: 01:33:27
Execution Progress: 9250/9250

WHEN MANAGING ASSET RISKS
PARTIAL VISIBILITY
IS JUST NOT GOOD ENOUGH.
WITH SEPIO, SEE ALL ASSETS. MANAGE ALL RISKS.
Learn more about Sepio's Asset Risk Management Platform >
www.sepiocyber.com



□	Severity	Explanation	Type	Detec
□	critical	Direct PPE: GitHub workflow 'Pre-...	Pipeline Reviewed Before Execution	pipeli
□	critical	Direct PPE: GitHub workflow 'Main /...	Pipeline Reviewed Before Execution	pipeli
□	critical	Direct PPE: GitHub workflow 'UI-Test'...	Pipeline Reviewed Before Execution	pipeli
□	critical	The repository has no protected...	Status Checks	status
□	critical	branch main is unprotected	Suspect Activity	unpro

THIRD-PARTY RISK MANAGEMENT

Modernize Your TPRM Program to Keep Up With Demand

Streamline Workflows and Maximize Your Team's Impact By Automating Steps So You Can Do More with Existing Resources

Simplify Monotonous Work So You Can Focus On Bigger Problems

TPRM teams spend countless hours on everyday tasks and burn through budgets and resources, leaving less time to focus on critical security concerns that will cause an impact.

Automate routine aspects of your program, from scoping your vendors to uncovering levels of inherent risk hiding in your portfolio. Turn elements of onboarding, ongoing monitoring, performance management, and even offboarding into a repeatable process to increase the volume of the third parties you focus on and free up more time to become a proactive protector of your organization.

Hands-Free Automation

Automate everything from assessment scoping to evidence collection with the click of a button. Run critical workflows in the background so that you can focus on impactful risk reduction.

Enterprise Integration

Seamlessly integrate with key enterprise systems such as Archer, MuleSoft, JIRA, Ariba, Archer and more through a robust web services-based API.

No-Code Configuration

Easily add features and functionality without relying on service engagements. Our platform is 100% configurable by the end user, meaning you don't have to wait weeks for the changes you need to meet program demands.

Reporting-as-a-Service

Provide stakeholders with the data that matters to them in seconds. Rapidly generate meaningful, board-ready reports that demonstrate the value of your program.

Implement Automation. Get Your Time Back.

Offload routine tasks to ProcessUnity to focus on TPRM work that matters.

- Sourcing – Automate the entire source to the onboarding lifecycle, simplifying RFx creation, supplier selection, and contracting.
- Onboarding – Streamline onboarding workflows, establishing a single, objective process for introducing new vendors to the business.
- Performance – Measure vendor performance against agreed upon SLAs and KPIs, track annual progress, and set threshold terms and alerts.
- Reporting – Generate dynamic reports and dashboards to get real-time visibility into the state of third-party risk.

ProcessUnity Third-Party Risk Management significantly reduces third-party onboarding and due diligence cycle times. Fueled by best-in-class workflow software, a universal data core for all TPRM information, the world's largest third-party risk exchange database and powerful artificial intelligence capabilities, ProcessUnity enables organizations to proactively mitigate first- and third-party risks.

ProcessUnity

Keep the Operation Running

TXOne Networks provides cybersecurity solutions that safeguard OT environments. Collaborating with top manufacturers and critical infrastructure operators, we develop practical, operations-friendly cyber defenses.

txone.com

MACH37®
CYBER ACCELERATOR

GET LAUNCHED

Our Mission

Today's real-time global connectivity has more complex threats and rapidly changing technology than ever before. In response, enterprise and consumer markets demand a steady stream of innovative new capabilities and solutions. MACH37 Cyber Accelerator® catalyzes the skills, foresight, and drive of the cyber industry's leading entrepreneurs, technologists, thought-leaders, and investors to anticipate that demand and accelerate the next generation of disruptive, high-growth cyber companies.

Our Program

Since 2013, MACH37® has operated in the heart of the cyber industry, just outside Washington D.C. in Northern Virginia. Our unique 90-day mentor-driven program leverages our workshops and expansive network of cyber experts from the public and private sectors to provide insights on how to build new cyber solutions and generate traction in the market. We emphasize the Lean Startup methodology and push technical founders out of the building so they develop and test their assumptions in a real world setting through brokered meetings with potential customers, channel partners, and investors. Using data collected from the market, we work with entrepreneurs to help them discover product-market-fit and hone their go-to-market strategy in a rapid time frame to build sustainable business models and drive growth.

MACH37® provides founding teams with extensive one-on-one mentorship from experts in entrepreneurship, strategy, public and private sector sales, marketing, product development, and venture capital investment. The advice from business and technical savvy mentors coupled with direct engagement with organizations facing cyber-related issues creates valuable connections that help founders prime a market for early product adoption. We give cyber startups a competitive advantage to attract seed-stage and Series A investors and become the next generation of leading cyber companies.

500-600
startups from around the world screened per year

450+ mentors world-wide

91 companies launched

84% of graduates are still in business

64% of graduates have raised follow-on investment post-Demo Day

$1M average seed round

hello@venturescope.com
www.venturescope.com
@venturescope

VentureScope®

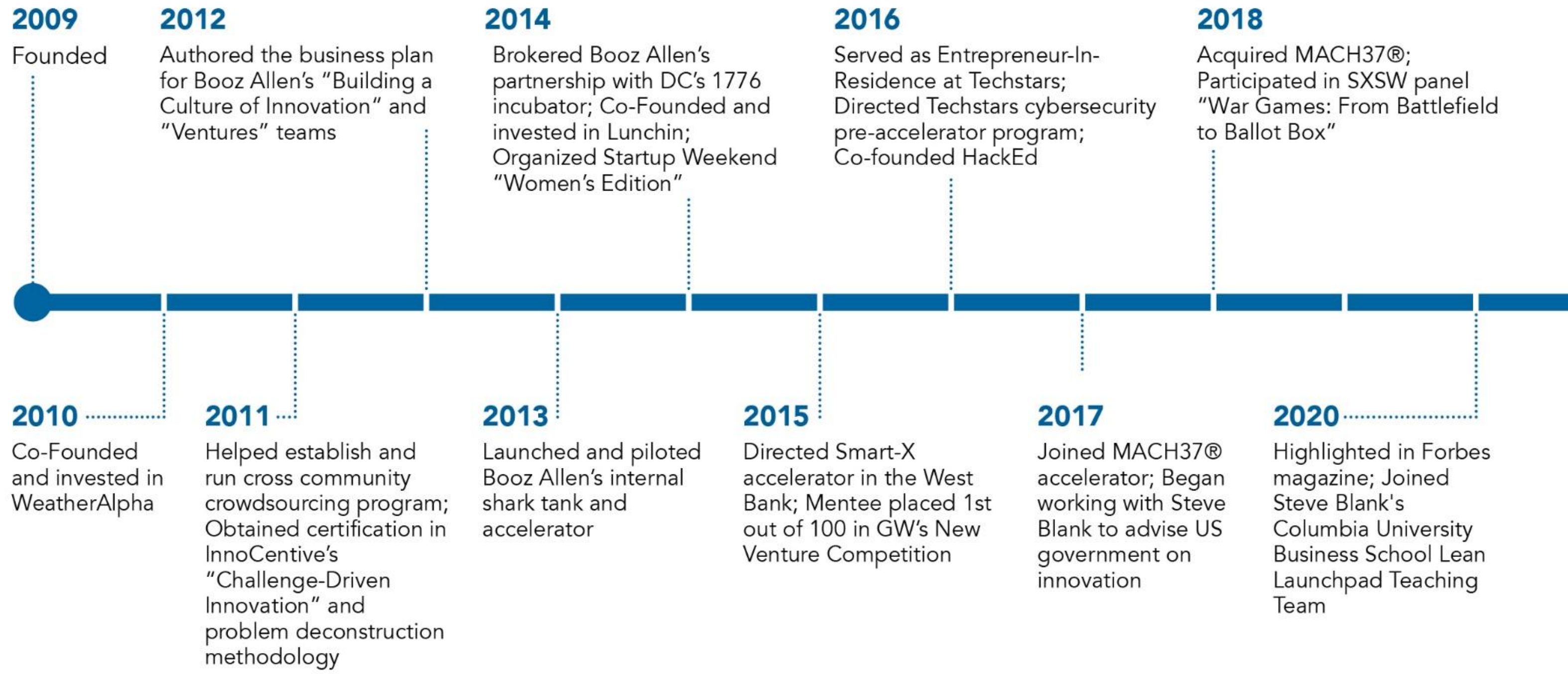
STRATEGY · DEEP TECH · INVESTMENT

VentureScope® works with creative entrepreneurs, venture capital investors, and large private and public sector organizations around the world that are trying to solve interesting problems. Our team specializes in problem deconstruction and framing, product development, business model refinement, go-to-market strategies, build-buy-partner decisions, strategic partnerships, investment and growth analysis, and a variety of innovation methodologies. Whether you're a budding entrepreneur, a scrappy startup, an experienced investor, or an established organization developing a new service or capability, we will not only advise you on what to do, but work as part of your team to apply our recommendations.

Our team has over 60 years of combined experience launching new business ventures, investing in promising startups, running startup accelerators, teaching and providing strategic innovation and general management consulting services to large private and public sector organizations. We own and operate the MACH37 Cyber Accelerator®. We're on the pulse of emerging and over-the-horizon technology, and are tracking their growth and development against important industry problems to inform our dealflow and give you exceptional advice.

Expertise

LEAN STARTUP METHODOLOGY
BUSINESS MODEL STRATEGY
PROBLEM DECONSTRUCTION & FRAMING
PRODUCT DEVELOPMENT
GO-TO-MARKET STRATEGY
REVENUE GENERATION
TECHNOLOGY SCOUTING & INVESTMENT DEALFLOW
BUILD-BUY-PARTNER DECISIONS
INVESTMENT & GROWTH ANALYSIS
STRATEGIC PARTNERSHIPS
CHALLENGE-DRIVEN & OPEN INNOVATION
INNOVATION PIPELINE DESIGN & IMPLEMENTATION
CREATIVITY & STRATEGIC FACILITATION
INSTRUCTIONAL DESIGN & EXPERIENTIAL TRAINING
HUMAN PERFORMANCE



2009
Founded

2010
Co-Founded and invested in WeatherAlpha

2011
Helped establish and run cross community crowdsourcing program; Obtained certification in InnoCentive's "Challenge-Driven Innovation" and problem deconstruction methodology

2012
Authored the business plan for Booz Allen's "Building a Culture of Innovation" and "Ventures" teams

2013
Launched and piloted Booz Allen's internal shark tank and accelerator

2014
Brokered Booz Allen's partnership with DC's 1776 incubator; Co-Founded and invested in Lunchin; Organized Startup Weekend "Women's Edition"

2015
Directed Smart-X accelerator in the West Bank; Mentee placed 1st out of 100 in GW's New Venture Competition

2016
Served as Entrepreneur-In-Residence at Techstars; Directed Techstars cybersecurity pre-accelerator program; Co-founded HackEd

2017
Joined MACH37® accelerator; Began working with Steve Blank to advise US government on innovation

2018
Acquired MACH37®; Participated in SXSW panel "War Games: From Battlefield to Ballot Box"

2020
Highlighted in Forbes magazine; Joined Steve Blank's Columbia University Business School Lean Launchpad Teaching Team

Altitude Cyber

"Built on passion and expertise, Altitude Cyber delivers strategic advisory services specifically tailored for founders, investors, startups, and their boards. Our unique approach fuses strategic insight with financial acumen to help your company soar to new heights."

Dino Boukouris

Managing Partner, Altitude Cyber

Guiding cybersecurity businesses globally through every stage of growth with tailored advisory services for founders, CEOs, investors, and boards.

Founders & CEOs

Altitude is your trusted advisor throughout your entrepreneurial journey. We guide you as you grow your business, navigate fundraising processes, construct advisory boards, plan your long-term exit strategy, develop strategic relationships with key partners and investors, and more.

Investors

We offer a range of strategic advisory services to support your existing portfolio companies, as well as your potential investments or acquisition targets. Our solutions are tailored to fit your needs, with flexible engagement models that align incentives to maximize outcomes.

Boards

We provide in-depth strategic advisory services, tailored to align with the evolving needs of growing businesses. Our support includes strategic business and corporate development, mergers & acquisitions, corporate finance, long term exit planning, advisor selection, and more.

Firm Highlights

Decades of experience as world class operators and advisors

Highly curated research and thought leadership on strategic activity in the cyber market

Deep industry relationships and partnerships across strategic and financial partners

Cyber Network

15,000+	Cyber Executives
3,000+	Investors
1,000+	CISOs

Cyber Knowledge

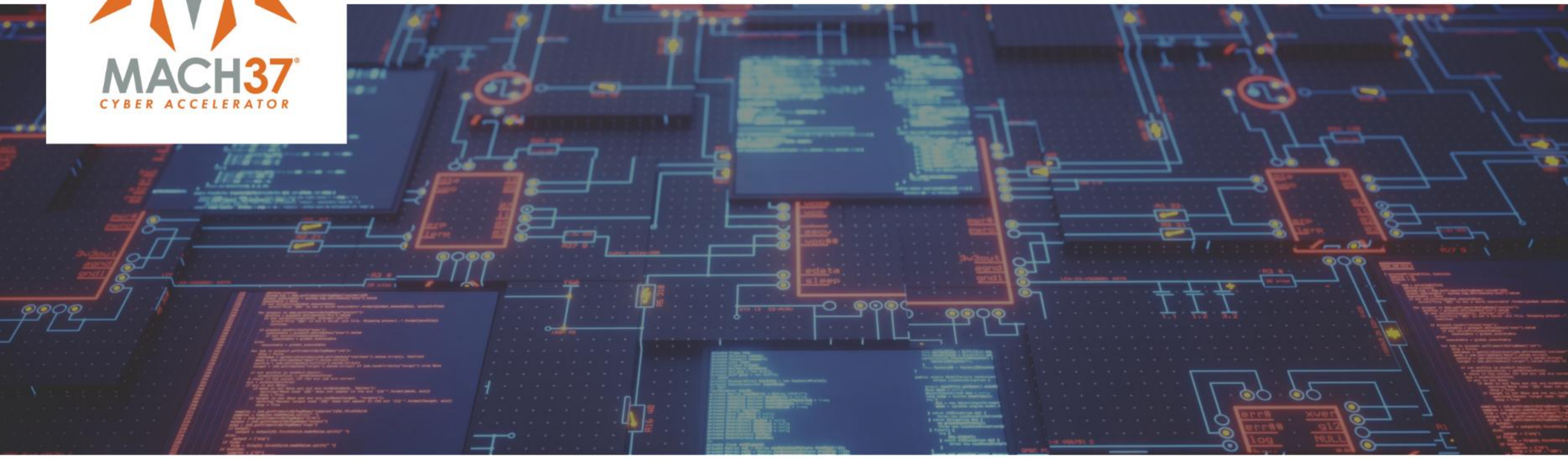
4,500+	Company Tracker
3,000+	M&A Transactions
8,500+	Financing Transactions

Extensive, global relationships with cyber executives, investors, CISOs, policy influencers, and service providers

Altitude Cyber, LLC | www.altitudecyber.com

For inquiries or further information please contact Altitude Cyber at: **dino@altitudecyber.com**

MACH37
CYBER ACCELERATOR



Our Industry Focus

- Cybersecurity
- Artificial Intelligence
- Machine Learning
- Space/Aerospace
- Quantum Computing
- Cyber Physical Systems
- Internet-of-Things
- Industrial Control Systems
- Neural Networks

Our Executive Team

Jason Chen	CEO & Executive Director	jason@venturescope.com
Jennifer Quarrie	COO, CWO & Strategy Director	jennifer@venturescope.com

Notable Alumni

RunSafe SECURITY

SylLab Systems

HUNTRESS

breachbits

HYPERQUBE

ATOMICORP

VIRGIL SECURITY

SYNCURITY Built by Analysts, For Analysts

MACH37 CYBER ACCELERATOR

hello@venturescope.com | www.mach37.com | @MACH37cyber

GAN ACCELERATOR

VentureScope® STRATEGY · DEEP TECH · INVESTMENT

Optery FOR BUSINESS

PC EDITORS' CHOICE PCMAG.COM 2022, 2023, 2024

Remove your employees' personal data from the internet

- Prevent phishing & other social engineering attacks
- Reduce identity theft & fraud
- Protect your team from malicious actors
- Safeguard against real world harassment

AS SEEN ON

SXSW · SECURITYWEEK · CR Consumer Reports · PC PCMAG.COM · TC · CNET · ZDNet · SC MEDIA

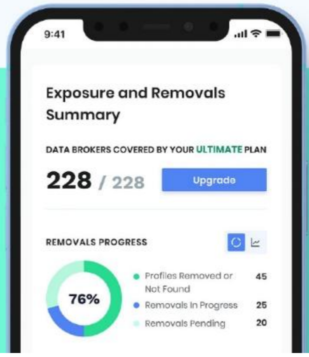
Why Optery for Business?

We're exclusively focused on data broker removal so you get the privacy & protection you need.

- ✓ Patented Search Technology
- ✓ Transparent Exposure & Removal Reporting
- ✓ No Affiliations with Data Brokers
- ✓ Clear, Affordable & Flexible Pricing
- ✓ Monthly Automated Scans & Removals
- ✓ Comprehensive Data Removal From Hundreds of Sites
- ✓ SSO/SCIM/SAML Integration Options
- ✓ SOC 2 Type 2 Certified

Create your free business account

business.optery.com/signup



9:41

Exposure and Removals Summary

DATA BROKERS COVERED BY YOUR ULTIMATE PLAN

228 / 228

REMOVALS PROGRESS

● Profiles Removed or Not Found	45
● Removals In Progress	25
● Removals Pending	20

CYBER DEFENSE
MAGAZINE
You can't see
your threats
from the ground.
Get a 40k foot view
for free...
by reading
Cyber Defense Magazine

RSAConference™2025

San Francisco | April 28 – May 1 | Moscone Center

Many Voices.
One Community.

Together we secure.

Join us at RSA Conference 2025!

Cybersecurity's greatest challenges demand more than one perspective. That's why RSAC 2025 unites thousands of voices from around the world to collaborate, innovate, and secure our digital future.

From April 28 – May 1 you'll hear groundbreaking Keynotes, explore hands-on sessions, and participate in exclusive networking opportunities. This is where the global cybersecurity community connects to share insights and find solutions.

Why Attend?

- Hear from top experts tackling today's toughest challenges in cybersecurity.
- Experience cutting-edge solutions at the Expo that will drive your strategies forward.
- Collaborate with peers to unlock innovative solutions and gain fresh perspectives.
- Expand your network with professionals from every corner of the globe, forging connections that last a lifetime.

Be a part of something bigger. RSAC 2025: **Many Voices. One Community.**

Register now at RSAConference.com/cyberdefense25

#RSAC

ARTICLES

AI and Elections

The Case for a Unified Federal Approach in the United States

By Shivani Shukla, Associate Dean of Business Analytics and Professor of Analytics, University of San Francisco

Artificial intelligence (AI) technologies are transforming U.S. elections, creating new opportunities as well as critical security challenges. AI's capabilities to predict voter behavior, automate campaign strategies, and even generate political communications are advancing rapidly. At the same time, the integrity of democratic processes is now at imminent risk due to AI's encroachment. As believable deepfakes, cyberattacks, and data manipulation become more prevalent, relying on technology in the voting process demands stronger precautions and defenses. Establishing a unified cybersecurity framework will help safeguard elections, protect voter data, and uphold democratic rights in the face of these evolving AI-driven threats.

AI and U.S. elections

A growing number of states are implementing or considering laws to regulate generative AI in political campaigns to address the risks of AI's potential to mislead or suppress voters. Research shows a patchwork of state-specific rules, with 19 states already enacting laws against AI-generated deepfakes or synthetic media in elections. Early incidents, including AI-generated impersonations of political figures, have heightened concerns about the misuse of generative AI.

Laws in some states mandate disclosure of AI-generated content, while others allow legal recourse for affected candidates. These efforts vary widely, as some states provide exemptions for satire or parody and differ on whether violations are criminal offenses. Experts argue that federal action and a comprehensive framework are necessary, as state-level regulations alone cannot fully safeguard elections from evolving AI threats.

In November 2024, the Biden administration announced its support of a United Nations cybercrime treaty. The treaty's key provisions aim to enhance international cooperation in preventing and combatting cybercrime through a common framework. Its measures include consistent definitions for cybercrime offenses, structured guidelines for law enforcement actions, and collaboration among member states. This effort supports the global unification of standards in cybersecurity.

Cybersecurity threats posed by AI

As AI models rapidly advance in analyzing complex information and generating highly believable content, their integration into elections introduces benefits and challenges. AI can be weaponized for launching believable cyberattacks, but also can be leveraged to defend against them—making it AI versus AI. AI-driven cyberattacks can disrupt voting and target critical electoral infrastructure. For instance, attackers could employ AI to orchestrate fake 911 calls, diverting emergency resources and creating openings for physical attacks on polling stations. Additionally, AI-enabled "data poisoning" involves introducing misleading information into training data, which can degrade the effectiveness of AI systems designed to secure electoral campaigns and processes.

States with weaker cybersecurity defenses are especially vulnerable. With security efforts technologically unsophisticated and fragmented across states, those lacking robust protections experience heightened data manipulation risks or attacks on voting systems.

The lack of a unified federal cybersecurity framework

The fragmented approach to election cybersecurity in the United States is a crucial vulnerability. While the Cybersecurity and Infrastructure Security Agency (CISA) provides some guidance and resources, implementation varies widely across states, leading to inconsistent protections. This state-by-state disparity results in security gaps, leaving voters in some regions more exposed to risks.

CISA outlines a cybersecurity toolkit and other resources to protect elections. To address election security, three primary categories of cyberthreats—phishing, ransomware, and distributed denial of service (DDoS) attacks—require distinct steps for understanding, protection, and detection. Phishing attacks involve cyber actors using emails, texts, and websites to deceive election officials into disclosing information or installing malware. Ransomware locks or steals data, and DDoS attacks overwhelm servers and hinder access to voting information.

This toolkit, while effective, doesn't yet account for the added layer of complication that the inclusion of AI in election activities would present. A unified effort toward security could foster collaborative efforts between federal and state agencies, enhancing collective resilience against AI-driven threats. One potential solution is to integrate cybersecurity into the AI tech stack to embed inherent protection mechanisms, which could provide a protective layer even in the face of delays in the implementation of regulations for AI development and usage.

Designing a unified federal cybersecurity framework

A unified federal cybersecurity framework ensures that AI technologies are resilient, compliant, and resistant to misuse by building safeguards directly into the development environment. Here are the summarized recommendations:

Engage in data security and privacy protection

- Data encryption, anonymization, and storage protocols. Use strong encryption standards for data at rest and transport layer security/security sockets layer (TLS/SSL) protocols for data in transit. Implement critical management systems for secure encryption key handling. Apply data anonymization techniques (e.g., k-anonymity, synthetic data) during preprocessing. Secure storage with encrypted cloud solutions and role-based access controls; ensure off-site backup storage for ransomware protection.
- Privacy by design. Integrate privacy protocols early in development through automated checks in continuous integration and continuous delivery (CI/CD) pipelines and follow privacy frameworks, ensuring compliance with regulatory guidelines.
- Detect poisoned data. Automate data validation scripts to detect anomalies and outliers. Use data-filtering tools to manage noisy data before training. Employ models to cross-check for poisoning attempts by comparing predictions.

Ensure model integrity and a defense against cyberattacks

- Adversarial training and testing. Generate adversarial examples during training to improve resilience. This is particularly consequential in the case of deepfakes. Use libraries that provide automated robustness checks against adversarial attacks.
- Robustness testing. Conduct tests to verify model explainability and robustness under stress. Simulate attacks using principles of resilience testing to identify vulnerabilities.

Secure AI development and a deployment environment

- DevSecOps for AI. Automate security checks within CI/CD pipelines to identify vulnerabilities early. Perform regular scans on dependencies to reduce risk from third-party libraries.

- Containerization and isolation. Use containers with built-in security modules to enforce isolation. Deploy applications with strict security policies to ensure isolated environments.
- Role-based access control and monitoring. Implement secure authentication and fine-grained access controls. Set up real-time monitoring systems for ongoing security oversight. Log and audit activities to ensure traceability of access and actions.
- Cloud security with zero-trust architecture. Enforce identity verification through multifactor authentication. Use micro-segmentation to limit access to sensitive data across users and tenants.

Implement a governance and compliance model

- Governance framework. Define governance policies aligned with industry security and compliance standards. Implement model risk management processes to maintain consistent compliance.
- Version control and auditability. Use version-controlled repositories for model tracking and transparency. Automate audit processes to facilitate accountability and traceability.

Develop a threat detection and incident response plan

- AI threat monitoring. Integrate threat detection models within deployed applications for continuous monitoring. Use intrusion detection systems o provide real-time alerts on unusual behavior.
- Incident response plan. Establish a structured response playbook specifying roles, responsibilities, and communication. Conduct regular exercises to prepare teams for cybersecurity incidents.

This approach unifies election security by embedding cybersecurity and AI protections across data handling, model integrity, and deployment. It targets key threats, including phishing, ransomware, DDoS, and integrates proactive AI-specific safeguards, such as adversarial training and zero-trust architecture. A collaborative federal framework enables shared governance and compliance, aligning federal and state efforts. Continuous threat monitoring and structured incident responses ensure preparedness against evolving attacks.

Building ethical AI systems in the presence of open-source models

Even with the presence of these built-in technology safeguards, no system would be devoid of vulnerabilities. The prolific open-source development within AI has paved way for their performance to be on par with the more established models including those by Open AI, Google, and Microsoft. Integrating security measures into a tech stack of open-source models will be challenging. Ethical considerations and technical measures are crucial to ensuring the responsible use of AI in elections. Further complicating the matter is that every individual and institution will have their own interpretation and application of ethical standards.

Benefits of a unified approach

A unified federal approach offers a range of benefits to states and voters. For example, it would standardize protections across all states to close the current gaps in electoral campaigning and security. Additionally, a unified framework will strengthen electoral infrastructure resilience and ensure that every citizen’s vote is equally secure, irrespective of their state. Ultimately, implementing standardized cybersecurity practices within the tech stack can enhance voter data protection, provide more robust AI safeguards, and increase public confidence in the electoral process.

A comprehensive framework will facilitate collaboration between private sector stakeholders, state governments, and federal agencies. Moreover, it can enable the swift identification and mitigation of emergent threats, guaranteeing that the nation’s infrastructure can adjust to new obstacles as they emerge.

About the Author

Shivani Shukla is the Associate Dean of Business Analytics and Professor of Analytics at the University of San Francisco. She specializes in operations research, statistics, and AI, with several years of experience in academic and industry research. Shivani can be reached on LinkedIn.

The SME Cybersecurity Paradox: Why Smaller Businesses Are Prime Targets

Simon Hughes, Senior Vice President of Global Distribution at Cowbell, breaks down the growing cybersecurity risks facing SMEs in the U.S. and challenges the misconception that smaller businesses are less appealing to hackers.

By Simon Hughes, SVP, Global Distribution & General Manager UK, Cowbell Cyber

The latest statistics on business size and cyber risk seem clear enough—larger businesses, especially those with revenues exceeding $50 million, experience cyber incidents 2.5 times more frequently than other enterprises.

It makes sense: the larger the business, the more valuable the data assets, and the more complex the IT infrastructures—meaning more potential entry points for attackers. The higher public profile of larger companies can also make them targets for reputation-damaging attacks.

While all of the above is true, this does not mean that small and medium-sized enterprises (SMEs) are flying under the radar when it comes to cyber threats—contrary to what many may believe.

In fact, SMEs are becoming increasingly prime targets for cybercriminals for a number of reasons. Firstly, despite their size, these businesses often hold valuable customer data. Take SMEs within public administration and educational services, for example. Operating as small, specialized entities providing services to schools, government departments, or local communities, they can hold highly valuable customer data such as personally identifiable information (PII), financial details, health information, or user behavior data.

Smaller firms also typically struggle with budget constraints that often lead to outdated IT infrastructure and weak security measures, which make them easier prey. The fact we're currently seeing a rise in attacks on educational institutions—up 70% from three years ago—shows just how vulnerable underprepared sectors can be.

Another point to consider is the fact that SMEs are often part of larger supply chains, creating a weak link that hackers can exploit to access larger, more prominent organizations. This correlates with a huge rise in supply chain attacks, which have grown more than five times (431%) between 2021 and 2023, with further growth projected in 2025. Exploiting the trust between interconnected organizations and their vendors or suppliers, these attacks can potentially compromise multiple entities through a single breach, including all the smaller companies in the chain.

Finally, it's worth noting that while smaller firms may face a lower frequency of attacks overall, the consequences of a single incident can be devastating without the resources and resilience of a larger firm, including significant financial losses, crippling downtime, business interruption, and in some cases, even closure.

Common SME cybersecurity mistakes and how to address them

With the above in mind, it's more important than ever to identify the cybersecurity mistakes SMEs typically make and for small business owners to understand that their size doesn't make them invisible to attackers. Among the most common mistakes are skipping software updates, overlooking employee training—giving rise to human error, one of the most significant vulnerabilities in any organization's defenses—and underestimating the sophistication of today's threats.

While each sector faces unique challenges and vulnerabilities that require tailored approaches to cyber risk management, consider the following measures to significantly improve a small business's security posture:

- **Conduct regular, comprehensive cyber risk assessments:** Assessments should be tailored to your industry's specific threats and vulnerabilities and involve identifying critical assets and data, evaluating existing security controls, assessing threats and vulnerabilities, determining potential incident impacts, and prioritizing risks based on their likelihood and potential consequences. Tools like Cowbell Factors can also offer valuable benchmarks against peers, helping identify areas where your organization excels or needs improvement.

- **Don't underestimate the value of cybersecurity training for employees:** To address human error, training should be ongoing, role-specific, and tailored to the unique threats employees may encounter. Phishing awareness, particularly important for small businesses, should be a central focus. Effective programs should cover recognizing (and reporting) phishing attempts—especially difficult with recent advances in AI—safe browsing and email practices, handling sensitive data securely, password security, multi-factor authentication (MFA), social engineering awareness, and secure remote work practices.

- **Strengthen incident response and backup systems:** Together, these measures ensure organizations can recover quickly and minimize disruption in the event of a cyber incident. A robust incident response plan should define clear steps, roles, and responsibilities during an attack, along with procedures for containing and mitigating impacts, preserving evidence for legal purposes, and conducting post-incident analysis to improve future responses. Equally important are comprehensive backup systems, which must be regular, automated, and securely stored offline or in segmented networks to protect against ransomware.

- **Improve due diligence across the supply chain:** To counter the rise in supply chain attacks, SMEs must vet third-party vendors, regularly audit key suppliers, and develop a robust third-party risk management program.

- **Manage technology risks by addressing the most vulnerable systems:** SME leaders should establish a comprehensive patch management strategy to ensure all operating systems and server-side technologies are consistently updated with the latest security fixes. Additionally, for content management and collaboration platforms, it's essential to implement strict access controls, use encryption, and regularly perform security audits to safeguard against potential threats.

When considering the above, remember that cybersecurity is not a one-time effort—it needs to be treated as an ongoing process that receives continuous attention and adaptation to new threats.

A necessity, not an option

The SME segment represents over 99% of all businesses and 44% of the American GDP, yet SMEs are one of the most underserved segments of the American economy when it comes to cybersecurity. However, simply by implementing the above tips, business leaders can significantly enhance cyber resilience.

With cyberattacks on the rise, safeguarding digital assets isn't just an option anymore—it's a necessity for the survival and future growth of SMEs.

About the Author

Simon Hughes is Cowbell's SVP, Global Distribution & General Manager UK. Simon is a seasoned underwriter with over 13 years of experience in the insurance industry. He began his career at Lloyd's and has since gained valuable experience with the multi-national reinsurer SOVAG and CFC Underwriting, a UK-based specialty insurer. At CFC, Simon was a member of the cyber team for six years, serving as a cyber underwriter and senior leader focusing on small to medium-sized enterprises. Simon helped build the UK and EU cyber underwriting teams to achieve market-leading and profitable growth in a rapidly developing market. He is a proven leader with a deep understanding of cyber risk and insurance and has been instrumental in driving success in all his previous roles. Simon can be reached online at LinkedIn and at our company website https://cowbell.insure/.

Ten Cloud-Agnostic Cybersecurity Tips for Protecting Your Data Across Platforms

By Hooman Mohajeri, Vice President of Security Services at BlueAlly

When it comes to rapidly scaling operational processing power and expanding digital storage, cloud platform solutions are unmatched. Offering unparalleled flexibility, cloud platforms have quickly become essential for businesses of all sizes. However, as with any technological innovation, the cloud introduces a range of complex security risks that organizations must carefully navigate.

While most enterprises rely on cloud services from providers like AWS, Azure and GCP, implementing strong internal security measures is a key requirement for maintaining regulatory compliance. These protections are essential not only for safeguarding customer data but also for preserving consumer trust, employee confidence, competitive advantage and brand reputation.

By adopting cloud-agnostic data security strategies, organizations can ensure comprehensive protection across various platforms, independent of specific providers. The following strategies align with best practices recommended by leading cloud experts. Concepts such as Zero Trust— which mandates continuous verification of every user, device, and transaction regardless of network—illustrate how companies can enhance their cloud security posture.

1. Identity and Access Management (IAM)

Effective identity and access management (IAM) is critical for securing cloud environments. IAM enables organizations to control who has access to resources, what they can do and under what conditions. By minimizing unauthorized access to sensitive data, organizations can drastically reduce security risks.

Best Practices:

- Implement the principle of least privilege, granting only the minimum permissions necessary for each user or service.
- Enforce multi-factor authentication (MFA) for all user accounts.
- Rotate static access credentials regularly and avoid embedding credentials in code.
- Adopt a Zero Trust approach to identity: verify every access attempt, regardless of source or location.
- Leverage just-in-time (JIT) access and privileged access management (PAM) solutions to grant permissions only when and where they are needed.
- Implement attribute-based access control (ABAC) where possible to enable dynamic, context-aware permissions based on user attributes, resource properties, and environmental conditions—providing more flexible and granular access management than traditional role-based approaches while reducing administrative overhead and security risks.

2. Data Encryption and Protection

Encryption is essential for protecting sensitive data, ensuring that it remains confidential even if compromised. Encrypting both data at rest and in transit minimizes the risk of unauthorized access and data leaks in the cloud.

Best Practices:

- Enable encryption by default for all data, both at rest and in transit.
- Implement secure key management with automated rotation and lifecycle management.
- Use automation to ensure all network traffic is encrypted (e.g., enforcing Transport Layer Security (TLS) for all connections).
- Implement automated scanning and remediation for unencrypted data stores or improperly configured encryption settings.
- Employ data loss prevention (DLP) tools to prevent unauthorized data exfiltration.

3. Network Security and Zero Trust

Securing an organization’s network traffic is fundamental to protecting its cloud assets from unauthorized access and external threats. Adopting a Zero Trust model ensures that all network transactions are continuously verified, significantly reducing the chances of a security breach.

Best Practices:

- Implement network segmentation and micro-segmentation to isolate workloads and reduce the blast radius.
- Configure strict ingress and egress firewall rules based on least privilege principles.
- Secure connections using encrypted communication channels.
- Implement micro-segmentation by dividing networks into isolated zones at the workload level, enforcing application-aware policies that control all communication between segments based on verified identity, context, and behavior—while continuously monitoring east-west traffic patterns to maintain Zero Trust principles across the environment.
- Implement software-defined perimeters (SDP) to create dynamic, identity-centric network boundaries.

4. Continuous Monitoring and Logging

Routine monitoring and logging are essential for detecting security incidents and misconfigurations in dynamic cloud environments. Without comprehensive monitoring, it is difficult to identify threats before they escalate. Consistent logging also provides critical data for audits and compliance.

Best Practices:

- Implement centralized logging and monitoring across all services.
- Set up alerts for specific security events, such as:
- Unauthorized access attempts or successful logins from unusual locations.
- Changes to IAM policies or security group configurations.
- Unusual application programming interface (API) calls or high volumes of data transfer.
- Creation or modification of privileged accounts.
- Encryption failures or disabling of security controls.
- Secure logs against tampering and ensure authorized access only.
- Implement automated response systems for immediate action on critical security incidents.

5. Security Automation and DevSecOps

Automating security in cloud environments helps ensure consistent, scalable protection by reducing human error and enforcing security best practices. DevSecOps embeds security controls directly into the CI/CD pipeline, making protection an integral part of the development lifecycle.

Best Practices:

- Automate security patching and vulnerability management.
- Use Infrastructure as Code (IaC) to deploy secure configurations.
- Implement automated incident response workflows.
- Integrate security into the CI/CD pipeline (DevSecOps), including static, dynamic and software composition analysis tools to detect vulnerabilities early in the development process.
- Employ automated compliance checks to ensure configurations meet security standards and configuration drift is detected in a timely manner.

6. Resilience, Backup, and Disaster Recovery

Building resilience through backups and disaster recovery planning is crucial for mitigating security failures. Even with the best security measures in place, incidents can still occur. Having a robust recovery plan ensures that your organization can swiftly restore operations.

Best Practices:

- Implement automatic, geographically diverse backups.
- Encrypt backups and regularly test restoration procedures.
- Develop and regularly update a comprehensive disaster recovery plan.
- Implement redundancy and failover mechanisms for critical systems.
- Conduct regular disaster recovery drills to ensure preparedness.

7. Compliance and Governance

Strong governance and regulatory compliance are non-negotiable in many industries. Organizations must ensure that their cloud environments meet industry standards and legal requirements while implementing governance frameworks that continuously monitor compliance and scale with the environment.

Best Practices:

- Utilize compliance monitoring tools aligned with relevant standards (e.g., GDPR, HIPAA, SOC 2, ISO 27001, FedRAMP, etc.).
- Regularly audit and update security policies.
- Implement automated compliance checks and reporting to maintain continuous compliance.

8. AI and Machine Learning (AI/ML) Security

As AI/ML becomes more widespread, securing AI workloads and data is increasingly important. Safeguarding these assets is vital for preventing malicious activity and ensuring the reliability of AI-driven operations.

Best Practices:

- Implement strict access controls for AI/ML models and training data.
- Use anonymization techniques, when possible, to protect sensitive data used in AI training.
- Monitor AI systems for potential bias or unexpected behavior.
- Update and patch AI/ML frameworks and libraries regularly.

9. Container and Serverless Security

Securing containers and serverless functions is essential as organizations increasingly adopt these architectures. These resources operate in environments that require specialized security considerations, particularly around runtime protection and monitoring.

Best Practices:

- Enforce runtime security for containers and serverless functions.
- Deploy trusted base images and regularly scan for vulnerabilities.
- Apply the principle of least privilege to container orchestration platforms.
- Implement function-level monitoring and logging for serverless applications.

10. Third-Party Risk Management

Managing third-party risk is critical in cloud environments, where external services and integrations are commonly used. Ensuring the security of these third-party services helps protect your cloud environment from external threats.

Best Practices:

- Conduct thorough security assessments of third-party providers.
- Implement strong API security measures for all integrations.
- Monitor third-party access and activity within your cloud environment.
- Review and update third-party permissions routinely and access rights, and remove integrations if the vendor is no longer needed.

Conclusion

Cloud security is an ongoing process requiring continuous evaluation and improvement. By adopting these strategies organizations can significantly enhance their cloud security efficacy.

As cyber threats evolve, prioritizing cloud security and embracing a comprehensive, well-constructed approach is essential for secure and scalable cloud operations. Remember, while most cloud providers offer robust security features, the ultimate responsibility for securing your data and applications in the cloud lies with your organization.

About the Author

Hooman Mohajeri assumed the role of Vice President of Security Services in 2023, having co-founded Strata Consulting and served as its Chief Security Officer before BlueAlly acquired the company. Bringing a robust 20+ year background in IT, which began during his time working for a civilian division of the Air Force and has since been applied across multiple prominent Silicon Valley companies, Hooman specializes in security architecture, risk management and aligning security programs with business objectives. With a bachelor’s in computer science and key certifications including CISSP and CISM, Hooman's executive direction is marked by clear communication, collaboration and a results-driven approach. His vision is to foster trust-based customer relationships and establish BlueAlly's security division as a sales driver and leading innovative solutions provider within the industry.

Hooman can be reached online at LinkedIn and at our company website https://www.blueally.com/.

14 Million Victims of Malware Breaches in the U.S. Healthcare Sector

Critical Need for Multi-layered Cybersecurity Strategy

By Rhoda Aronce and Ashwini Bhagwat, Senior Threat Researchers at SonicWall

Healthcare is a data-driven business, storing vast amounts of sensitive personal and medical information, such as social security numbers, medical histories, and financial data, making them attractive targets for exploitation and extremely valuable on the black market. This year alone, over 14 million people were affected by data breaches caused by malware targeting the U.S. healthcare industry. Given the rapid adoption of digital tools, AI, and platforms during and after the COVID-19 pandemic, the attack landscape of healthcare organizations has become increasingly broad and highly attractive to those with ill-intent.

Due to their critical operations and the high probability of financial gain, healthcare organizations have thus become prime targets for ransomware. However, disrupting access to patient data or medical systems can have life-threatening consequences. Because of this, healthcare organizations are more likely to pay ransoms to restore operations quickly and avoid any disruption to care or service to patients who could be adversely affected.

91% of Healthcare Breaches Involve Ransomware

In 2024, ransomware was leveraged in an alarming 91% of malware-related data breaches in the healthcare sector, with Lockbit emerging as one of the most notorious ransomware groups targeting this industry. Lockbit claimed responsibility for the high-profile breaches of LivaNova and Panorama Eyecare, a medical device manufacturer, affecting over 180,000 U.S. patients, and an eyecare company affecting close to 400,000 individuals.

Another significant group, BlackCat (ALPHV), was implicated in the Change Healthcare data breach, where a $22 million ransom was paid under false pretenses, leading to a subsequent ransom demand by another group, RansomHub.

Both Lockbit and BlackCat (ALPHV) operate as Ransomware-as-a-Service (RaaS), allowing them to scale their operations by recruiting affiliates who carry out attacks in exchange for a cut of the ransom payments. This evolving model enables even those with limited technical expertise to launch sophisticated ransomware attacks, increasing the frequency, scale, and impact of these incidents.

Digital Systems Creating Multiple Access Points

The increasing integration of digital systems, such as electronic health records, telemedicine platforms, and the Internet of Medical Things (IoMT) devices, has created multiple access points for attackers. For example, the Cl0p Ransomware group exploited a zero-day vulnerability in MOVEit (CVE-2023-34362), a secure file transfer application, to inject SQL commands and access customer databases. This breach leaked sensitive healthcare information, including treatment plans, from CareSource, a non-profit organization that manages Medicaid, Medicare, and Marketplace programs.

Rise in Phishing and Social Engineering Attacks

Healthcare workers' focus on patient care often makes them susceptible to phishing and social engineering attacks. Cybercriminals exploit this by crafting targeted campaigns that maliciously trick unsuspecting employees into revealing credentials or downloading malware, as seen in the 2024 Los Angeles County Department of Mental Health breach.

Overall, in 2024, ransomware groups targeting the healthcare sector have exploited several critical vulnerabilities, leveraging well-known flaws to infiltrate networks, escalate privileges, and deploy ransomware. Our data shows about 60% of vulnerabilities leveraged by threat actors against healthcare targeted Microsoft Exchange.

Best Defense Against Threats

To defend against cyber threats, healthcare organizations must implement a multi-layered cybersecurity strategy, focusing on regular updates, strong access controls, and 24x7x365 monitoring.

- **Regular updates and patch management:** Regularly updating operating systems, applications, and security tools ensures that the latest security patches are applied. For example, vulnerabilities like ProxyShell and ProxyLogon in Microsoft Exchange Server were exploited because many organizations delayed applying patches.
- **Strong access controls and authentication protocols:** Implementing multi-factor authentication (MFA) reduces the risk of unauthorized access from compromised credentials. Additionally, using Zero-Trust Network Access (ZTNA) and secure SD-WAN, makes sure that only the right people can get into sensitive healthcare systems, cutting down the chances for attacks
- **Continuous monitoring:** Continuous 24x7x365 monitoring is vital for healthcare organizations to detect and respond to cyber threats in real-time, minimizing the risk of data breaches and service disruptions. With healthcare systems under constant attack, around-the-clock monitoring ensures that any suspicious activity is quickly identified and mitigated before it escalates into a major incident.
- **Enlist a Trusted Security Vendor:** Engage with a reputable Managed Security Service Provider (MSSP), highly adept at stopping evasive threats and blocking attacks and equipped with the most up-to-date security threat information and innovative solutions to thwart the same.

Bad actors never sleep thus your security protocols should constantly be vigilant, monitoring round-the-clock for any untoward activity. Cyber threats are not a matter of if but when and those healthcare companies best prepared to deal with the same—with the right measures, protocols, monitoring, and trusted security partners—will be the ones that weather the severe ramifications of bad actors' intent on exploiting any and all vulnerabilities.

About the Authors

Rhoda Aronce and Ashwini Bhagwat serve as Senior Threat Researchers at cybersecurity leader SonicWall. SonicWall's security solutions, including advanced firewalls and threat detection tools, have successfully prevented over 26,000 attacks in 2024 by providing real-time threat intelligence and rapid response capabilities. To learn more about SonicWall's findings in its 2024 SonicWall Threat Brief, please visit https://www.sonicwall.com/threat-report.

Rhoda Aronce and Ashwini Bhagwat can be reached directly at raronce@SonicWall.com and abhagwat@SonicWall.com respectively.

Cybersecurity in 2025 - The New Risks Every Business Must Address

Businesses must understand the nature of cyber risks from AI-powered attacks and quantum computing vulnerabilities to supply chain disruptions and advanced social engineering tactics

By Babar Khan Akhunzada, Founder & CISO, SecurityWall

As we look ahead to 2025, the cybersecurity landscape is becoming increasingly complex. With new technologies, evolving threats, and shifting regulatory demands, businesses must proactively address emerging risks to protect their data and infrastructure. This article explores the new and evolving cybersecurity risks that organizations will face by 2025, backed by insights and data from reputable sources across the cybersecurity space.

1. AI-Driven Cyberattacks - The New Face of Cybercrime

One of the most transformative changes to the cybersecurity landscape is the growing use of **artificial intelligence (AI)** in cyberattacks. AI-powered tools allow cybercriminals to automate and enhance their tactics, enabling them to execute highly targeted and more sophisticated attacks. This shift is set to accelerate as we move toward 2025.

The Impact of AI on Cybersecurity Threats

As AI evolves, it can enable cybercriminals to automate **phishing** campaigns, creating convincing, personalized messages that are more likely to deceive recipients. Moreover, AI's ability to generate **deepfakes** poses a growing threat, with attackers using these tools to impersonate key personnel or executives, gaining access to sensitive company data.

Google's Security Blog highlights that while AI can bolster cybersecurity defenses, it also empowers attackers to create threats that are harder to detect. According to recent reports, the use of AI in cybercrime will only intensify, requiring businesses to adopt AI-based detection systems capable of identifying and neutralizing these evolving threats before they cause harm.

For businesses to stay ahead, investing in **AI-driven security technologies** and **machine learning systems** that can identify unusual patterns of behavior and detect malicious activities in real-time will be crucial. Google Cloud predicts that AI-enhanced cyberattacks will become increasingly prevalent by 2025.

2. Quantum Computing and the Encryption Crisis

With the rise of **quantum computing**, current encryption methods could soon be obsolete. Quantum computers possess the power to break traditional encryption algorithms, which could compromise sensitive data and critical infrastructure. This emerging threat is a game-changer for cybersecurity.

Preparing for the Quantum Challenge

While quantum computing is not yet fully realized, its potential to decrypt conventional cryptographic systems is undeniable. Businesses that rely on **public-key cryptography** (such as RSA) could find their data vulnerable once quantum computers become more accessible. As noted by The Times, **quantum-resistant cryptography** is already being developed to withstand these future attacks, and organizations must prepare for this shift.

In response, experts recommend that businesses begin **transitioning to quantum-safe encryption** today to avoid potential vulnerabilities in the future. Regulatory bodies, such as the **U.S. National Institute of Standards and Technology (NIST)**, are already working on post-quantum cryptographic standards. Staying ahead of the quantum threat by investing in next-gen encryption technologies will be essential for data security by 2025. The U.S. Federal Communications Commission (FCC) has proposed a new rule urging telecom companies to enhance their network security against unauthorized access or interception of communications.

3. Ransomware Attacks - A Growing Threat to Supply Chains

Ransomware has been a persistent threat for several years, but by 2025, cybercriminals are expected to target **supply chains** more aggressively. Cyberattackers are no longer just focused on individual organizations; they are leveraging vulnerabilities in third-party suppliers to launch devastating attacks that can disrupt entire industries.

Supply Chain Vulnerabilities

Ransomware remains one of the most significant cybersecurity threats. However, by 2025, the focus of ransomware attacks will shift from targeting individual organizations to more **disruptive** supply chain attacks. Cybercriminals will exploit vulnerabilities in smaller suppliers or third-party vendors to gain access to larger organizations, aiming for maximum disruption. The nature of ransomware attacks is evolving. Instead of simply encrypting data, attackers may leverage **multifaceted extortion** tactics, threatening to release sensitive data publicly unless the victim pays the ransom. According to Cyber Defense Magazine, these types of attacks are likely to become more common as businesses become more resilient to traditional ransomware attacks.

To combat this threat, businesses must not only enhance their own cybersecurity but also assess the security posture of their **supply chain partners**. Implementing robust **backup systems**, conducting regular **penetration testing**, and ensuring that third-party vendors comply with the latest security standards will be essential in mitigating the risk of a ransomware attack.

4. The Rise of Social Engineering and AI-Powered Fraud

With the increasing use of **AI** in cybercrime, social engineering attacks are also becoming more sophisticated. Attackers will leverage generative AI tools to craft highly convincing **phishing emails**, impersonate trusted personnel, and exploit social media profiles to gain unauthorized access to systems.

New Game of Social Engineering in 2025

As AI continues to evolve, social engineering attacks will become more personalized and harder to detect. Using generative AI, attackers will be able to craft highly convincing phishing emails, impersonate individuals in text messages or phone calls, and exploit social media profiles to gather personal information. These attacks will be tailored to the recipient, making them more effective and dangerous.

Cybercriminals are using AI to analyze publicly available data from social media platforms to create personalized, targeted attacks. These attacks may include fraudulent job offers, fake customer service requests, or even impersonations of CEOs or other executives within an organization. According to Cyber Defense Magazine, these types of AI-driven fraud will become much more prevalent in the coming years.

To defend against these threats, businesses must prioritize **employee education** and ensure that staff members are equipped to recognize these increasingly convincing scams. Additionally, enforcing **multi-factor authentication (MFA)** and **email filtering systems** will help block malicious messages from reaching employees.

5. Zero-Trust Security Models Essential for 2025

As cyber threats continue to evolve, businesses are increasingly adopting the **Zero-Trust security model**, which assumes that no user or device is trustworthy by default, regardless of whether they are inside or outside the network.

Why Zero Trust is Crucial

Traditional perimeter-based security models are no longer sufficient to protect against modern threats. As cybercriminals develop more advanced attack strategies, businesses must verify every access attempt before granting it. According to TechRepublic, Zero Trust provides a comprehensive framework for reducing the attack surface by continuously authenticating users and devices and limiting access based on need-to-know principles.

Adopting a Zero-Trust model requires integrating identity and access management (IAM) tools, conducting regular security audits, and enforcing least-privilege access across all systems. By 2025, organizations that have not yet implemented Zero Trust could be exposed to an increasing number of threats. TechRepublic outlines the steps businesses should take to embrace Zero Trust.

6. Proactive Hybrid Security

As businesses move into more complex environments, such as cloud systems and interconnected networks, it is crucial to adopt a proactive approach to security. This is where **audits** and **penetration testing** (pentesting) come into play, providing businesses with the tools they need to identify vulnerabilities before cybercriminals can exploit them. But since penetration testing and auditing is getting very generic and not that impactful that's where hybrid audit and penetration testing comes in where human centric and automated mechanism transform the process via SaaS platforms.

Hybrid PTaaS on the other hand, simulates real-world cyberattacks to assess an organization's defenses and response mechanisms. By mimicking how hackers might exploit weaknesses in systems, penetration tests can uncover potential entry points not only to existing exploits but real hacker approach via dynamic testing. These tests allow businesses to identify risks that may not be visible during routine security scans, making them a critical part of a comprehensive risk management strategy.

By integrating **hybrid automated security audits** and **penetration testing services** into your cybersecurity strategy, businesses can continuously assess and enhance their security infrastructure. With continuous auditing, actionable insights, and real-time alerts empowers businesses to detect and address security gaps before they become serious threats.

7. Geopolitical Tensions and State-Sponsored Attacks

The geopolitical **environment** will continue to influence cyber threats in 2025. Nation-states, especially from regions like China, Russia, North Korea, and Iran, will continue to use cyberattacks as a tool for achieving political and economic goals. These state-sponsored attacks will target critical infrastructure, intellectual property, and sensitive governmental data.

Organizations must stay informed about the geopolitical risks and assess the impact of potential state-sponsored threats on their operations. Businesses operating in critical sectors such as energy, finance, and healthcare will need to invest heavily in **threat intelligence**, **incident response** capabilities, and **cyber resilience** to defend against these sophisticated threats.

8. Data Privacy - Stricter Regulations and Governance

As data privacy regulations become more stringent globally, businesses must take proactive steps to protect customer and employee data. Laws such as the **GDPR** and the **California Consumer Privacy Act (CCPA)** have already set high standards for data protection, and more countries are likely to follow suit.

The Data Privacy Landscape

With the integration of AI into business operations, data privacy risks have grown. AI tools may inadvertently expose sensitive information if not properly governed. To comply with regulations and protect against data breaches, businesses must implement **data governance policies** that prioritize transparency and accountability.

Additionally, businesses must ensure that all data processing activities are in line with global privacy standards. This includes enhancing data encryption, conducting regular privacy impact assessments, and ensuring data access is restricted to authorized personnel only.

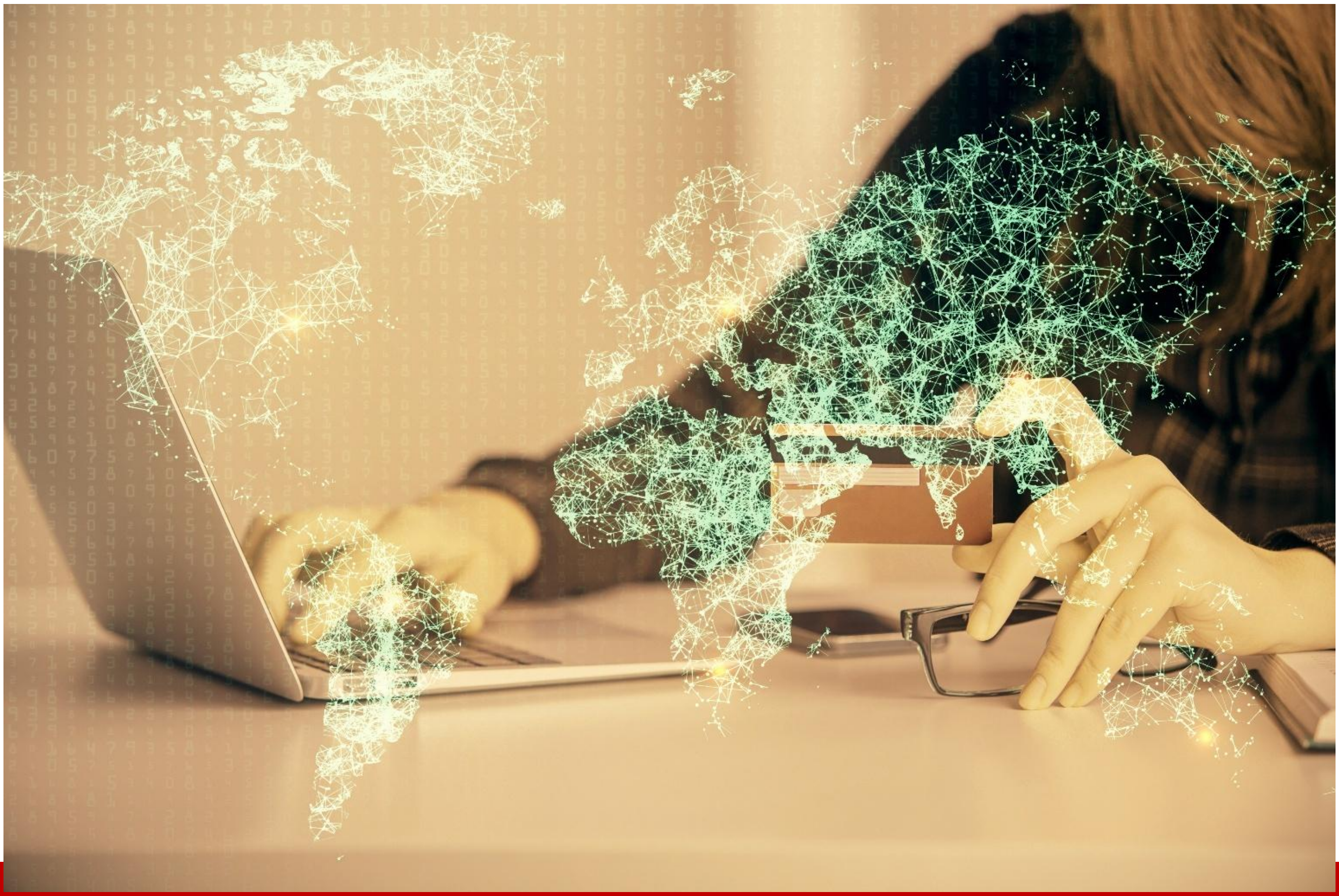
The cybersecurity threats businesses will face in 2025 are complex and varied, ranging from AI-driven attacks to quantum computing vulnerabilities and evolving ransomware tactics. To stay ahead, businesses must adopt cutting-edge security technologies, implement comprehensive security frameworks like Zero Trust, and prepare for regulatory challenges related to data privacy and governance.

By proactively addressing these risks, organizations can build a resilient cybersecurity plan that will protect their data, systems, and reputation as the threat continues to evolve. The future of cybersecurity demands vigilance, adaptation, and a commitment to continuous improvement.

About the Author

Babar Khan Akhunzada is a seasoned cybersecurity expert and entrepreneur, the Founder of **SecurityWall**, a leading cybersecurity firm that offers a **Hybrid Penetration Testing as a Service (PTaaS)** model. SecurityWall serves both startups and enterprises, specializing in **Penetration Testing**, **Audit**, and **Compliance** (SOC2, IBM AS400). Recognized by industry giants in Silicon Valley for his innovative security contributions, Babar is regular speaker at BlackHat, OWASP, BSides, InfoSec and many more frequently shares his insights on **Application Security**, **Cyber Warfare**, **OSINT**, **Cyber Policy**, **Forensics**, and **Red Teaming**, helping organizations stay ahead of emerging cyber threats.

For more information author can be reached online at email, twitter or website.



Impact Modeling Will Become a “North Star” of Cyber Resilience Planning in 2025

By Scott Kannry, Co-Founder and CEO, Axio

Traditionally, IT teams have relied on probability analysis as a primary guide for their resilience strategies. This meant assessing the likelihood that a specific type of cyber incident would occur and allocating resources to fortify high-risk systems and vectors, as needed. It's a useful framework that has—and will continue to—help companies surface potential threats and design strategies to address them. However, as the cyber landscape evolves, security teams must shift their approach as well.

In 2025, cyber incident impact modeling will take center stage as a primary driver of resilience planning. The growing consensus among security leaders is that overemphasizing probability can hinder rather than enhance resilience. By broadening their focus to include the consequences of incidents that *do* occur rather than solely emphasizing the probability of those that *might,* organizations will be better positioned to prioritize mitigation and recovery efforts.

The problem with an overreliance on probability analysis

An overreliance on probability analysis can create a false sense of security. For example, a threat deemed “low probability” may still carry devastating consequences if it materializes. A ransomware attack targeting operational technology (OT) systems, for example, while statistically uncommon, could paralyze critical infrastructure, halt production lines, or disrupt patient care.

This sole focus on probability can also lead to skewed resource allocations. An IT team, for example, might direct most of its efforts toward mitigating high-likelihood, low-impact incidents (e.g., phishing attempts) while neglecting preparation for low-likelihood, high-impact events. This misalignment can leave organizations vulnerable to the types of incidents that can cause the greatest harm.

Ultimately, probability analysis offers only part of the picture. By itself, it doesn’t answer the question that decision-makers care about most: “What would happen if this threat became a reality?”

Why impact modeling matters

Impact modeling expands the conversation from “What are the chances of this happening?” to include, “What would happen if it did?” By focusing on tangible consequences—whether financial, operational, or reputational—security leaders can better understand and prepare for the cascading effects of a cyber incident.

This approach isn’t just theoretical; it’s driven by real-world events. Recent high-profile OT incidents have underscored the critical need to plan for impacts, not just probabilities. Here are a few recent examples from this year that should give any team pause:

- A mass tech outage in July forced **Delta Air Lines** to ground flights across multiple airports and caused significant delays for passengers. The financial fallout included lost ticket revenue, increased operational costs, and potential reputational damage from frustrated customers, highlighting how even a single event can cripple critical infrastructure.

- A month later, a ransomware attack targeting systems at **Seattle-Tacoma International Airport** led to widespread delays and logistical challenges. The incident demonstrated how dependent modern transportation hubs are on interconnected systems. A breach in one area can ripple through airport operations, affecting airlines, passengers, and downstream logistics partners.

- When the medical systems at **Lurie Children’s Hospital** in Chicago were hit by a ransomware attack in January, it forced the cancellation of critical medical procedures. Beyond financial costs like lost revenue and incident response expenses, the attack raised life-or-death stakes, delaying urgent care for vulnerable patients and eroding public trust in the institution’s ability to safeguard sensitive data and ensure continuity of care.

These examples illustrate how focusing solely on probability can leave organizations unprepared for the devastating consequences of these incidents. Impact modeling ensures that decision-makers prioritize the right resources to address these scenarios and develop robust recovery plans.

The rise of impact modeling in 2025

In 2025, impact modeling will no longer be a secondary consideration in resilience planning—it will take center stage. Security leaders are increasingly recognizing that understanding and preparing for the aftermath of an attack is just as important as preventing the attack itself.

For example, impact modeling enables organizations to:

- **Quantify financial exposure:** By estimating the potential costs of a cyber incident, from lost revenue to regulatory fines, organizations can better allocate budgets toward high-impact risks.

- **Prioritize critical systems:** Impact modeling helps identify which systems and processes are most essential to business continuity, ensuring they are adequately protected.

- **Enhance recovery strategies:** By simulating the downstream effects of a cyberattack, organizations can develop more effective response and recovery plans.

By adopting impact modeling, organizations will be better positioned to answer the “what if” questions that drive resilience. This approach provides actionable insights that help organizations proactively mitigate risks, reduce downtime, and minimize financial losses.

Balancing probability and impact

It’s important to note that impact modeling doesn’t replace probability analysis entirely; rather, it complements it. Probability analysis still plays a role in identifying likely threats and guiding preventive measures. However, by combining probability with impact modeling, organizations can achieve a more comprehensive understanding of their risk landscape.

This balanced approach ensures that security teams allocate resources wisely, focusing on both high-likelihood and high-impact scenarios. For example, a ransomware attack targeting sensitive customer data might have a low probability but catastrophic consequences. By integrating impact modeling into their planning, organizations can ensure they are prepared for even the most unlikely events.

Building long-term resilience

As cyber threats become more sophisticated and interconnected, resilience planning must evolve to keep pace. Impact modeling provides the clarity organizations need to navigate an increasingly complex threat landscape. By focusing on tangible outcomes, security leaders can develop strategies that not only prevent incidents but also minimize their effects.

Understanding and preparing for the consequences of a potential attack has proven far more valuable to effective decision-making and long-term resilience. By placing impact modeling at the heart of resilience planning, organizations can ensure that their cybersecurity strategies align with business objectives, protect critical operations, and foster stakeholder confidence.

In 2025, impact modeling will no longer be a "nice-to-have"—it will be an essential tool for building and sustaining resilience. Security leaders who embrace this shift will be better equipped to protect their organizations from the ever-evolving cyber threat landscape.

About the Author

Scott Kannry is the Chief Executive Officer and Co-founder of Axio, a leading cyber risk management company. As the architect of Axio's four-quadrant cyber loss impact taxonomy and methodology for evaluating and stress testing insurance portfolios, Scott spearheaded a novel process designed specifically to better align overall cyber exposure with insurability. This approach was the first to codify the reality that cyber predicated losses can trigger numerous lines of insurance coverage. Scott has been recognized as a 40 Under 40 broker by Business Insurance magazine, a power broker by Risk and Insurance magazine, and an industry rising star by Reactions magazine. Scott can be found on LinkedIn here.

Evaluating the CISO

Two Methods to Assess a Security Leader's Performance

By Dmytro Tereshchenko, Chief Information Security Officer at Sigma Software Group

The CISO role has evolved dramatically in recent years. Today, CISOs are integral executive team members, shaping strategy, translating tech issues for different stakeholders, and managing budgets. This requires more than just cybersecurity and technical knowledge — it calls for strong skills in budgeting, communication, and leadership.

Moreover, CISOs operate under vastly different conditions across organizations. In some places, they might just be setting up a firewall, while in others, they might lead a team of 100 or more people. Budgets, domains, team sizes, and resources can also vary widely, making it difficult to develop a universal metric for evaluating a CISO's performance.

Daniel Lohrmann's 2018 article sparked an important conversation about how to assess CISOs in this broader role. Drawing on years of experience as a CISO and mentor for other security and risk leaders, I've slightly adapted Lohrmann's ideas. In this article, I reflect on five key groups with whom CISOs should build relationships, presented in a specific order.

Lohrmann's CISO Grading Tool

In his article, Lohrmann proposed evaluating CISO effectiveness through relationships with five groups of stakeholders. These relationship areas reflect factors such as trust, respect, project results, communication skills, and overall competence in engaging with the various groups that CISOs generally interact with regularly. They also highlight a CISO's ability to lead and inspire greatness in others.

- **Internal Security Team:** Relationships with your internal security team, including staff who report directly to you.
- **Internal Organizational Peers:** Relationships with business and technology professionals at a similar level across your organization. This includes internal customers you work with and protect.
- **Management:** Relationships with your boss(es) and other senior executives, including your boss's peers and those at higher levels.
- **Vendors:** How effectively you work with security providers, including managing contracts, acquiring contract staff, engaging with technology providers, and assessing new technology acquisitions.
- **External customers**: Relationships with broader organizational clients, including individuals who use your business partner's products and services.

As Lohrmann suggests, grading should be as simple as possible. To evaluate a security leader, he proposes to answer this question: *Does the CISO have a "good" (or even "very good" or better yet "great") relationship with this particular group? Does this group respect and trust the CISO as their security adviser?*

- **If only one group** trusts and respects the CISO: The CISO is unlikely to last long unless their boss strongly supports and protects them. Essentially, the CISO is in trouble.
- **If two groups** show trust, support, and respect: This reflects basic competence, but the CISO is average at best.
- **If three groups** trust the CISO: The CISO is doing well but should continue striving for improvement.
- **If four groups** trust and respect the CISO: This signifies an above-average performance.
- **If all five groups** trust, respect, and follow the CISO: they will support the CISO through both cyber successes and challenges. This is the mark of a truly exceptional security leader.

How to Become a Five-Star CISO: A Step-by-Step Guide

I've been using Lohrmann's grading tool for a few years now — first, as a CISO to evaluate my own effectiveness and later as a mentor and supervisor to transfer knowledge to other CISOs. Over time, I've slightly adjusted Lohrmann's approach, adding some important details and slightly changing the priorities.

Similar to Lohrmann, I'm evaluating five main areas. They go from the most important one to the least important. For each area, I'm using a star-based rating system, ranging from one star to five. As a CISO, it's challenging to stay focused on more than two or three complex tasks at a time. To ensure sustained progress, I don’t allow my mentees to move on to the next area until they’ve earned at least three stars in the current one. In some areas, there are essential components that must be addressed before achieving a high rating or advancing to the next stage.

1. Relationships with your internal security team

Building and evaluating relationships within your team should be your top priority. As a CISO, you participate in discussions and make decisions about complex technical issues, lead company cultural transformation, make decisions about team members' salaries, resolve conflicts, and address their various concerns. If your team respects you and values your opinion, you can rate yourself highly in this area. Mutual trust between you and your team is essential, and achieving it will enable you to accomplish far more. Establishing this trust is essential — it must be prioritized above all else.

Delegation skills are an essential component that should be evaluated separately in this area. Effective delegation is essential to prevent becoming a bottleneck, as micromanagement is unsuitable for the CISO role. Delegating complex tasks not only lightens your load but also helps foster the team’s overall competence. Without strong delegation skills, CISOs cannot rate themselves highly in their relationship with the internal security team.

2. Relationships with internal organizational peers

This area focuses on your relationships with other departments and their managers within your company. For example, in our organization, I collaborate with the following teams:

- InfoSec Board
- Service Center (IT Department)
- Compliance team
- HR Team
- Legal Team
- Accounting
- PR Team

The relationships with the first five stakeholders (InfoSec Board, Service Center, Compliance Team, Legal Team, and HR Team) are essential, as the CISO regularly interacts with them on various matters. While relationships with other teams, such as Accounting and PR, are beneficial, they are not as critical. **It’s ideal to establish connections with these teams, but failing to do so is not a significant setback.**

3. Security programs and projects

This area is not addressed in Lohrmann’s article, but I consider it to be one of the most important. A CISO is hired to lead, manage, and support specific projects or programs such as migrating to a cloud or hybrid infrastructure, implementing zero-trust principles, launching security awareness initiatives, or assessing risks and creating a roadmap for post-quantum cryptography implementation. The success of these initiatives ultimately falls under the CISO’s responsibility.

To execute these programs effectively, the CISO relies heavily on its team and internal organizational peers. As such, building strong relationships with both is essential for successfully delivering projects. Below are examples of projects and programs a CISO may undertake after excelling in the first two areas:

- Zero Trust Initiatives
- Migration to cloud or hybrid infrastructure
- Configuration and roll-out of EDR (Endpoint Detection and Response) and MDM (Mobile Device Management) tools
- Improvement of the Vulnerability and Patch Management program
- Security Awareness Program
- Enhancement of Application Security Program
- and more

The Zero Trust approach has become indispensable for all modern enterprise architecture, especially after the COVID-19 pandemic, when employees began connecting to company infrastructure and internal services literally from everywhere, not just offices. This approach proved highly effective for us in Ukraine during the full-scale russian invasion in 2022, ensuring security and resilience under extreme circumstances.

4. Relationships with your management

This area encompasses the following relationships:

- Linear Manager
- Board of Directors/Founders
- Ownership over the Security Budget

A CISO must have responsibility for the information security budget, which includes funding for the team, tools, and services. Without direct control over the budget, it becomes challenging to rate the relationship with management highly, as budget ownership is a critical aspect of the CISO's role.

5. Vendor Relationships

This area encompasses the following relationships:

- Vendors/Suppliers
- Customer/Vendor questionnaires.

How to implement this method

When onboarding a new CISO, begin with the first area: relationships with the internal security team. Evaluate their progress using a star rating system from 1 to 5 stars. Once they achieve at least 3 stars, they can move on to the next group of stakeholders. This approach can also be applied to assess the performance of an existing CISO.

About the Author

Dmytro Tereshchenko is Chief Information Security Officer at Sigma Software Group, a global tech company, and lecturer at Sigma Software University and SET University.

With over 21 years of comprehensive IT experience, including a decade specialising in cybersecurity, Dmytro brings extensive expertise in risk and incident management, secure SDLC, and regulatory compliance. Leveraging his profound software development background and cybersecurity expertise, Dmytro is a crucial member of Sigma Software Group's application security consulting service. In this role, Dmytro and his team help companies assess, develop, and implement tailored application security management systems to maintain and improve the security level of their online services portfolio.

Dmytro can be reached online at mailto:dmytro.tereshchenko@sigma.software and at our company website Sigma Software Group.

You May Be at Risk: How to Defend Against Ransomware In 2025

By Alan Chen, President and CEO, DataNumen

If you're in business, then you should have a solid line of defense against ransomware at the top of your to-do list. For every 11 seconds that go by, a ransomware attack hits a company head-on. If you're struggling to rationalize the scale of this, that's 7,800+ attacks per day, and the numbers are growing.

If you're not too familiar, ransomware attacks are basically a form of data stealing. Your files will get locked, encrypted, and held "for ransom" until you pay a fee to the attacker. But, like most things that are unpredictable in life, sometimes even paying the ransom is not enough to get your data back. And if that happens, your operations slow down or stop, you lose thousands of dollars, and productivity takes a tumble.

But don't panic! There are multiple legit ways to avoid paying when you recover your data from ransomware.

Keep reading to learn more, as this guide covers several proven ransomware recovery methods. We'll discuss options like AI tech, built-in Windows tools, etc. If you stay proactive, you can quickly and safely get your encrypted files back, so start taking notes!

Learning to Protect Yourself From Ransomware: The Ins and Outs

Ransomware attacks are really common – so common that 84% of companies deal with this issue. This means that you'll want to cover your bases to keep your data safe.

You'll probably want to get your data back ASAP. But before you jump the gun in defense, you should first understand the challenges you might run into.

Detecting Types of Ransomwares: Which Variants Should I Know About?

Tech is getting smarter, which means that the risks are increasing. Ransomware shows up differently in different cases, so you'll need more than one defense method, including:

- Doxware: Doxware threatens to leak your private data unless you pay.
- Wiper Malware: This type of ransomware doesn't try to encrypt; it tries to destroy data.
- Crypto Ransomware: Crypto variants encrypt your files and say they won't decrypt until you pay them.
- Locker Ransomware: This type of ransomware locks you out of your device completely.
- Scareware: Scareware tries to intimidate you and trick you into paying to get your data back.

So, What Kind of Damage Has Been Done, and How Much?

Don't know where to start? Firstly, you must evaluate the damage, and be quick. Any lost time just ups the chances of losing data and credibility, too.

Find out what's hurt and whether or not your backups are still useful. Data has revealed that 96% of attacks target backup systems.

How Can I Recover My Data? Common Methods Used

Next, you can start taking back your data, so to speak. A backup system like Windows System Restore is usually the fastest and most reliable option. Just take note that modern ransomware often disables this feature.

Another option is third-party decryption tools, depending on the type of ransomware. And of course, general data recovery tools are available.

But your best bet is to keep multiple types of backup in different locations. This approach has led to much better recovery rates. Some companies have even gotten to full restoration in <10 minutes with just 10 seconds of data loss.

DIY Recovery Methods: Get Creative

When in doubt, consider these do-it-yourself alternatives:

Option 1: Using Windows System Restore

First, try Windows System Restore. It can bring your system back to its previous state but does have its limits. For one, it won't recover your personal files. Also, some ransomware can compromise these restore points.

Option 2: Make Use of Your File History and Backups

Second, start doing regular backups. Here are some important things to consider if you want to truly back up your files and documents:

- Make sure to disconnect all of your backup devices when you aren’t using them.
- Keep a set of offline copies for your most important data.
- Only use the strongest, unbreakable storage methods.
- Plan for frequent backups on your schedule.
- Follow the 3-2-1 backup rule.

Option 3: Decryption Tools

Third, custom decryption tools can help return your files to you without you having to pay the ransom.

Actually, 55% of available decryption tools are completely successful, based on recent findings. As for partial recovery, the rate is just 4%. (Note, however, that 41% of these tools fail to recover any data.)

Option 4: Data Recovery Tools

Finally, if backups, Windows System Restore, and decryption don’t seem to work, you might need to get some professional data recovery software. DataNumen SQL Recovery is a top solution right now. It can recover SQL Server databases that have been attacked.

Remember, the success of any method will depend on the specific ransomware variant and how fast you respond to the attack. For the best defense, you should use several strategies at once, rather than just one.

Recovery Solutions for Small Businesses

Small businesses are perhaps even more vulnerable to ransomware than larger organizations are. Fifty-six percent of businesses had ransomware attacks hit them last year. And in that sector, 27% ended up having to pay the ransom. But worry not – here’s your complete guide to recovery that won't break the bank.

Emergency Response Procedures

Time is always of the essence when recovering data. This is why it's important to have a good emergency response. Your first priority should be implementing these key steps:

- Immediately disconnect infected systems from the network
- Document the scope of the attack
- Contact your IT support or security team
- Check backup systems for contamination
- Alert relevant authorities and stakeholders

Some studies are showing that companies whose backups were compromised paid an average of $2.30 million in ransom. On the other hand, companies with intact backups only paid $1 million.

Local Backup Restoration

Your local backup strategy should follow the "3-2-1" principle. This includes keeping *three* different copies of data, using *two* different storage mediums, and keeping *one* copy offsite.

For the best protection, you should use write-once storage techniques. Seventy percent of companies now use hardened disks on-site.

Cloud Backup Recovery Options

Small businesses may also turn to cloud solutions. The cloud offers strong protection against ransomware, and 89% of companies now use fixed clouds for backup. Consider applying these advanced features:

Feature	**Benefit**
Multi-cloud solutions	Prevent vendor lock-in
Immutable storage	Prevents backup encryption
Instant recovery	Minimizes downtime
Automated testing	Ensures backup integrity

You can speed up recovery by using cloud platforms with instant recovery capabilities. This allows you to restore systems on demand, cutting down the typical recovery time of days or weeks. Just remember that you need to properly test first. Studies show that only 35% of ransomware victims reach full recovery within a week.

What Are the Up-and-Coming Recovery Technologies?

Ransomware recovery tech is evolving fast. Cutting-edge solutions emerge to fight off more and more advanced attacks. These changes alter the way that people can protect and recover data.

AI-Powered Detection and Recovery Tools

Artificial Intelligence is changing ransomware detection with >99% precision in spotting threats. Your systems can now detect ransomware impact in near real-time.

They analyze file entropy changes, extensions, and header manipulations to stop attacks before they spread. Modern AI solutions also auto-assess the blast radius of attacks and initiate recovery tactics without human intervention.

Blockchain-Based Backup Solutions

Blockchain tech is a totally new way of securing backups. It works by using a decentralized, distributed ledger system. Your backup data receives a unique cryptographic fingerprint, making it impossible for attackers to alter or corrupt stored info. This technology gives you:

- Decentralized storage that prevents single-point failures
- Tamper-proof transaction records
- Independent verification of data authenticity
- Immutable audit trails

Immutable Storage Options

Immutable storage has emerged as your last line of defense against ransomware. Using Write-Once-Read-Many (WORM) technology, your backups become unchangeable once written. Modern immutable storage systems implement:

Feature	**Benefit**
Retention locks	Prevent unauthorized deletion
Access controls	Restrict modification attempts

Encryption	Protects data integrity
Automated testing	Ensures backup reliability

Zero-Trust Architecture Integration

Zero Trust principles are another innovation in data protection. They assume no implicit trust based on location or network. Your security framework verifies every access attempt through multi-factor authentication and enforces least-privilege access. This ensures that even if attackers breach your network, they can't access or change important backup data.

All of these emerging technologies work together for a strong defense against ransomware attacks. By combining them, you notably enhance your ability to recover from attacks without having to dip into your pockets.

Conclusion

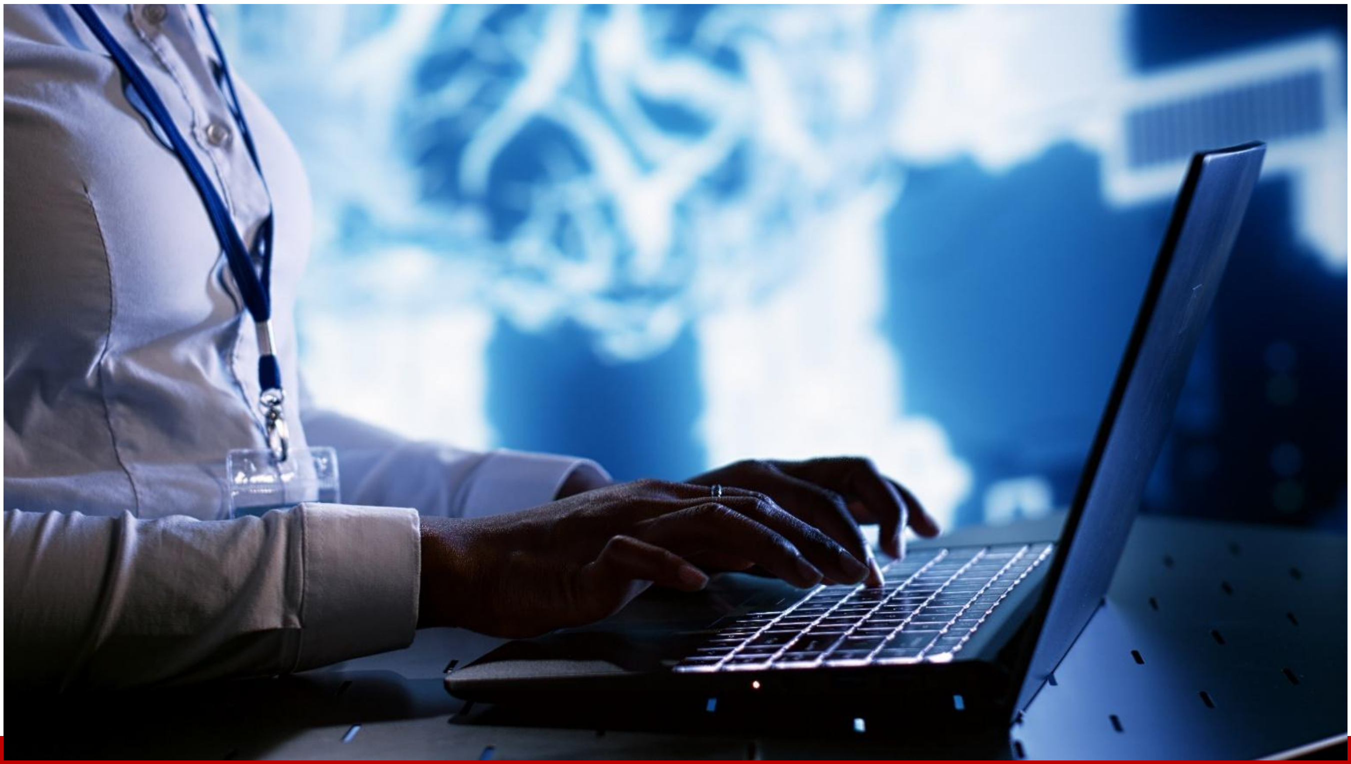
So, you've learned about the seriousness of ransomware attacks, the different ways they happen, and lines of defense against them. Whether you're part of a business or an individual, you can take some comfort in the fact that various recovery solutions exist. With a little help, you can regain control of your data. Modern tech like AI-powered detection, blockchain-based backups, and zero-trust architecture protect against even the most advanced attacks.

Your best defense combines traditional backup methods with new tools. Regular local and cloud-based backups, along with fixed storage solutions, speed up recovery and minimize data loss. Studies show that organizations using several tactics get better outcomes and rarely pay ransoms.

Remember, planning ahead and acting fast in response to attacks can make the difference between successful recovery and permanent data loss. Start implementing these recovery solutions today, test them regularly, and stay updated with the latest security measures. With the right tools and strategies in place, you can protect your systems and recover quickly from any ransomware attack.

About the Author

Alan Chen is the President and CEO of DataNumen, a leading data recovery company founded in 2001. The company provides recovery solutions for Outlook, Word, Excel, PDF, databases, and images. Their clients include global giants like IBM, Intel, Cisco, Microsoft, General Electric, Xerox, and Oracle. Alan can be reached online at pr@datanumen.com and at our company website https://www.datanumen.com/



A CISO’s Guide to Managing Cyber Risk in Healthcare

By Gaurav Banga, Founder and CEO of Balbix

Now more than ever before, our healthcare data is under attack. Of all of the sensitive information available on the dark web, medical records are among the most expensive, costing on average $1,000 - compared to just $1 for a Social Security Number. It's clear that our healthcare system has become a hot spot for phishing scams, unpatched vulnerabilities, ransomware, and patient data exposures, as most recently evidenced by the Change Healthcare data breach earlier this year. For Chief Information Security Officers (CISOs) on the frontlines of the fight, these staggering increases have sent an unequivocal message about the urgent state of data protection in the United States: The time for action is *now*.

But where do we start? As cyber threats to our healthcare ecosystem reach a critical juncture, CISOs are facing mounting pressure to reimagine data protection and cyber risk practices for the modern era. Even for the most seasoned CISO, this can be seen as a daunting task, requiring careful oversight of HIPAA compliance, IoT medical devices, and distributed data management. One wrong turn and your entire system could be at risk.

With data breaches involving Protected Health Information (PHI) costing nearly $11 million on average, time is of the essence for healthcare CISOs to mitigate cyber risks before they turn into a full-blown crisis. Here are three best practices to keep in mind.

Build a Robust Data Governance Framework

To help manage regulatory compliance and reduce cyber risk, CISOs should begin by regularly updating and reviewing data protection policies from the top down. This also includes regularly running risk assessments to identify and prioritize high-impact vulnerabilities across systems and IoT devices to ensure quicker remediation times. Worse, this past October nearly 5 million individuals were affected by a healthcare data breach due to compromises with network servers, email, and electronic medical records. By embedding agility and consistent vulnerability scanning directly into any data governance framework, CISOs can remain flexible during times of change, and more easily make their case to the Board for updated data security standards as a tool, not a hindrance, with security teams and developers ultimately bringing them to life.

More, CISOs can (and should) consider regularly engaging third-party auditors, who can ensure regulatory adherence from an unbiased perspective. When it comes to sensitive healthcare data, you can never be too careful, so it’s always better to err on the side of safety and prioritize high-risk vulnerabilities rather than pay for the consequences of indifference down the line. At the end of the day, developing a truly robust data governance framework can also enhance data security and create a culture of risk prioritization.

Embrace Next-Gen AI Solutions

Generative artificial intelligence (GenAI) has taken the world by storm in recent years for its ability to revolutionize laborious processes with efficiency in mind. And its impact on healthcare data protection is no exception. In fact, GenAI can play a significant role in addressing cybersecurity concerns in healthcare by providing CISOs with risk articulation, allowing security teams to better understand inbound threats based on location, teams, departments, and assets. These next-gen tools can interact directly with security operations personnel in natural language, enabling them to quickly find relevant data and IP addresses in order to triage red flags and speed up investigations.

Additionally, GenAI can automate traditionally time-intensive ticketing and operational tasks, streamlining remediation and patching processes. In doing so, security teams can spend time doing what they do best: thinking strategically, and innovatively, about how best to protect their company’s data. Of course, it’s no secret that bad actors – especially in the healthcare space – have gotten more elusive in recent years. Equipped with the latest in GenAI technology, however, healthcare CISOs now have an arsenal of tools at their disposal to best them at every turn.

Turn Mistakes into Mastery

Make no mistake: In the world of cybersecurity, there’s strength in numbers, and the mistakes of one CISO can easily be turned into “lessons learned” for another. Accordingly, by breaking down barriers impeding knowledge sharing and promoting cross-collaboration between companies, cybersecurity teams can learn from the past and ensure that they’re adequately prepared for the future. For better or worse, under new SEC guidelines, companies are now required to disclose material cybersecurity incidents they experience, as well as regularly share information regarding their cybersecurity risk management, strategy, and governance. By tapping into this publicly available information, healthcare CISOs can ensure they remain one-step ahead of the curve, applying strategic learnings to reinforce the protection of PHI and personally identifiable information (PII).

Where We Go from Here

Ready or not, large-scale cyberattacks in the healthcare space aren't going anywhere anytime soon. No longer can cybersecurity teams take a reactionary approach to data protection, simply waiting for risks to appear before acting on them. On the contrary, healthcare CISOs must always be ready for the unexpected, employing (and enforcing) precautionary measures that anticipate potential threats before they happen. By following the steps outlined above, CISOs can create a new cybersecurity playbook for the healthcare sector, ensuring that private healthcare information stays private and protected.

About the Author

Gaurav Banga is the CEO and Founder of Balbix, an AI-powered cybersecurity risk management platform.

2025 Outlook: Turning Threats into Opportunities in a New Era of Innovation

By Ravi Srivatsav, CEO and Co-Founder of DataKrypto

We're excited to share what’s top of mind for us as we head into a new year, based on conversations with our customers, technology leaders and cybersecurity innovators. As we step into 2025, the cybersecurity landscape is at a pivotal juncture. The challenges of AI-driven threats, evolving data privacy standards, relentless breaches, and the looming quantum computing era demand vigilance and innovation.

#1 Continued government regulation and the rising cost and consequences of data breaches will pressure companies to uplevel data privacy initiatives to a strategic business imperative.

With data breaches continually rising, data privacy is as significant a concern as ever. Standards around the globe, such as the UK’s General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), also pressure the U.S. government to keep up. At the same time, the cybersecurity industry demands regulation to help companies protect their customers and their brands.

Many non-technology industries need to be faster to update their legacy infrastructure, but struggle due to cost constraints and limited resources. With the continued movement toward digitalization and the use of vast cloud data storage, this situation cannot continue. Businesses simply can’t afford the high cost of a breach. This scenario is especially true in healthcare, which remains a primary target of cyber-attacks.

Many organizations have relied on cyber insurance for protection in the event of an infringement, but the sheer volume of breaches triggers insurance providers to terminate coverage when negligence is deemed a factor. In addition to the steep regulatory fines and penalties resulting from a breach, companies also face class-action lawsuits from their business and consumer customers, costing organizations hundreds of millions, if not billions, of dollars. Company executives and Boards of Directors are now being held personally liable when customer data falls into the wrong hands, tainting their reputations and subjecting them to punitive action.

In 2025, organizations will increasingly address data privacy strategically and operationally, investing in new infrastructure and technology to develop stringent data protection to avoid the costly consequences of cybersecurity attacks. Adversely, such investments can create new attack surfaces, which will be addressed with innovative, privacy-enhancing technologies (PETs) like secure multi-party computing (SMPC), trusted execution environments (TEEs), confidential computing, and fully homomorphic encryption (FHE).

#2 Data breaches will lessen as cyber developers focus on building “secure by design” applications that protect data throughout its lifecycle.

Today’s relentless onslaught of data breaches costs companies millions yearly and erodes trust in their brands. This scenario has left organizations scrambling to find and invest in solutions that enable end-to-end data protection throughout its lifecycle — safeguarding data at rest, in use, in transit, and every point in between.

For several years, Fully Homomorphic Encryption (FHE) was touted by cryptography experts as an ideal solution to close the gaps created by traditional encryption and protect data at all times. Traditionally, technology’s high incremental costs, integration complexities, and performance bottlenecks have prevented its widespread adoption and practical implementation for real-world business use cases.

We expect a dramatic shift in 2025 toward more widespread adoption of FHE, a trend that will continually expand in years to come. New FHE innovations that make real-world deployment practical, affordable, and manageable will help companies across industries maintain continuous data protection and minimize the impact of many prominent attacks (see below). As attackers realize their efforts to breach systems and access confidential data are ineffective, they will eventually focus elsewhere.

#3 Cybersecurity vendors will introduce “quantum-safe” solutions as quantum computing poses new risks.

As quantum computing advances, organizations worldwide are growing increasingly concerned about its potential impact on cybersecurity. While experts estimate the post-quantum computing (PQC) era is still five to 15 years away, forward-thinking companies are preparing for this inevitable future. Hackers aren't waiting for the PQC era; they're harvesting data now, anticipating future decryption capabilities.

In August 2024, the U.S. Department of Commerce’s National Institute of Standards and Technology (NIST) finalized its principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer, encouraging computer system administrators to transition to the new standards as soon as possible. At the same time, NIST stated that the 2048-bit keys used by Rivest–Shamir–Adleman (RSA) encryption should continue to offer sufficient protection through at least 2030.

In 2025, as the world prepares for a PQC future, companies face a more immediate threat: the gaps in data protection when data is in use for analysis and computation, and when it moves between different stages in its lifecycle. Advanced encryption algorithms, such as Fully Homomorphic Encryption (FHE), are being adopted to overcome these gaps.

In response to the forthcoming quantum computing threat combined with the ongoing need for end-to-end data protection, we see two trends emerge:

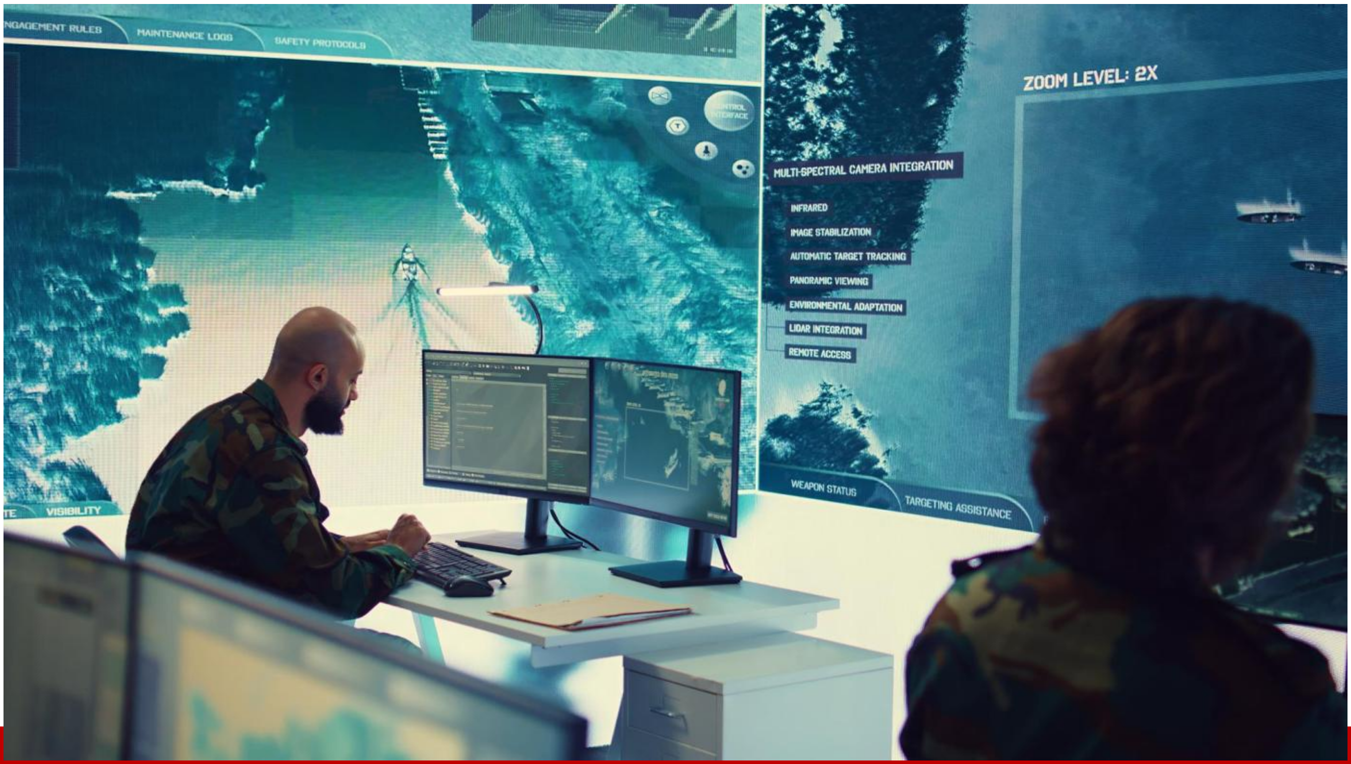
1. Organizations will prioritize implementing advanced quantum-resistant cryptographic techniques, such as Fully Homomorphic Encryption (FHE) based on symmetric encryption.
2. Cybersecurity vendors will advance algorithms already in development to make quantum attack-proof security systems a reality.

As we look ahead to the coming year, we're standing on the precipice of a new era in cybersecurity. It's not just about defense anymore; it's about innovation, about turning challenges into opportunities. As cyber threats grow in sophistication, 2025 will identify the trailblazers who turn these challenges into opportunities, setting a new standard for resilience and trust in an increasingly digital world.

About the Author

Ravi Srivatsav is Co-Founder and CEO of DataKrypto. Ravi is a serial entrepreneur with extensive experience in the tech industry. Most recently, he was a partner at Bain & Company, advising Fortune 500 companies. Before that, he served as the Chief Product and Commercial Officer at NTT Research. He was also the Founder of ElasticBox and led it to a successful acquisition by CenturyLink.

DataKrypto website: https://datakrypto.com/company-2/, and Ravi can also be reach https://x.com/datakrypto and https://www.linkedin.com/company/datakrypto/



Advancing Defense Security Through Zero Trust Segmentation

By Gary Barlet, Public Sector Chief Technology Officer, Illumio

The FY2027 Zero Trust deadline requires Department of Defense (DoD) agencies to meet target level goals of the Pentagon's Zero Trust Strategy. This requirement aims to fundamentally transform the way DoD handles cybersecurity, moving from traditional perimeter-based defenses to a more dynamic, adaptive, and resilient framework. Unlike the conventional security models that rely on strong perimeter defenses to keep threats out, Zero Trust operates on the principle that threats can originate from anywhere — both inside and outside the network – and relies on a "never trust and always verify" concept – constantly monitoring, authorizing, and authenticating every workload, application, user, device, or system.

A central component of the Zero Trust architecture is Zero Trust Segmentation (ZTS), technology based on Zero Trust principles that divides a network into small, isolated segments and controls access to each segment. This plays a key role in protecting valuable assets, mission data, and national security interests.

Zero Trust Segmentation: An Essential Piece in the Zero Trust Architecture

According to NIST, the Zero Trust architecture adheres to these tenets: everything is considered a resource; all communications are secured – whitelisting only pre-approved applications, processes, and devices within the network; access is granted per session based on dynamic policies; the integrity and security of all assets are monitored; and strict authentication and authorization are enforced.

ZTS applies these tenets to its security methodology. By adhering to the principle of “least privilege” access and enabling continuous visualization of all communication patterns and traffic between workflows, devices, and the internet, ZTS restricts lateral movement if an attack were to occur.

While the DoD recognizes the critical role of ZTS in enhancing cybersecurity, it is prioritizing foundational elements of the Zero Trust framework first. Initial stages focus on strong identity and access management, robust network and application security, and improved endpoint security, which are crucial for supporting security tactics like ZTS.

For example, the DoD’s Zero Trust Strategy consists of seven key outcomes, including reducing attack surfaces through proactive actions enabled by microsegmentation of the DoD Information Enterprise. The DoD also released the DoD Zero Trust Capability Execution Roadmap, which lists ZTS as a key capability. Following this, the U.S. Air Force included an area in its newly released Zero Trust Strategy focused on expanding segmentation capabilities. By adopting ZTS, DoD agencies are not only aligning with strategic objectives, but also fortifying their defenses against evolving cyber threats, ensuring the protection of critical missions, and maintaining national security.

Zero Trust Segmentation Helps Warfighters Meet the Mission – Safely and Securely

To ensure DoD agencies are utilizing ZTS to its fullest effect, they should start with increasing end-to-end visibility to map out all assets and data flows. From there, agencies can identify high-value assets and assess associated risks, which will prepare them to define security policies for precise traffic management and control.

Another key component of ZTS is recognizing that attacks are inevitable – and putting the appropriate measures in place. Through continuous visualization, the isolation of high-value assets, and limiting the lateral movement, these proactive steps reduce the risk of widespread damage by attacks when they inevitably occur. Like how cars are equipped with seatbelts and airbags to reduce the fallout of a car accident, ZTS puts proactive steps in place to reduce the impact and damage when the worst occurs.

ZTS’ granular control over network traffic allows for precise enforcement of security policies, essential for maintaining robust security in complex environments where traditional methods may fall short due to their rigidity and lack of adaptability. ZTS ensures agile operations can remain in place and that rapid recovery efforts can be deployed, if necessary.

From a risk management perspective, ZTS facilitates proactive vulnerability identification and mitigation – allowing detailed monitoring of all traffic patterns further enhances security by enabling early detection of suspicious activities or deviations from normal traffic behavior.

Additionally, ZTS helps prioritize risk mitigation efforts and allocate resources strategically. This proactive approach not only strengthens overall cybersecurity but ensures resilience against evolving cyber threats. By embracing ZTS, mission warfighters can establish a robust defense framework that adapts to the dynamic nature of cybersecurity challenges, safeguarding critical operations and mission-critical assets effectively.

Advancing Defense Readiness Through ZTS

Implementing ZTS is crucial for the DoD because it enhances the security and resilience of its cyber infrastructure. By ensuring full visibility across all traffic patterns, identifying vulnerabilities and risks, isolating critical assets, and containing potential breaches, ZTS prevents lateral movement of threats – minimizing damage and operational disruption. This ensures mission-critical systems remain secure and functional.

ZTS not only safeguards sensitive information but strengthens the DoD's ability to swiftly and effectively respond to evolving cyber threats. It achieves this by implementing strict access controls, continuously monitoring network activities, and applying policies that limit access based on user roles and context. This means that even if a threat actor breaches one segment of the network, they cannot easily move to other segments.

ZTS can help the DoD achieve its mission, maintain operational integrity, protect sensitive information, and enable a robust defense against sophisticated cyber adversaries.

About the Author

Gary Barlet is the Public Sector Chief Technology Officer, at Illumio, where he is responsible for working with government agencies, contractors and the broader ecosystem to build in Zero Trust Segmentation as a strategic component of the government Zero Trust architecture. Previously, Gary served as the Chief Information Officer (CIO) for the Office of the Inspector General, United States Postal Service. He has held key positions on several CIO staffs, including the Chief of Ground Networks for the Air Force CIO and Chief of Networks for the Air National Guard CIO, where he was responsible for information technology policy and providing technical expertise to senior leadership. He is a retired Lieutenant Colonel from the United States Air Force, where he served as a Cyberspace Operations Officer for 20 years. Gary can be reached online at https://www.linkedin.com/in/gary-barlet-4384115/ and at our company website https://www.illumio.com/

AI In Cybersecurity: Empowering Lean Teams to Defend Against Big Threats

By David Atkinson, CEO, SenseOn

Cybersecurity teams are shrinking, with nearly half of UK businesses (46%) relying on just one individual to oversee their cybersecurity. In the public sector, team sizes average three, while private sector teams are typically limited to just two members. This level of staffing illustrates how stretched security resources have become, where limited personnel means lean teams face ongoing challenges in securing their organisation's defences.

Fortunately, leaner teams don't have to mean weaker security. Advances in artificial intelligence (AI) are helping businesses streamline threat detection and response, reduce alert fatigue, cut costs, and enable cybersecurity professionals to shift their focus from reactive responses to strategic initiatives, moving away from false alarms and manual processes.

AI in cybersecurity works by collecting and analysing data from various points across an organisation's network - from system logs to network traffic - to automatically identify unusual patterns that may indicate a threat. Through continuous learning, AI can discern between regular and anomalous behaviours, such as outbound data traffic or unexpected login attempts. This automated detection is especially valuable for lean IT teams, helping them overcome three major hurdles in cybersecurity: time, visibility, and expertise.

Time: Moving from reactive to proactive

Due to the limited time lean teams have, they often operate reactively. When an issue arises, a ticket is logged, requiring immediate attention from the cybersecurity professional. This focus on immediate needs leaves little time for proactive security measures like patch management, user training, and device hardening.

One of AI's strengths is its ability to drastically reduce false positives by learning an organisation's "normal" behaviour patterns. This significantly cuts down on the volume of alerts that require manual investigation, saving significant amounts of time. For instance, AI can quickly differentiate between a command-and-control attempt and an employee streaming a sports event from overseas. By filtering out such false alarms, AI enables lean teams to dedicate their limited resources to genuine threats and long-term security improvements.

Visibility: Breaking down data silos

Most organisations still rely on siloed security tools, which limits visibility and makes life difficult for lean teams, especially those without dedicated security engineering resources. When security staff want to improve network visibility, they often face configuration challenges that make achieving comprehensive oversight complex and time-consuming.

AI-driven security solutions help by consolidating and filtering security data, giving teams a unified, coherent view of their network. This "single pane of glass" approach not only provides detailed insights into potential threats but also eliminates the need for expensive, specialised tools for each function. By simplifying data presentation and reducing the number of tools in use, AI enhances visibility, allowing teams to better monitor their environments without additional complexity.

Skills: Filling the expertise gap

With cybersecurity skills in short supply, many lean teams struggle to find the expertise needed to improve their organisation's security posture. In fact, 70% of IT and cybersecurity decision-makers say that the skills shortage increases risks to their organisations.

AI offers a way to bridge this skills gap by performing expert-level analysis on vast amounts of data and identifying patterns that suggest genuine threats. When threats are detected, AI can automatically isolate compromised endpoints, terminate malicious processes, and organise data within established frameworks like MITRE ATT&CK for easier reporting. This automation can cut the mean response time to under 10 minutes, enabling staff to respond to incidents without the need for additional hires or extensive expertise. In essence, AI equips lean teams with advanced threat detection and response capabilities that would otherwise require a much larger, highly skilled workforce.

Enterprise-level AI benefits

In many organisations, lean security teams must manage increasingly complex security environments. AI presents a unique opportunity for these teams to achieve enterprise-level protection without the need for a large-scale infrastructure or expanded workforce. However, for AI to reach its full potential, access to high-quality, consolidated data is essential.

If the data AI relies on is fragmented across multiple tools or not designed for AI analysis, it can struggle to deliver accurate results. Solutions that aggregate data from endpoints, cloud workloads, and network traffic into a single, cohesive format offer a distinct advantage, enabling AI to more accurately detect and respond to threats.

By using AI-based tools that unify data effectively, security teams can automate threat detection and response, significantly reducing the time and manual effort required. AI empowers lean teams to operate with the sophistication and efficiency of larger, resource-intensive operations by providing advanced capabilities that would otherwise be out of reach.

With AI as an enabler, lean cybersecurity teams can rise to the challenge, turning limited resources into a powerful defence strategy. Through the power of automation, advanced analytics, and streamlined processes, AI is helping lean teams do more with less, bringing them closer to the goal of resilient, proactive cybersecurity.

About the Author

David Atkinson is the Founder and CEO of SenseOn. He has over fifteen years' experience working within the UK's specialist military units and Government environments where his close work with CISOs enabled him to identify flaws with current cyber defence approaches, highlighting the need for a new technology to deal with the increasing velocity of cyber-attacks.

David can be reached online at LinkedIn and at our company website https://www.senseon.io/

DORA Is Here: Guidance For US Companies on How to Comply

By Avani Desai, CEO of Schellman

Cybersecurity has become a non-negotiable priority for organizations operating across borders. From ransomware attacks on critical infrastructure to data breaches that expose sensitive customer information, the stakes for businesses increase year after year. These challenges have prompted regulatory bodies around the globe to enforce stricter standards, including the European Union's Digital Operational Resilience Act (DORA) that came into full effect in January.

Although DORA primarily targets EU-based financial institutions, its implications extend far beyond Europe. U.S. companies that serve EU clients, particularly in the financial and Information and Communication Technology (ICT) sectors, must comply to avoid significant financial, operational, and reputational risks. Understanding DORA and taking proactive measures can protect businesses while demonstrating a commitment to operational excellence in the global marketplace.

What is DORA, and Why Should U.S. Companies Care?

DORA is an EU regulation aimed at fortifying the digital resilience of financial institutions and their critical ICT service providers. It ensures organizations can withstand and recover from digital disruptions, including cyberattacks, to maintain economic stability and societal functioning.

The financial sector, essential for both economies and society, relies heavily on ICT systems, often outsourced to third-party providers. This dependency introduces risks, as disruptions in these services can have cascading effects across other sectors and economies. DORA addresses this by holding EU financial institutions and their ICT supply chains accountable for operational resilience.

For U.S. companies, the implications are clear: if a business provides cloud computing, cybersecurity, or data processing services to EU financial institutions, compliance with DORA is non-negotiable. Non-compliance risks include legal penalties, operational disruptions, and damaged client relationships. Beyond its immediate scope, DORA reflects a global shift toward stricter cybersecurity regulations. Preparing for DORA positions businesses to adapt to similar frameworks emerging worldwide, safeguarding future operations and client trust.

Key Components of DORA That Affect U.S. Companies

DORA's requirements cover multiple aspects of operational resilience, with provisions that U.S. companies need to prioritize. The first is risk management frameworks; DORA mandates that companies adopt an ICT risk management framework to identify, mitigate, and respond to threats. This involves regular assessments, board-level involvement, and comprehensive incident response planning, all of which are critical for U.S. businesses to maintain partnerships with EU clients.

Another element is incident reporting and response. Under DORA, companies must report significant ICT-related incidents, like cyberattacks, data breaches or system failures, to EU authorities within specific timelines, including details on the cause, impact, and mitigation measures. For U.S. firms, this means establishing processes for detecting and classifying incidents quickly. Additionally, operational resilience testing is a cornerstone of DORA compliance. Regular vulnerability assessments, penetration testing, and scenario-based drills ensure systems are prepared for real-world cyber threats.

Third-party risk management is also an important focus area. EU financial institutions are responsible for the resilience of their supply chain, which includes ICT service providers. Businesses must demonstrate compliance through updated contracts, audits, and evidence of strong security practices. Finally, information sharing is encouraged under DORA to enhance collective resilience. Firms must establish secure channels for sharing cyber threat intelligence with EU partners and clients.

Why Act Now? The Risks of Non-Compliance

The risks of ignoring DORA are significant and multifaceted. Regulatory authorities can impose fines and penalties for non-compliance, but the consequences extend beyond that. Being perceived as a weak link in a client's cybersecurity chain can result in irreparable reputational damage, leading to lost business opportunities and strained relationships.

Operational risks are also a major concern. Insufficient resilience measures can lead to service disruptions, data breaches, and prolonged recovery periods. These challenges erode client trust and can cause cascading issues throughout operations – including an impact on the bottom line. The cost of non-compliance for DORA can be steep. As global cybersecurity regulations tighten, addressing gaps now will save significant resources in the future while positioning an organization as a leader in operational resilience.

Independent third-party assessments offer an objective evaluation of an organization's systems, identifying vulnerabilities that may be overlooked internally. These assessments can be conducted in-house or by external experts, depending on the organization's resources and needs. External experts can thoroughly assess risk management frameworks, incident response plans, and resilience practices, while simulating real-world threats to uncover weaknesses before they are exploited. While third-party assessments provide external validation, internal evaluations offer a deeper, hands-on understanding of specific systems and processes.

Regardless of the approach, the key is to proactively assess vulnerabilities to strengthen security posture. Engaging independent experts can signal a business's commitment to security, building trust with EU partners and clients, and offering a competitive advantage in a security-conscious market. Businesses should carefully evaluate whether internal or external assessments best suit their needs, as both approaches offer unique benefits for DORA compliance.

Next Steps for U.S. Companies

To be compliant with DORA, businesses should begin with a thorough gap assessment. This will help identify any weaknesses in current cybersecurity and operational resilience practices. Next, they should evaluate existing systems to pinpoint areas for improvement. Strengthening incident response protocols is also crucial – organizations should review current plans to ensure they meet DORA's strict reporting requirements and establish clear processes for efficiently detecting, classifying, and mitigating incidents.

Regular testing should also be prioritized. Vulnerability assessments, penetration tests, and resilience drills would become routine parts of a cybersecurity strategy. Finally, businesses should consider engaging a trusted partner. Working with a third-party assessor can provide the expertise and resources needed to streamline compliance efforts and ensure alignment with DORA's standards.

Complying with DORA: An Investment in the Future

DORA's reach extends beyond the EU, profoundly impacting U.S. companies serving EU financial institutions. Achieving compliance ensures regulatory alignment and also strengthens organizational resilience, builds client trust, and positions businesses for success in a world of growing regulatory demands.

By adhering to DORA's standards, businesses can mitigate immediate risks, protect their reputation, and fortify operations against future challenges. Investing in compliance is more than meeting legal requirements—it's a strategic decision to enhance security, bolster client confidence, and thrive in an increasingly cybersecurity-conscious world.

About the Author

Avani Desai is the Chief Executive Officer at Schellman, the largest niche cybersecurity assessment firm in the world that focuses on technology assessments. Avani is an accomplished executive with domestic and international experience in information security, operations, P&L, oversight and marketing involving both start-up and growth organizations. She has been featured in Forbes, CIO.com and The Wall Street Journal, and is a sought-after speaker as a voice on a variety of emerging topics, including security, privacy, information security, future technology trends and the expansion of young women in technology.

Avani sits on the board of Arnold Palmer Medical Center and Philanos; is Audit Committee chairwoman at the Central Florida Foundation; and is the Co-Chair of 100 Women Strong, a female-only venture capitalist-based giving circle that focuses on solving community-based problems specific to women and children by using data analytics and big data. Avani Desai can be reached online at our company website https://www.schellman.com/

3 Ways FinOps Strategies Can Boost Cyber Defenses

By Laurence Dale, CISO, Surveil

As organizations deepen their reliance on cloud technology, many are adopting FinOps – a strategic blend of financial management and technical expertise – to better manage costs and strengthen cybersecurity. Why is this approach increasingly popular? Businesses often overspend on cloud services by as much as 30% due to limited visibility and control. FinOps tackles this inefficiency by optimizing cloud spending, which frees up resources for vital cybersecurity investments. This both reduces IT waste and strengthens data protection and compliance, setting up a business for a secure – and successful – future. In this article, discover three ways FinOps strategies can help boost your organization's cloud security.

1. Cost-Optimization for Security

Security remains a priority for organizations, especially in the face of evolving threat actors and increasingly sophisticated cyber-attacks. FinOps helps organizations to identify and eliminate inefficiencies in their cloud spending. This creates opportunities to reallocate resources toward robust security measures such as advanced threat detection systems, robust controls such as multi-factor authentication (MFA) and zero-trust network access (ZTNA) and continuous monitoring tools and services.

By providing visibility into cloud costs, FinOps uncovers underutilized or redundant resources and subscriptions, or over-provisioned budgets that can be redirected to strengthen cybersecurity. Through continuous real-time monitoring, organizations can proactively identify trends, anomalies, or emerging inefficiencies, ensuring they align their resources with strategic goals. For example, regular audits may uncover unnecessary overlapping subscriptions or unused security features, while ongoing monitoring ensures these inefficiencies do not reoccur. This newfound efficiency can fund measures like advanced threat detection systems, new protection measures, or security training programs. FinOps ensures every dollar spent on cloud services delivers value – transforming waste into a secure, streamlined cloud environment.

2. Risk Reduction

By improving visibility and transparency, FinOps enables teams to identify weaknesses – and risks – across licenses, identities, devices, and access points. This insight is particularly valuable in strengthening identity and access management (IAM), ensuring that access controls are properly configured, and multi-factor authentication (MFA) is consistently used to protect critical systems and sensitive data.

A FinOps approach also involved continuous monitoring, which not only identifies potential security gaps before they escalate but also matches security measures with organizational goals. Furthermore, FinOps helps with financial risk management by assessing the costs of potential breaches and allocating resources effectively. Through ongoing risk assessments and strategic budget adjustments, organizations can make better use of their security investments, which will help to maintain a robust defense against threats while still achieving their business aims.

3. Enhanced Compliance and Governance

Meeting standards like GDPR, HIPAA, or PCI-DSS can be both complex and costly – but complying with these regulations is vital for keeping cyber defenses strong. A FinOps approach simplifies the challenge of meeting the most up-to-date regulations by automating compliance reporting. This enables organizations to then make use of cost-effective tools from cloud providers to meet regulatory requirements.

Moreover, governance frameworks are built into FinOps principles, which leads to consistent application of security policies and procedures. This includes setting up governance frameworks that define roles, responsibilities, and accountability for security and financial management. By integrating governance into FinOps practices, organizations can ensure that security measures are aligned with financial goals and that there is a clear understanding of how security investments impact overall cloud spending.

In summary, adopting a FinOps strategy offers organizations a powerful way to optimize cloud spending while enhancing cybersecurity. By focusing on cost optimization, risk reduction, and improved compliance, businesses can effectively direct resources toward strengthening their defenses against evolving threats. FinOps not only helps reduce inefficiencies from holistic visibility of cloud usage but also ensures that security measures are continuously monitored and aligned with strategic objectives. At a time when both cloud costs and cyber risks are on the rise, integrating FinOps with cybersecurity is an essential strategy for any organization aiming to secure its future in the cloud.

About the Author

Laurence Dale is the CISO at Surveil – an analytics and insights engine – which can help optimize IT spending to reduce waste and unlock funds for investment in crucial cyber defenses. Throughout his 25-year technology career, Laurence has gained invaluable global experience through several senior IT leadership roles. Laurence has been responsible for driving the digital, security, and commercial capabilities of multi-national organizations across the FMCG, technology, and manufacturing industries, as well as the UK public sector. In 2017, Laurence took the position of Chief Information Security Officer (CISO) at Essentra PLC., where he led the cyber-risk and privacy management transformation programs. This was followed by a promotion to Group IT Director (interim CIO), leading the global IT team through two major divisional divestments.

Laurence's LinkedIn can be found here https://www.linkedin.com/in/laurencedale/. Our company website is https://surveil.co/

4 Lessons Learned From 2024's Biggest Cyberattacks

By Zac Amos, Features Editor, ReHack

Studying the history of hacking incidents teaches cybersecurity experts that anything can be accessed if someone is determined enough. Cyberattacks have been around since before the internet. The first hacking incident happened in 1834 when two people stole data about the financial market by tapping into the French Telegraph System. Others used wireless telegraphy throughout the years.

The first computer-based hacking incident was thought to occur on a college campus. MIT limited how much time students could spend on computers. In 1962, Allan Scherr decided they should get more. He used a punch card, printed all the passwords in the university's system and passed them out to students.

Computer viruses emerged, followed by more sophisticated hacking. Eventually, phishing, SQL injections, ransomware and denial of service attacks joined the fray. Today, hackers are tapping into the power of artificial intelligence (AI) to up the ante.

Biggest Cyberattacks of 2024

Since the COVID-19 pandemic, more employees have worked remotely than ever before. Although some companies offer a hybrid situation, many others allow people to fully work from home (WFH), leaving doors open for cyberthieves to enter.

One report showed that around 25% of employees working remotely didn't know their work device's security protocols. Collaboration apps were of particular concern, allowing hackers more entry points to proprietary information.

Some of the most notable attacks of 2024 showed where vulnerabilities lie. If companies with large information technology (IT) budgets fall victim to AI bots and cybercriminals, then small businesses are also at risk.

1. Ticketmaster

In May 2024, Ticketmaster Entertainment LLC was attacked by a cybercriminal group called ShinyHunters. The hackers got in through a third-party cloud storage provider and stole the names and contact information of 560 million worldwide customers.

The cyberthieves tried to sell user information online. Credit card details were encrypted, so the company didn't address the issue of what data might be compromised. The event highlights the importance of third-party hosting providers and shows vulnerabilities in cloud storage.

2. Dell Technologies

Also in May 2024, Dell Technologies suffered a data breach by a threat actor called Menelik. He was proud of his accomplishment of stealing data for 49 million customers and outsmarting a huge company's IT department, bragging that he used Dell's portal and created partner accounts to get to the information.

Later in the year, Dell also suffered a hacking incident targeting employee information. The two incidents highlight just how sophisticated hackers are becoming with new tools such as AI and having greater access to other hackers they can learn from.

3. The City of Helsinki

The city of Helsinki, Finland, fell victim to a hacker who exploited a weakness in a remote access server, proving even government entities aren't immune to cyberattacks. They gained access to student, parent and faculty data.

The lesson learned from the attack is that IT systems must be updated regularly, and automating updates can help prevent them. The hacker went right in the front door of the servers, not even trying to hide their entry.

Small businesses might find it beneficial to hire a professional hacker to identify system weaknesses so they can be fixed before an incident occurs.

4. Other Major Incidents

Those are just three of the many hacking incidents in 2024. A few others include:

- **Change Healthcare:** Hackers requested a ransom payment or they'd continue to disrupt health care operations software.
- **Sav-RX:** Cyberthieves stole patients' contact and financial data, proving ongoing monitoring is a must.
- **Microsoft:** Hackers from Russia accessed executive accounts through an old account that didn't have two-factor authentication (2FA) activated.

Lessons to Enhance Cybersecurity

Small-business owners and cybersecurity professionals can learn a lot by studying 2024's hacking incidents. Knowing the game plan of hackers is the first step to securing a website. Of course, cybercriminals constantly come up with new techniques to get around security systems, so IT leaders must keep up with trends and test their servers repeatedly.

There are several lessons to hold onto as the world leaves 2024 and heads into a new year with even more cyberthreats than before.

1. Train Employees

Many workers fail to fully understand how a simple error like failing to install 2FA can put the entire company at risk. Spend time training staff about phishing and basic security measures, especially for those working from home.

The majority of phishing scams start with the user clicking on a link. Make it a companywide policy that no one sends links in emails and they should never click on one, always going to a browser and typing in the address instead.

2. Keep Backups

Having full backups can get a site up and running again quickly. Otherwise, those in health care and other crucial sectors may fall victim to ransomware demands. Having a backup can make websites operational while IT figures out how to increase security.

3. Be Proactive

Small businesses must take the lead in protecting their servers from ever-increasing attacks. Hackers are savvier than ever before, so company leaders must know the trending methods and safeguard their systems.

Ideally, IT should install software that continuously scans for weaknesses and patterns that indicate hackers are in the system. Stopping an incident in its tracks can prevent data loss and customer concerns over leaked personal details.

4. Choose Industry-Specific Protections

Some industries are more at risk than others. Cybercriminals have attacked every type of business imaginable in 2024. However, a focus on health care, education and big business led to ransom demands and crucial data being leaked.

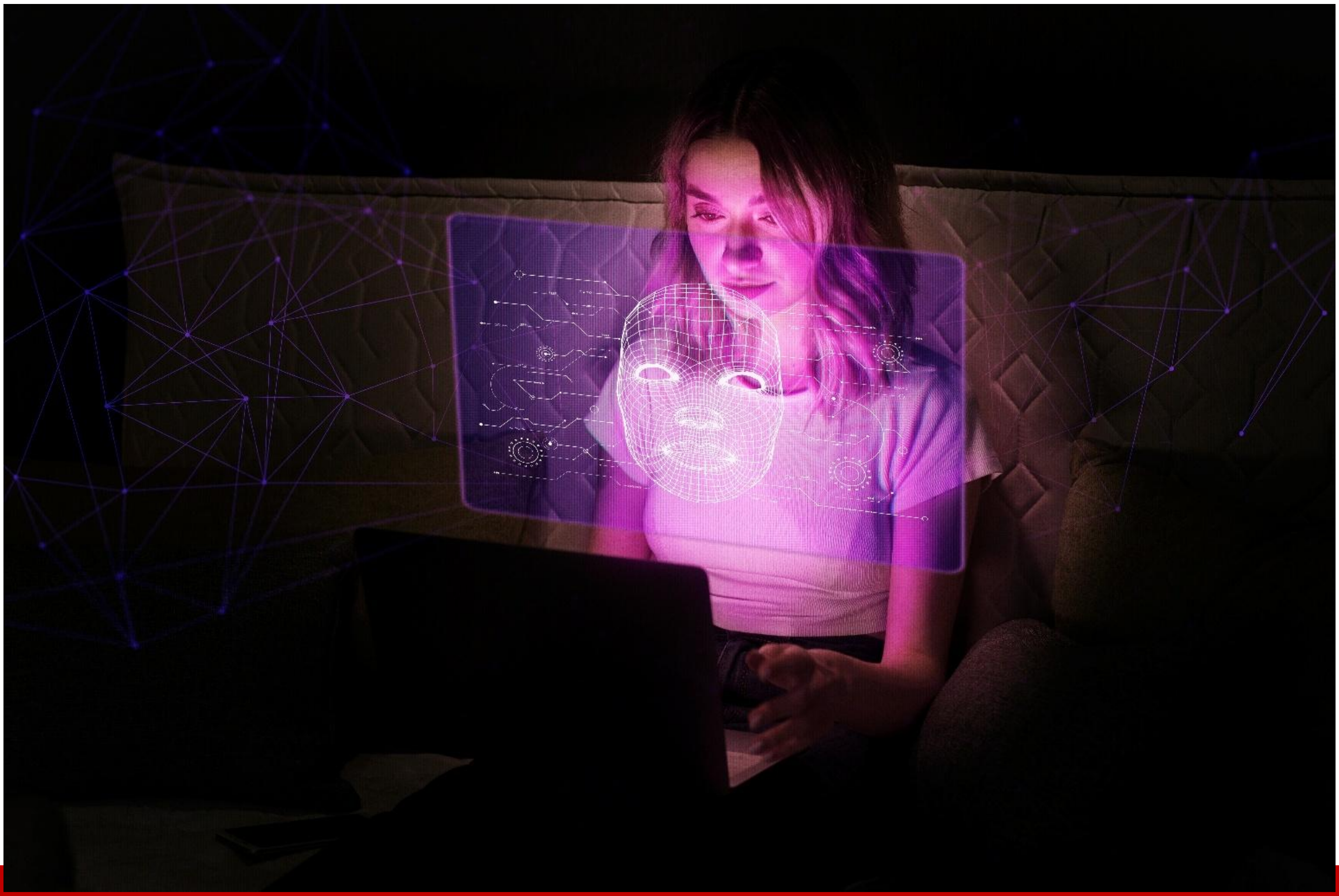
An interruption in the financial or health industries can be detrimental and even deadly in some cases. The ability to stop such attacks and get back online quickly reduces the damage.

Awareness and Action Are Key

Cybersecurity continues to evolve as cyber attackers develop new methods. It's crucial to pay attention to third-party software providers, cloud computing and internal server protections. A successful cybersecurity plan considers all potential threats and eliminates the most likely ones. By being proactive, small businesses can avoid an incident and protect customer data.

About the Author

Zac Amos is the Features Editor at ReHack, where he covers cybersecurity and the tech industry. For more of his content, follow him on X (Twitter) or LinkedIn.



From Awareness to Action: Transforming Cybersecurity with Human Risk Management

Evolving your security program to address today's complex human risk challenges

By Bret Fund, SVP and General Manager of Infosec Institute

Security awareness training has been a cornerstone of cybersecurity programs for years — and it's been effective. In 2021, the Verizon Data Breach Investigations Report found that 85% of breaches involved human mistakes like social engineering. Every year since then the number has dropped: 82% in 2022, 74% in 2023 and 68% in 2024.

Despite this positive momentum, many organizations are hitting a plateau in their training effectiveness. After all, nearly seven out of ten breaches are still connected to employees. Education is essential, but there will always be a crucial gap between security knowledge and actual behavior — one that traditional awareness approaches alone struggle to bridge.

As someone who's worked extensively with security leaders, I've observed this challenge firsthand. Our approach must evolve to match today's threat landscape and workplace dynamics.

Understanding the behavioral security gap

Think about driver's education. We all learn the rules of the road, but knowing those rules doesn't automatically translate to perfect driving behavior. We might speed up to get through a yellow light or check our phones despite knowing the risks. Similarly, employees often know security best practices but may circumvent them to accomplish immediate goals.

This reality is costly. IBM reports that security incidents stemming from human actions typically take over 200 days to identify and contain, making them among the most expensive breaches organizations face. We must move beyond simply making employees aware of security practices to actively supporting and reinforcing secure behaviors in real time.

The evolution of human risk management

Human risk management represents the natural evolution of security awareness programs. Rather than replacing traditional awareness training, it builds upon that foundation by connecting security education directly to real-world behaviors and risks.

The core difference lies in monitoring, measuring and mitigating human risk. Instead of relying solely on simulated phishing tests or annual training completion rates, human risk management integrates with your existing security stack, from email security to DLP solutions, to provide visibility into actual employee behaviors and security events.

Here are some of the critical components of human risk management:

- **Behavioral insights:** Understanding people's thinking and behavior is crucial to effective security awareness. By leveraging behavioral science principles, organizations can design training programs that resonate with employees and motivate them to adopt secure behaviors.
- **Data-driven decision-making:** By analyzing data from various sources, such as security logs, incident reports and user behavior analytics, organizations can identify trends and patterns. This data-driven approach allows for more targeted and effective training interventions.
- **Continuous learning and adaptation:** The cybersecurity landscape is constantly changing. To stay ahead of threats, organizations must adopt a continuous learning approach. This involves providing regular updates, conducting frequent training sessions and using real-world examples to illustrate potential risks.
- **Empowering employees**: Employees are often the first line of defense against cyber threats. Organizations can create a security awareness culture by empowering them with the necessary knowledge and tools. This includes providing clear guidelines, encouraging open communication, and recognizing and rewarding secure behavior.

Creating a culture of security accountability

The goal isn't to catch employees doing something wrong. It's to empower them to make better security decisions. Employees receiving immediate, relevant feedback tied to their work activities are more likely to understand and internalize secure behaviors.

For example, if an employee triggers a DLP alert by sending sensitive data to a personal email, a human risk management approach would immediately provide a quick reminder about data handling policies. This just-in-time guidance is more effective than waiting for the next annual training session.

Breaking down operational silos

One of the most significant advantages of human risk management is the ability to unite traditionally separate security functions. Security operations teams often operate independently from governance, risk and compliance (GRC) and training teams, leading to disconnected efforts and missed opportunities for improvement.

Integrating security alerts with training initiatives creates a feedback loop that benefits both sides. The security operations center (SOC) team's insights inform training content, while practical training reduces alert volume. This integration helps demonstrate concrete ROI through measurable reductions in security incidents.

Benefits across the organization

By breaking down these silos and fostering collaboration between security operations, GRC and training teams, organizations can achieve a more holistic and effective approach to security. This unified approach leads to several benefits across organizations.

For CISOs and security leaders, human risk management provides:

- Unified visibility across security awareness and operations
- Clear metrics showing behavioral change impact
- Reduced alert volume as employee behaviors improve
- Better allocation of security resources

For employees, the benefits include:

- Less interruption from lengthy training sessions
- More relevant, contextual security guidance
- Greater understanding of how their actions affect security
- Improved ability to self-regulate security behaviors

For security operations teams, it helps:

- Reduce alert fatigue through better user behavior
- Focus resources on genuine threats rather than user mistakes
- Create stronger alignment with awareness and compliance teams

Starting your human risk management journey

If you're considering evolving your security awareness program toward human risk management, here are some practical first steps:

1. **Start a dialogue between your security operations and awareness teams.** Understand what alerts they're seeing and which human behaviors are creating the most security noise.
2. **Look at your existing security stack**. Many organizations already have the tools needed to gather behavioral insights. They just need to connect and analyze the data differently.
3. **Focus on culture change.** Position human risk management as an enhancement to help employees work more securely rather than another layer of restrictions.
4. **Start small and iterate.** Choose one or two key behaviors to focus on initially, measure the impact and expand from there.

Remember, this is a journey, not a destination. The goal is continuous improvement in your security culture, not perfection overnight. By cohesively bringing together awareness, operations and behavioral change, we can build more resilient security programs that work with, not against, human nature.

About the Author

Bret Fund is the SVP and General Manager of Infosec, a Cengage Group company, where he focuses on helping organizations and individuals build a culture of cybersecurity and close their skills gaps. Prior to this role he was SVP of Alternative Credential Products at 2U where he focused on driving growth and profitability for the products in his portfolio. In previous roles he was the VP of Education at the Flatiron School, where he oversaw the program development and operations for their consumer and enterprise facing products, and the Founder and CEO of SecureSet, an immersive education company focused on educating the next generation of cybersecurity professionals. Before that, he was an Assistant Professor of Management and Entrepreneurship at the University of Colorado in Boulder.

Bret can be reached online via LinkedIn and at our company website: https://www.infosecinstitute.com/

Enhancing Security, Agility, and Collaboration: The Role of Zero Trust in Mission Partner Environments

By Russ Smith, Field Chief Technology Officer, Zscaler

As modern military operations increasingly rely on multinational partnerships, coalition forces need secure, agile ways to share information. The Department of Defense (DoD) has developed frameworks like Mission Partner Environments (MPEs) and Combined Joint All-Domain Command and Control (CJADC2) to support collaboration across domains—air, land, sea, cyber, and space. CJADC2 integrates capabilities across allies, enabling them to communicate and coordinate in real time.

To support these objectives, a Zero Trust architecture is fundamental to empowering warfighters with immediate access to the data and intelligence they need to make informed decisions that will determine mission success or failure and advance the CJADC2 vision. Zero Trust safeguards the data from adversaries, reinforcing operational resilience.

The Imperative for Secure, Cross-Domain Coalition Collaboration

Effective and secure data sharing lies at the heart of coalition operations. Zero Trust supports CJADC2 by establishing secure "Cyber Lines of Communication" (CLOCs) that don’t rely on a single, monolithic network architecture. Securing Lines of Communication is fundamental for military success in every warfighting domain. As documented by Karl von Clausewitz during the Napoleonic Wars, military strategists use LOCs to move critical resources around the battlefield, and in the cyber domain, that critical resource is information. By verifying every access request based on identity and context, Zero Trust enables real-time, secure data sharing across coalition partners. This approach eliminates implicit trust in network location and shifts security to the user and data level, aligning with CJADC2's need for decentralized, responsive command and control

How Zero Trust Enables Mission Partner Environments within CJADC2

Zero Trust is also critical for MPEs, facilitating rapidly deployed, secure, and flexible access for CJADC2 operations across diverse coalition network requirements. CJADC2's global scope requires MPEs to operate seamlessly across different infrastructures without relying on full network control. With Zero Trust, coalition forces securely exchange sensitive information through each partner's infrastructure while minimizing risks associated with legacy, network-centric models.

Zero Trust enhances MPEs for CJADC2 in key ways:

1. **Enhanced Security Across Coalition Networks**: By enabling identity- and policy-based access controls, Zero Trust reduces risks from unauthorized users and lateral movement within coalition networks. This approach meets CJADC2's requirements for cross-domain information sharing, ensuring only verified coalition members can access specific data or applications.
2. **Greater Agility and Responsiveness**: Zero Trust enables CLOCs, providing real-time access to critical applications and data. This flexibility supports CJADC2's mission for agile, adaptable command structures, enabling coalition forces to respond effectively to changing conditions.
3. **Simplified Infrastructure and Reduced Costs**: Zero Trust removes the need for extensive cross-domain solutions and network-specific security hardware, minimizing costs. Its transport-agnostic approach allows MPEs to use any network, including commercial internet, 5G, or satellite, empowering coalition forces to connect securely over available channels without complex network requirements.

Lessons from the Afghanistan Mission Network and SABRE

The DoD's experience with the Afghanistan Mission Network (AMN) revealed the limitations of traditional, network-centric coalition environments. AMN's federated architecture allowed coalition members access to a central NATO network but will struggle with scalability and agility for future conflicts. Building on these lessons, the DoD is developing the Secret and Below Releasable Environment (SABRE) program to support MPEs. Through Zero Trust principles, SABRE can enable coalition partners to use their own infrastructures while still securing access to shared applications and data. This approach aligns with CJADC2's goal of flexible, unified command and control across coalition networks.

Balancing Security, Accessibility, and Agility in CJADC2

Zero Trust offers an effective model for balancing the three core requirements—security, accessibility, and agility – that coalition information sharing in CJADC2 demands:

- **Security**: Zero Trust enforces identity- and context-based controls at every interaction, reducing the risk of unauthorized access and lateral movement, even if a network is compromised. This principle strengthens MPEs supporting CJADC2, where data must be secured at each access point to protect sensitive, mission-critical information.
- **Accessibility**: By enabling secure access over any network, Zero Trust enhances connectivity across coalition forces, allowing for seamless data flow and collaboration regardless of infrastructure constraints. This ensures effective communication across all domains.
- **Agility**: Zero Trust allows MPEs to adjust access controls dynamically, delivering the agility CJADC2 requires to meet diverse mission demands. Coalition forces can respond quickly to real-time threats or operational changes without extensive network reconfigurations.

Balancing these factors ensures CJADC2 can deliver on its promise of unified, agile command and control across coalition forces, whether for peacekeeping, humanitarian relief, or combat operations.

Moving Forward: Zero Trust as a Key Enabler of CJADC2

CJADC2 requires secure, responsive information sharing across multiple domains, and Zero Trust provides the means to create CLOCs that adapt to coalition forces' needs. As CJADC2 initiatives like SABRE progress, Zero Trust will play an essential role in creating a secure, interconnected command and control system that supports complex, multi-domain operations. In an era where military readiness depends on speed, security, and access, Zero Trust establishes the foundation for a responsive and secure coalition network, supporting both immediate mission success and long-term strategic objectives.

About the Author

Russ Smith is a Field CTO supporting Zscaler's DoD Team. He joined Zscaler after a 30-year Air Force career culminating as the Deputy Chief Information Officer at the United States Special Operations Command. During his post-military career, he was a research analyst with the Institute for Defense Analyses, the vice president of the cyber practice at SAIC, and a security account lead at Accenture Federal Systems. Smith holds master's degrees in Systems Technology (Joint Command, Control, Communications and Computers) from the Naval Postgraduate School and in Military Operational Art and Science from Air University, and a B.S. in Computer Information Science from Bloomsburg University of Pennsylvania. He is also certified as an Information Systems Security Professional, Project Management Professional, Chief Information Officer, and Chief Information Security Officer.

From IoT to AI: How Governments Can Navigate 2025's Cyber Security Landscape

By Bill Diaz, Vice President of Vertical Solution Business at Check Point Software

In 2024, artificial intelligence (AI) took center stage in cyber security, and it's not going away anytime soon. Looking ahead to 2025, we see service providers of all types expanding their networks to the edge, implementing advanced 5G technologies, and preparing for a shift to Open Radio Access Networks (oRAN) and 6G. AI will be an integral part of all these operations. In the world of managed security service providers (MSSPs), providers are looking for ways to expand their offerings to include these advanced technologies in a secure, automated platform to enterprise and SMB clients alike. Moreover, government at all levels is on high alert for cyber-attacks from bad actors of all stripes – from domestic and international cybercriminals to nation states. Executive orders and other policy initiatives have driven AI-powered security to the forefront, and in the year ahead, policymakers will aim to streamline regulatory hurdles to accelerate security transformation in the face of these looming threats.

Security at the Edge

Mobile edge computing offers a host of important benefits for telcos and their customers – which is to say, pretty much everyone with a cell phone. It provides lower latency, better connectivity and reliability, higher capacity, and more scalability. Edge computing is enabled by nodes connected to the central network that are physically closer to end users, which allows processing to occur at the edge instead of sending everything to the datacenter and back. Innovations like autonomous vehicles and growing IoT networks will rely on these networks to function. To realize the full benefits of this important technology, networks have to be secure-by-design, something existing IoT networks notoriously lack. Often, IoT networks run outdated firmware and weak security. They're difficult to update remotely, and often require manual, on-site intervention to make changes, which produces the gaps in security and lack of oversight that make them so vulnerable. In the age of AI, attackers have deployed a variety of sinister attacks that exploit this dynamic, including zero-click attacks, which do not require any user intervention at all to do damage. A single unprotected device at the hardware level can infect the whole network. As edge computing nodes proliferate, laying the groundwork for a level of connectivity that enables the innovations of tomorrow, the attack surface grows along with it.

In 2025, we'll see the focus on edge security and IoT security sharpen significantly. The investments telcos are making in edge computing to enable IoT networks are undermined severely by the relative weakness of IoT security. As more and more of our everyday data processing takes place at the edge, we can expect those that emphasize security to differentiate. That means deploying edge-based threat detection, so that threats are analyzed at the entry point to the network where they can be stopped, rather than traditional perimeter-based security, which sends traffic to the headquarters network for inspection. Implementing data minimization protocols like pre-processing at the edge will be important as well – AI enables us to perform basic analytics on data inputs before transmitting them across the network, reducing the likelihood that sensitive data from things like personal vehicles or medical IoT devices might be leaked. Solutions like zero trust network access, secure web gateways, firewalls-as-a-service, and cloud access security brokers will become table stakes for those that seek to drive the benefits of 5G and beyond.

The MSSP Connection

Managed security service providers are an essential part of the transformation taking place now and into 2025. It's clear now that no organization, no matter their size, is immune to cyberattacks. The largest enterprises and mom-and-pops alike can be extorted by ransomware gangs or frozen by DDoS attacks. MSSPs are looking for new ways to provide enterprise and SMB clients with the advanced offerings they'll need to do business in the modern threat environment. In the year ahead, the platform approach will dominate. The scale of the threat landscape demands a level of automation that can be delivered most efficiently as a service. While some enterprises will build proprietary networks and security, most organizations don't have the resources, or, crucially, the expertise to design these networks from the ground up, especially considering that most legacy networks that will serve as the foundation were not built with security as a primary consideration. Instead, MSSPs will offer advanced, secure-by-design programs that can be tailored to each organization's unique needs, relying on the platform approach to centralize the management of the network. This centralized management is crucial to effectively secure the diffuse networks and automated processing that will be the basis for more and more operations as time goes on. At the same time, this produces new revenue streams for MSSPs themselves.

Government on High Alert

We've seen attacks on government agencies by private and by state-sponsored groups for several years now. State-sponsored groups obviously have resources that enable them to engage in harmful offensive activity that others could not or would not. In some cases, profitability isn't a primary objective. In these cases, we see private enterprises, even SMBs, breached by foreign threats with a variety of goals, from intelligence-gathering to harming important economic enterprises. Attacks by private groups on utilities and other critical infrastructure, like the Colonial Pipeline attack, have demonstrated that far more damaging attacks are imminently possible. Government at all levels is on high alert for attacks on agencies, seaports, military and intelligence installations, and more from domestic and foreign bad actors alike. In the year ahead, we'll see an increased policy focus on cyber security. This will take the form of executive orders and other administrative actions to encourage the ethical use of AI, increased funding for cyber initiatives across the board, and, crucially, streamlined regulatory hurdles that will allow organizations to accelerate their AI-powered security roadmaps. The nexus between government and the private sector – both security providers and users – will be of foremost importance in 2025, with each segment playing a crucial role in securing networks for everyday citizens, important economic entities and industries, and critical infrastructure.

Security Drives Innovation

We've reached a point where no innovation is safe unless it is secure-by-design. The sophistication of attackers, amplified by AI tools that exponentially augment the attack surface and reduce the cost of offense for bad actors, virtually guarantees attacks where there's profit or geopolitical advantage in it, which puts organizations of all kinds at risk. To realize the promising innovations just on the horizon, and indeed beyond, networks will need to be secure-by-design. In 2025, this dynamic will become clear, as enterprises, service providers, and government alike set their priorities on building networks that are secure from the ground up.

About the Author

Bill Diaz is Vice President of Vertical Solution Business at Check Point Software

Bill is a Telecom Industry Executive with over 34 yrs of Sales, Account Management, Engineering, Operations, Delivery, Program Management and Relationship Building experiences with Senior Level Clients and Colleagues in both Domestic and International environments.

Mr. Diaz leads Check Point's Vertical Solutions Business Unit consisting of our Telco, Cable, Colo, MSSP and Public Sector (Fed/SLED) organizations. He manages a talented group of cyber security business, sales and technical professionals across the Canadian, United States and Latam Markets. He focuses on selling, delivering and supporting an E2E Security portfolio consisting of Cloud, Network, End Point, SASE and a robust set of Managed Services offerings.

Mr. Diaz has established, built, and scaled the business by 5X over the last 3.5 yrs with double digit growth during the last 24 months.

Bill can be reach at our company website: https://www.checkpoint.com/ and https://www.linkedin.com/in/william-a-diaz

Cyber Resilience Needs an Innovative Approach: Streamlining Incident Response for The Future

By Emre Tinaztepe, CEO & Founder Binalyze

As cyber threats continue to grow in complexity and frequency, organizations are being forced to rethink their approach to cyber resilience. Traditional methods, focused primarily on prevention and detection, are no longer enough. Today, it's not just about stopping an attack but ensuring that when a breach does occur, the response is swift, effective, and minimally disruptive to business operations. This calls for an innovative approach—one that streamlines incident response and turns it into a value-generating process rather than just a defensive manoeuvre.

The Flaws in Traditional Incident Response

Incident response has historically been a reactive process, often hampered by time-consuming manual procedures and a lack of historical and real-time visibility. When a breach is detected, security teams scramble to piece together what happened, often working with fragmented information from multiple sources. This approach is not only slow but also prone to errors, leading to extended downtime, increased costs, and sometimes, the loss of crucial data.

Moreover, the traditional incident response process tends to be siloed, with different teams handling different parts of the response. This lack of cohesion can result in miscommunication and delays—further exacerbating the impact of the breach.

The Need for an Innovative, Streamlined Approach

To truly enhance cyber resilience, SOC teams need to adopt a more streamlined, integrated approach to incident response. This new approach should prioritize speed, accuracy, and collaboration, ensuring that all aspects of a breach are handled in a unified manner. By automating key aspects of the investigation process, SOC analysts can play more of a role early on to significantly reduce the time it takes to analyze, investigate, and respond to threats.

Why Streamlined Incident Response Adds Value

1. **Speed and Efficiency**: The quicker an enterprise or MSSP organization can respond to an incident, the lower the risk of disruption and the less damage it incurs. An innovative approach that automates and streamlines the collection and analysis of data in near real-time during a breach allows security teams to quickly understand the scope and impact, enabling faster decision-making and minimizing downtime.
2. **Improved Accuracy**: Automation reduces the risk of human error, which is often a significant factor in traditional incident response processes - riddled with fragmented methodologies. By centralizing and correlating data from multiple sources, an automated investgation system provides a more accurate, consistent and comprehensive view of the incident, leading to better informed, more effective containment and remediation efforts.
3. **Cost Reduction**: Streamlining incident response with faster investigations not only saves time but also reduces costs associated with manual processes, extended downtime, potential fines from regulatory bodies, and impact of reputational damage. With a more efficient process, incident response teams can allocate resources more effectively, prevent burnout and reduce the financial impact of breaches.
4. **Scalability**: As businesses grow, so do their attack surfaces. A streamlined, automated approach to investigation and incident response can easily scale with the organization, ensuring that security remains robust even as complexity increases.
5. **Enhanced Compliance and Reporting**: With regulations becoming more stringent, the ability to quickly generate accurate reports on security incidents is critical. An innovative investigation and

incident response solution can automate the documentation process, ensuring compliance with industry regulations and standards.

A Future-Ready Approach to Incident Response

In the fast-evolving threat landscape and ever-changing environment, being able to respond to incidents with speed and precision is no longer a luxury—it's a necessity. Organizations that embrace this new, streamlined approach to automated investigation and response will not only enhance their cyber resilience but also turn security into a strategic asset that supports business continuity and growth.

For those looking to lead in this new era of cyber resilience, investing in innovative solutions that simplify and accelerate the incident investigation process is key.

About the Author

Emre Tinaztepe is the Founder and CEO of Binalyze. Before founding Binalyze, Emre worked in various positions at global endpoint security companies. His areas of expertise include Reverse Engineering, Malware Analysis, Driver Development, and Incident Response. He also led the development of an Anti-Malware suite used by millions of users to protect their devices against cyber-attacks, as well as teaching Malware Analysis and IR classes at TOBB university.

Emre can be reached via LinkedIn and at our company website www.binalyze.com

Discover how Binalyze AIR is revolutionizing incident response by streamlining and automating the investigation process for enterprises or MSSPs, ensuring any organization is ready for whatever comes next. Learn more here.

The Recoverability Factor: Four Key Trends in Data Recovery

By Stephen Young, Executive Director at Assurestor

The scale, frequency and cost of cyberattacks is well documented. But what's often overlooked in a seemingly never-ending cycle of prevention and protection are the nuances in what we call the 'recoverability factor'. This a company's readiness to respond and recover from a major data attack or other disaster.

Knowing that at some point your data – and potentially your whole business – will be threatened, focus shifts from security and prevention to recovery. The operational, financial and reputational implications can be catastrophic, so reducing the amount of data impacted and speed of recovering operational status then becomes the priority.

But the recovery phase can be chaotic and stressful, and there are no second chances to conceive a new disaster recovery strategy. Organisations must execute on the plan they have put in place. This is not the time to discover any shortcomings or failings. In some cases, experienced technical staff can work around a flawed or poorly thought-out plan, but it isn't something they have trained for – and to be fair shouldn't have to do.

An organisation's ability to recover systems and data is non-negotiable. There is no room for doubt – and if there is, any uncertainty needs to be identified and addressed before disaster strikes. But in a recent Assurestor survey, we discovered that rather than being fully prepared, senior IT professionals are not fully confident in their data recovery capabilities.

Here we look at some of the key trends coming out of the data.

Lack of confidence is an issue

The vast majority (78%) of our survey respondents admitted they had suffered data loss due to system failure, human error or a cyberattack at least once in the past 12 months. Yet only just over half (54%) are confident they could recover their data and mitigate downtime in a future disaster.

The fact that only just over half think their data is recoverable is concerning. How can your readiness for recoverability be reported confidently to the business and to senior stakeholders? Confidence comes from identifying an organisation's realistic needs, without compromising on cost or making sure you have the right tools for the job.

Data recovery on the business 'fitness agenda'

Survey respondents were clear in what they are lacking from the business in terms of disaster recovery planning, with 39% pointing to a lack of skills or expertise in-house, 29% to a lack of investment or budget, and 28% to a lack of senior support.

Recoverability is no longer a choice but must be part of a company's fitness agenda. Support from the top down is critical, as is sufficient funding to avoid fostering a culture of complacency. If those tasked with protecting the business in the event of system failure, a cyber-attack or human error do not feel that threats are taken seriously enough, then their approach and attitude may well reflect this.

Aligned with a thorough testing regime is the confidence to report that systems are recoverable, and the business is ready to respond. It also leads to a culture of professionalism about an aspect of IT that often sits in the shadows – until it's needed.

The testing 'gold standard'

Thoroughly and repeatedly testing systems and disaster recovery processes is non-negotiable. But one in five senior IT professionals say they test just once a year or less, while 60% of respondents check their data is fully recoverable and usable once every six months.

The testing 'gold standard' is twice-yearly, non-invasive full failover tests supported by monthly system boot tests and data integrity checks. As well as rigorous data validation, testing the ability of workloads (applications and data) for failover capabilities should be baked into the recovery plan. This should also allow for network and connectivity testing, an often-overlooked component in the testing process.

The challenge is that many technologies deployed to recover systems and data do not allow for non-disruptive testing. While testing can be carried out, these tests can never be thorough enough without significant disruption and, as a result, deliver a compromised test. Organisations need to put in place a well-structured recovery environment to optimise data recovery testing and ensure it can be conducted in the least disruptive way to the business.

Fail to plan, plan to fail

Two-thirds of respondents said they review and update their disaster recovery plans at least every six months. But there's risk it could fall down the priority list. Disaster recovery and data backup is a priority that all business functions should push for and be adapted to meet any newly identified requirements after frequent recovery testing.

As part of this planning process, you should ask two other important questions. First, what constitutes a 'disaster' today? The traditional image of fire, flood and acts of God is outdated. The increasing threat and sophistication of cyberattacks is the new reality. Second, how long can you afford to be down? Can you afford to lose any data without significant impact? Do some maths on what the cost of just one hour of downtime would be. Without this visibility your recovery plan may be flawed.

About the Author

Stephen Young, Executive Director at Assurestor is **a** seasoned business owner and entrepreneur, innovation in technology has been central to Stephen's career for over 30 years.

Across varying facets of IT, Stephen's experience covers infrastructure, software development, datacentres, service and support, IT governance combined with management, finance and business development. With roots in software development and service and support, Stephen's commitment to detail, thoroughness and uncompromising customer support has been a continuous thread through his businesses and has been a major factor to their success.

Stephen can be reached online at **https://www.linkedin.com/in/stephenyoung996/** and at our company website: https://www.assurestor.com/

A Switch (Back) To On-Prem Solutions to Maximize Control & Security

By Itay Glick, VP of Products, OPSWAT

As organizations reassess their data security strategies at year end, many are considering moving from cloud services to on-prem solutions to gain greater control over their data and mitigate the risks associated with cloud vulnerabilities. Following many high-profile breaches in 2024 and the theft of customer data from multi-cloud data warehousing platforms, malicious attackers continue to exploit weaknesses in cloud infrastructure.

The widespread breaches and resulting data exposures have sparked concern in many industries, particularly for organizations that deliver the critical infrastructure the nation relies on. To mitigate the risk of exposure through cloud service attacks, organizations will reconsider their infrastructure and deployment strategies in the year ahead to improve their security posture, reduce reliance on third-party providers, and better align with compliance requirements.

The Trend Towards On-Prem Deployment

Multiple high-profile breaches in 2024 affected cloud-based services, allowing attackers to gain access to thousands of organizations and more than 100 million individuals. By compromising a cloud service, malicious actors can compromise customer instances and use stolen customer credentials to exfiltrate valuable data. Although some vulnerabilities can both be exploited on-prem and in the cloud, it's also clear that cloud vulnerabilities are frequently exploited at scale. These high-profile breaches have led many organizations to reassess their infrastructure strategies.

In response, security teams in various industries, particularly those handling sensitive data, are considering moving to on-prem deployments. This would minimize the risk from cloud weaknesses, including vulnerabilities, stolen credentials, misconfigurations, insecure APIs and interfaces, poor identity and access management (IAM), data exposure, and lack of control across a complex and increasingly interconnected ecosystem. While returning to on-prem systems requires an investment in hardware and in-house knowledge, it also offers several advantages. On-prem deployments enable teams to:

- Maintain operations independent of internet connectivity and minimize reliance on 3rd party vendors
- Provide enhanced security capabilities in an air-gapped environment
- Monitor operations in real-time with greater visibility and minimal latency
- Create and implement redundant systems and failover mechanisms on-site

These benefits make on-prem solutions an attractive option for organizations prioritizing data control and security.

On-Prem Offers Enhanced Data Control

Unlike the shared responsibility models offered by cloud providers, on-prem deployment gives organizations complete ownership of their environment. This approach provides in-house security teams with direct access to stored data. As a result, they can implement custom security measures tailored to the specific needs of their organization, minimizing the risk of breaches and unauthorized access. On-prem deployment also offers greater flexibility in managing configurations, updates, and data storage, aligning with internal policies, complex regulatory requirements, and industry-specific standards.

Despite these advantages, on-prem solutions do require significant investment in hardware and maintenance. However, these investments may be offset by potential savings. For example, according to IBM's Cost of a Data Breach Report 2024, public cloud breaches averaged $5.17 million, while on-prem breaches were the least expensive at $4.18 million on average.

Regulatory Alignment

While cloud solutions offer scalability and reduced upfront costs, on-prem deployment provides several unique advantages for regulatory compliance. On-prem deployment may simplify compliance with industry-specific regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the General Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI-DSS). Keeping all data stored within the organization's own servers, often in an air-gapped environment, may make compliance simpler. For instance, healthcare organizations can more easily implement the physical safeguards required by HIPAA when data is stored on-site. This option also provides increased data privacy, because sensitive information remains within the company's physical location, rather than being stored in a potentially poorly secured cloud offering.

And while returning to on-prem requires organizations to purchase hardware and manage it in-house, security teams also then gain full control over it. This enables them to customize the hardware and security controls to their unique needs and make upgrades as needed, with full visibility into changes in the environment. Along the same lines, on-prem deployment reduces dependency on external providers, which minimizes third-party risk and may even improve operational continuity when third-party services are disrupted by breaches or other unexpected events. A few key benefits of on-prem deployment for security and compliance teams include:

- Easier adherence to industry-specific regulations
- Greater control over data storage locations, helping teams meet diverse data sovereignty requirements
- Simpler to maintain audit trails and implement specialized compliance measures

These benefits make on-prem deployment particularly attractive for organizations in highly regulated industries or those handling sensitive data, providing the control and security necessary to meet specific compliance requirements.

Time to Switch Back

While cloud-first approaches have dominated the past decade, expect many organizations to start moving back towards on-prem deployments in 2025. For organizations operating in critical infrastructure sectors, this path is particularly compelling. The sensitive nature of their operations, combined with the increasing infiltration of nation-state actors in critical infrastructure, will drive these organizations to move away from cloud-first deployments to regain complete control of their environments.

About the Author

Itay Glick serves as Vice President of Products at OPSWAT and brings more than 17 years of executive management experience in cybersecurity at global technology companies based in the U.S., Europe, and Asia. Before OPSWAT, he served as AVP of network and cloud security at Allot, and before that, founded his own company and played a key role in managing the development of equipment for the lawful interception market on behalf of Verint Systems. Itay launched his career as a software engineer in an elite intelligence unit of the Israel Defense Forces. He holds an M.B.A. from Bar-Ilan University and a B.Sc. in electrical engineering from the Technion – Israel Institute of Technology. Itay can be found on LinkedIn here.

Top Kubernetes Threats in 2024 And How Amazon EKS Mitigates Them

By Riddhesh Ganatra, Founder, Code B Solutions

Introduction to Kubernetes and Amazon EKS

As a key technology for container orchestration, Kubernetes has been widely used in many industries to effectively manage and deploy applications.

But its increasing popularity has also made it a prime target for cyberattacks. A managed Kubernetes solution, Amazon Elastic Kubernetes Service (EKS), makes Kubernetes administration easier and offers resources to improve workload and infrastructure security.

Amazon EKS stands out for its capacity to handle contemporary threats while integrating easily with AWS's security ecosystem, which is important for businesses to prioritize cybersecurity in 2024.

The Role of Amazon EKS in Cybersecurity

By fusing AWS security solutions with native Kubernetes features, EKS guarantees a secure Kubernetes environment.

This combination gives enterprises the ability to put in place layered security measures, such as network isolation, encryption, and access control.

For instance, a financial company utilizing EKS might use IAM policies to limit access to sensitive resources and encrypt Kubernetes secrets to protect client data. Similar to this, a healthcare provider might use EKS's network controls and private API endpoints to secure patient records.

Because of these features, Amazon EKS is a dependable option for upholding secure operations in increasingly intricate cloud-native settings.

Key Kubernetes Threats in 2024

1. Misconfigured Access Control

Inadequate role-based access control (RBAC) settings can allow unauthorized users or applications to access sensitive data or services.

How EKS Mitigates This Threat:

- EKS integrates with AWS Identity and Access Management (IAM) to ensure fine-grained access control over Kubernetes resources.
- It supports defining RBAC policies that limit access based on user roles and namespaces.
- Tools like AWS Security Hub can be used to monitor access configurations for vulnerabilities continuously.

2. Supply Chain Attacks

Container images sourced from third-party registries may contain malicious code or vulnerabilities.

How EKS Mitigates This Threat:

- Amazon ECR (Elastic Container Registry) integrates with EKS to store and scan container images for vulnerabilities before deployment.
- EKS can enforce policies to ensure that only signed and verified container images are used in production.

3. Insecure API Endpoints

Exposed Kubernetes API servers can be exploited for unauthorized access and lateral movement within the cluster.

How EKS Mitigates This Threat:

- EKS allows clusters to be configured with private API endpoints, ensuring they are only accessible from within the VPC.
- Network Access Control Lists (NACLs) and security groups can further restrict access to specific IPs or subnets.

4. Runtime Threats to Containers

Once a container is running, application code or base image vulnerabilities can be exploited to execute malicious activities.

How EKS Mitigates This Threat:

- Integration with Amazon GuardDuty enables continuous monitoring of suspicious activity in running containers.
- Tools like AWS Inspector can scan running workloads for known vulnerabilities and misconfigurations.
- Pod security policies (PSPs) can be enforced to restrict the permissions granted to containers, such as blocking privilege escalation.

5. Data Exfiltration

Compromised pods or misconfigured storage can lead to the unauthorized transfer of sensitive data.

How EKS Mitigates This Threat:

- EKS supports encryption of data at rest and in transit using AWS Key Management Service (KMS).
- Kubernetes network policies can be used to restrict pod-to-pod and pod-to-service communication, minimizing the risk of data leakage.
- Amazon VPC Flow Logs can monitor and analyze network traffic to detect anomalies.

6. Distributed Denial of Service (DDoS) Attacks

Kubernetes clusters exposed to the internet can be targeted by DDoS attacks, disrupting application availability.

How EKS Mitigates This Threat:

- AWS Shield and AWS Web Application Firewall (WAF) can protect applications running in EKS from DDoS attacks.
- EKS allows for auto-scaling, enabling the cluster to handle increased traffic during attacks while maintaining service availability.

Conclusion

In 2024, as Kubernetes continues to underpin cloud-native deployments, securing clusters against modern threats is critical.

Amazon EKS provides a stronghold for building a secure Kubernetes environment by combining AWS security features with Kubernetes-native capabilities.

By addressing threats such as misconfigured access, supply chain vulnerabilities, and runtime risks, EKS empowers organizations to operate securely in an evolving threat landscape.

Implementing Amazon EKS with a focus on cybersecurity can be a strategic step toward safeguarding modern applications and ensuring compliance with emerging security standards.

About the Author

Riddhesh Ganatra is a Founder at Code B Solutions Pvt. Ltd. Code B offers expert services for custom web and mobile app development, cloud computing, and DevOps consulting solutions. Our company agenda is to help clients bridge the execution gap with end-to-end technology planning, implementation, and management.

Navigating Cyber Security Implementation Challenges in SMBs

By Anwar Manha, Head of IT Security & Infrastructure, Alabbar Enterprises

Cyber Security is often low priority for SMBs. Many SMBs lack dedicated security specialist; instead, security responsibilities are typically handled by IT department which is already overwhelmed with general IT support tasks and a firefighting approach. implementing new security controls on this environment is always challenging, most of the organization see it as an IT/Security department project rather than it's a business project. When trying to implement new security program or controls it is important to consider common roadblock and their solutions in the context of SMBs, following are the most common obstacles and their solutions when implementing cybersecurity practices in an SMB.

1. Security Culture

Most SMB lack the security culture, many organizations has very loose policies on security, and employees are not well aware of the security implications of their actions. educating the end users on importance of cyber security should be the utmost priority. Without this You can spend hundreds of thousands of dollars and still have a weak system. Every employee should understand the role they play to protecting the organization. Leadership team should demonstrate the commitment to security by leading through example

2. Monitoring and Optimization

Security implementations are not a one-time task, it's an ongoing process, continuous monitoring and optimization of security controls are crucial for the success of security programs. Threat landscape are changing rapidly, so a onetime task become outdated quickly. Security postures and risks are always a point in time. Regular audit and assessment should be performed on the implemented security controls. It is also important to conduct the root cause analysis after incidents to prevent future breaches and refine security controls

3. Compensatory Security controls

In order to cop up with SMB business flexibility and requirements, its always to have compensatory security controls, there may be a situation where flexible approach is needed to balance the business requirements and security needs. This will ensure risks are mitigated when standard security controls are not feasible due to the operational limitation and this must be signed and approved by stake holders to avoid any future dispute. It is important to refine and asses compensatory control timely to ensure these controls are remain effective

4. Compliance and Legal

Many SMBs lack specialised legal department, and are unaware of compliance and regulatory requirements of the industry they are in, such as data protection and privacy laws. which is often overlooked. SMBs wake up from this when they get fined or involved in a legal issue. This is should be one of the top most priority in every security programs. These challenges can be addressed by Understanding local and global authority regulations, standards and guidelines. Or consult with an expert who can lay the foundation. conducting a routine compliance audit and implementing automated tools can help adhere with the regulations.

5. Risk Management

by introducing a security program SMB can minimize the chance of being compromised, but not completely out of the risk, the remaining risk after the security control implementation should be managed appropriately. SMB can follow the standard risk management practices by adopting the following action for the risks, Avoid the risk, mitigate the risk, transfer the risk or accept the risk and it should be signed by senior stake holders to ensure clarity and alignment

Additionally, SMBs should conduct regular risk assessments to identify new vulnerabilities and threats. Continuous monitoring and improvement of the security program are essential to address emerging risks effectively. Educating employees about cybersecurity best practices plays a crucial role in reducing human error as a potential threat vector. Collaborating with third-party experts can enhance the organization's ability to mitigate complex risks. Finally, SMBs should ensure their incident response plan is well-documented and regularly tested to respond effectively in case of a security breach. The success of security programs in SMB is always depend the senior management support and employee's active contribution.

About the Author

Anwar Manha, Head of IT Security & Infrastructure, Alabbar Enterprises. He is a seasoned IT leader who can design, implement, and manage complex IT systems, infrastructure, and security solutions across multiple domains. Currently, he works as an IT Manager at Alabbar Enterprises, a leading conglomerate in the GCC with diverse businesses in retail, food & beverage, and design.

At Alabbar Enterprises, he oversees and leads the IT infrastructure, IT security, IT operations, and strategic planning, ensuring the alignment of IT with business objectives and compliance with best practices and standards. He also leads cyber security initiatives, conducting risk analysis, implementing security policies and procedures, and providing security awareness and training.

Anwar Manha can be reached online at anwarmanha@yahoo.co.in

The Rise Of AI-Powered Cyber Threats: How Adversaries Are Using “Good Enough” Tactics to Outsmart Defenders

By Aaron Shaha, Chief Threat Research and Intelligence at Blackpoint Cyber

As we move into 2025, organizations are laser-focused on maximizing resources and achieving better business outcomes. Increasingly, this translates into leveraging AI and automation to streamline operations, improve efficiency, and enhance cybersecurity efforts. While we’re not on the brink of AI achieving sentience, its role in cybersecurity is undeniable—particularly in automating repetitive, time-consuming tasks.

However, the same tools that empower defenders can be easily weaponized by adversaries, leading to a heightened and more complex threat landscape. Cybercriminals are adept at exploiting AI's capabilities, applying timeless strategic principles like the one articulated by General George S. Patton: “A good solution applied with vigor now is better than a perfect solution applied ten minutes later.” This mindset is evident in the rise of identity-based attacks, where attackers prioritize effectiveness over sophistication, using breached credentials and straightforward techniques rather than investing in costly, intricate exploits.

The Rising Threat of Infostealers

One prominent trend in the cyber threat landscape is the widespread use of infostealers. These easily deployable tools are often distributed via malvertisements and other common delivery methods. Despite their simplicity, infostealers pose a significant threat due to their ability to harvest massive amounts of sensitive data efficiently.

When combined with AI, the implications become even more alarming. AI allows adversaries to analyze and operationalize the data harvested by infostealers at scale. For instance, attackers can automate the validation of credentials across multiple platforms, streamlining account takeovers. This fusion of automation and data-driven targeting increases the success rate of attacks and accelerates their execution.

The growing dependence on identity-based attacks underscores why credentials remain a prime target. Unlike advanced exploits that require deep technical expertise and substantial resources, credential-stuffing attacks rely on readily available information—breached passwords—to achieve their objectives quickly and effectively.

AI-Driven Social Engineering

The threat doesn’t stop with credentials. AI is amplifying the sophistication of social engineering attacks, making them harder to detect and more convincing. Cybercriminals now have access to the same cloud-based or standalone AI tools that cybersecurity teams rely on. These tools can ingest vast amounts of publicly available data—from social media posts to corporate websites—and generate hyper-personalized phishing campaigns.

Consider a scenario where AI that is trained on a target's online activity crafts a phishing email tailored to their recent social media interactions. Worse yet, imagine receiving a phone call that sounds like your CEO, thanks to AI-powered voice cloning. This level of authenticity in attack vectors represents a significant evolution in cybercriminal tactics.

Even the most basic social engineering scams—such as SMS messages from a “CEO” requesting gift cards—remain alarmingly effective. With AI enhancing these tactics, attackers can scale operations while maintaining a layer of legitimacy that was previously difficult to achieve.

Identity at the Center of the Storm

The convergence of traditional hacking techniques with identity-based attacks is another concerning trend. Once attackers gain access to enterprise systems—such as Office 365—they can exploit tools like the Microsoft Graph API for persistence, lateral movement, and data exfiltration. While some methods, such as setting up mailbox forwarding rules, are straightforward, others involve sophisticated maneuvers that evade detection.

Although technologies like passkeys and hardware-based authentication offer promising solutions for mitigating identity-related threats, widespread adoption remains challenging. Implementation complexity, cost considerations, and user resistance hinder the broader deployment of these advanced authentication methods, leaving gaps for attackers to exploit.

Preparing for 2025: A Dynamic Landscape

As we approach 2025, the intersection of AI, automation, and cybercrime presents a dual-edged sword. On one side, defenders can access powerful tools to detect and mitigate threats. On the other hand, adversaries are leveraging those same tools to scale operations, refine tactics, and enhance their success rates.

The challenge lies in staying ahead of the curve. Cybersecurity teams must prioritize resilience, focusing on proactive strategies to counter AI-driven threats. This includes:

- Enhanced training to recognize sophisticated phishing and social engineering attempts.
- Adopting robust identity protection measures, such as multi-factor authentication (MFA) and zero-trust architectures.
- Investing in AI-driven defense mechanisms capable of identifying and neutralizing threats before they escalate.

In 2025, even "simple" attacks could have huge consequences due to the amplification power of AI. As defenders, we must anticipate these emerging trends and build robust systems to mitigate their impact. The cybersecurity landscape is evolving rapidly, and only those prepared to adapt will successfully navigate the challenges ahead.

By embracing a proactive and adaptive mindset, we can ensure that AI and automation serve as defense tools rather than exploitation avenues.

About the Author

Aaron Shaha is Chief of Threat Research and Intelligence at Blackpoint Cyber. He is a Strategic Information Security Executive and subject matter expert with a record of pioneering cyber security trends by developing novel security tools and techniques that align with corporate objectives. Known for building and leading strong teams that provide technology enabled business solutions for start-ups, industry leaders (Deloitte and its Fortune clients) and government agencies (NSA). Skilled at developing information security strategies and standards, leading threat detection and incident response teams to mitigate risk, and communicating effectively across all levels of an organization.

Aaron can be reached online at www.linkedin.com/in/aaronshaha and at our company website www.blackpoingcyber.com

2025 Cybersecurity Trends and Predictions: Adapting To An Era Of Evolving Threads And Technology

By Julien Richard, VP of InfoSec at Lastwall

All organizations today rely on technology. Whether you're a small non-profit, a government agency, a hospital, or a traditional business, digital tools power everything from communications to service delivery to data management. This dependency means that every organization, regardless of its mission or sector, faces cyber risks.

For organizations heading into 2025, these cybersecurity challenges are both a pressing concern and a strategic priority. As we look toward the future, organizations must prepare for both established and emerging threats. 2025 represents another step in the ongoing evolution of cybersecurity, where vigilance against both familiar and emerging threats remains crucial.

Evolution of Threat Actors & Attack Methods

To understand these emerging threats, we need to examine how attackers and their methods are changing. State-sponsored actors are becoming increasingly specialized while significantly escalating their operations. Evidence shows a clear increase in both the frequency and scale of their attacks, and these teams will continue developing their capabilities. Their growing collaboration with criminal groups creates a powerful combination of state resources and criminal expertise. This surge in state-sponsored cyber operations, occurring against a backdrop of rising global tensions, presents an increasingly dangerous threat to organizations worldwide.

The criminal world has evolved into a sophisticated ecosystem, particularly in ransomware operations. Different groups now specialize in specific aspects of an attack - some focus solely on gaining initial access to networks, while others purchase this access to deploy ransomware. These criminal groups will continue developing their tactics, building on strategies of data encryption, theft, and leaks. Where they once avoided targeting critical infrastructure for fear of consequences, they've grown increasingly bold in attacking hospitals, food supply, and other essential services. This trend will likely persist as attackers show less concern about drawing attention from law enforcement.

Technology Transitions & Security Challenges

As with previous years, 2025 will bring major technology advancements that introduce new security headaches. The Windows 10 end-of-life (EOL) situation demonstrates this well - unlike previous upgrades, organizations face more than just a software update. Many computers simply can't run Windows 11 due to hardware requirements, leaving companies with tough choices: replace working hardware, keep running unsupported systems, or find alternative solutions. These vulnerable systems become prime targets for information-stealing malware, designed to harvest credentials and provide attackers with initial access to networks.

Compounding these risks, the speed of attacks continues to increase. The time between a vulnerability being discovered and being exploited is shrinking from weeks to days, sometimes even hours. While large organizations remain prime targets, attackers are increasingly focusing on smaller vendors and previously overlooked systems. This shift is no accident - automated scanning tools make it easy to identify vulnerable systems across the internet, and attackers have found that targeting smaller operations requires less effort while still generating significant returns.

Moreover, modern networks mean these threats can spread quickly through connected systems. A security gap in one area - like an outdated operating system or an unpatched application - can give attackers access to an entire network. For smaller vendors, the notion of being "too small to target" is no longer a viable defense strategy. If your system is vulnerable, it will be discovered.

Emerging Technologies: Reality vs. Hype

In the coming years, AI adoption will enter a more mature phase across all sectors. Organizations are expected to move beyond initial experiments towards implementing more practical, targeted applications for AI in their operations. This shift will lead to a more balanced approach - AI will likely become a powerful tool for security teams, while remaining a complement to human expertise rather than a replacement.

Both defenders and attackers are finding practical uses for AI. Security teams are using it to spot unusual patterns and respond to threats faster, while attackers are using it to find system weaknesses and automate their attacks. As AI tools get better at discovering vulnerabilities, we're seeing a new kind of arms race between ethical security researchers and malicious actors.

Looking ahead, quantum computing poses a unique challenge. Although practical quantum computers aren't here yet, the timeline for their development remains uncertain. When quantum computing does mature, current security methods that protect sensitive data and communications could become vulnerable. This uncertainty is why forward-thinking companies are already investigating "post-quantum" encryption. Given the complexity of encryption systems, implementing and maintaining them requires significant effort, making it crucial for organizations to start planning now to assess the potential impact and prepare their security infrastructure for the future.

Data Security in a New Era

Traditional data breaches will remain a major threat, but their impact continues to evolve. Beyond immediate financial losses, organizations must now consider how stolen data might be used in future attacks. Customer information, intellectual property, and business communications remain valuable targets, with breaches potentially causing cascading effects throughout an organization's operations.

As companies feed more information into AI systems and build larger data lakes, they're creating additional targets for attackers. The risk isn't just about data theft anymore - it's about how stolen information could be used to train malicious AI models or manipulate legitimate ones. When employees use AI tools to process business data, they may inadvertently expose sensitive information. Organizations must carefully balance the productivity gains of AI tools with the potential risks of data exposure.

We anticipate more sophisticated attacks targeting both traditional data stores and new AI systems. Attackers might focus on poisoning data sets, manipulating AI training data, or exploiting the connections between different data sources. The ripple effects of a data breach in 2025 could extend far beyond the immediate exposure of sensitive information, particularly as attackers combine traditional breach tactics with innovative ways to monetize stolen data.

External Factors Shaping Cybersecurity in 2025

The cybersecurity landscape for 2025 is influenced by more than just technology. As cryptocurrency values rise, we see two major impacts: First, the stockpiles of digital currency that threat actors have accumulated through past ransoms and attacks become more valuable, giving them more resources to fund new tools, recruit talent, and launch sophisticated campaigns. Second, as cryptocurrency valuations rise, the assets themselves become prime targets, driving a surge in attacks on crypto wallets, exchanges, and blockchain systems.

The incoming U.S. administration's policies suggest a shift away from cybersecurity priorities. With key agencies facing potential funding reductions and fewer security-focused initiatives, organizations might receive less guidance and support in addressing cyber risks. This shift in government priorities comes at a time when cyber threats continue to grow more sophisticated.

Looking Ahead

The cybersecurity challenges of 2025 will likely combine familiar threats with new complexities. Technology transitions like Windows 10's end-of-life, alongside evolving tactics from both state-sponsored actors and cybercriminals, will create new security challenges for organizations to navigate. AI will take on a more practical role in both attack and defense, while the timeline for quantum computing remains uncertain but important to watch.

Data breaches will continue to evolve, affecting both traditional systems and new AI-powered tools. External factors, such as cryptocurrency fluctuations and geopolitical shifts, will continue to shape the threat environment in ways that technical solutions alone can't address.

While predicting specific threats in such a dynamic field is difficult, one thing is clear: cybersecurity in 2025 will demand that organizations remain informed, agile, and prepared for rapid change. Amid these emerging challenges, the foundational principles of security - like patch management, access control, adequate cryptographic controls, and security awareness - remain as crucial as ever in preventing successful attacks.

About Julien Richard

Julien has been battling cyber threats for over 20 years and currently serves as the VP of InfoSec at Lastwall. The holder of multiple certifications (OSCP, CISSP, CRISC, CRTP, and more), he has tackled everything from provincial governments to online casinos and has been a key player in building security teams/programs from the ground up at different companies.

As a passionate Security Researcher, Julien is committed to responsible disclosure and the protection of good-faith security research. He has shared his insights at various infosec events, is the founder of the Atlantic Cybersecurity Collective, the organiser of the Policy Village at BSides Ottawa, and sits on the advisory board of the Canadian Cybersecurity Network.

Julien can be reach on LinkedIn here.

The Intersection of Digital Credit Solutions and Cybersecurity: Protecting Consumer Data in the Automotive Finance Industry

Safeguarding Financial Data: Cybersecurity Strategies for Modern Auto Lending Platforms

By Pete MacInnis, CEO, eLend Solutions

Digital credit solutions deliver convenience, speed, and flexibility. Along with its benefits, however, comes risk. Protecting consumer data has always been a priority for dealerships. It's now a more complex initiative as cyberattacks in the industry increase due to more sophisticated hackers.

Automotive finance stands at a crucial point. You want to increase your lead-to-sales ratio, reduce friction in the process, adhere to the FTC (Federal Trade Commission) Safeguards Rule, and apply the best cyber protections. There are learnings to take from known breaches and proactive plans you can make to achieve these objectives.

The State of Data Breaches and Cyber Threats in the Automotive Industry

The automotive industry is under attack by opportunistic cybercriminals. They target these businesses because of the extensive amount of PII (personally identifiable information) available. Customers who go through a credit pull now have their PII within databases and platforms.

Unfortunately, this PII isn't always as secure as it should be. Hackers are always looking for easy ways to infiltrate a network, and they are finding success.

One of the biggest stories of automotive cybersecurity was the CDK attack. It was a ransomware incident. Hackers took control of the entire platform, causing disruptions across dealerships, from sales to service operations to loan processing. In all, it impacted over 15,000 businesses.

This incident wasn't a direct attack on dealerships. It was a side-door approach of breaching a vendor to get to all the valuable PII. It's one example of a growing trend of ransomware, which has cost the industry over $920 billion since 2021.

A favorite mechanism to enact ransomware or malware is phishing. Cybercriminals have found success here, as well. Research concluded that 36% of dealership data breaches started with a phishing attack.

The auto industry has a target on its back, and most in the industry feel unprepared to battle these threats. A cybersecurity study by eLend revealed that only 42% of dealers feel prepared to manage a breach.

What does your dealership need to do to be prepared? It's vital since the probability of one keeps increasing.

Dealership Best Practices to Safeguard Consumer Data

Cybersecurity, as an operational initiative, continues to try to stay a step ahead of hackers. It's a volatile environment because what worked today may no longer do so tomorrow. Adapting to cyber-criminal techniques is an ongoing strategy.

Your best defense is actually a strong offense. The protocols to put in place include:

- **Encryption**: Whether PII is in transit or at rest, it should always be encrypted. One challenge you may find is that legacy systems don't offer this. If that's the case for you to achieve this cybersecurity best practice, you may need to update your tech stack.
- **Secure data storage**: Your databases are ripe with PII, and this data needs to be in a "digital vault." It includes regular backups of this sensitive data offside or in a cloud environment. You should also test the integrity of these storage mechanisms often.
- **Security auditing**: The two most important auditing tactics to perform regularly are vulnerability assessments and penetration testing. Conducting these should identify weaknesses, misconfigurations, or other security concerns. From these findings, you can take action to fix them before hackers exploit them.
- **Employee training**: Your staff can be your weakest link or strongest ally. Recall that many breaches result from phishing, which means there was a human element to the incident. Regular and consistent cybersecurity training for employees is crucial in preventing successful phishing.

All of these components are internal safeguards. Dealerships must also address consumer awareness around data privacy issues.

Consumers Become More Aware of Data Privacy and Expect Transparency

It would be hard for the average consumer to be unaware of data privacy and security. Headlines of breaches come almost daily, and 37% of U.S. adults said they received a notification of a breach in 2023. As a result, 73% are more concerned about data privacy than they were a few years ago.

With awareness comes doubts about the security of businesses and their use of consumer data. Dealerships provide the required disclosures about data use, but it doesn't hurt to explain those in simple terms. Doing so offers greater transparency over how dealers collect and use consumer data.

In fact, doing this could be another way to build trust and loyalty. In considering other ways to strengthen data privacy and security, you can look to other industries that are more mature in their cybersecurity journey.

What the Auto Industry Can Learn from Finance and Healthcare

Finance and healthcare are two of the most regulated industries, and they generate, use, store, and analyze lots of consumer data. Cyber criminals are constantly trying to breach these organizations for PII and PHI (protected health information).

Both have layers of protection, but they aren't immune to attacks. What they do have are frameworks, protocols, and laws that govern how they must treat consumer data. The auto industry does have to adhere to regulations like the Safeguards Rule and PCI-DSS (Payment Card Industry Data Security Standard).

There's much to learn from finance and healthcare since they've been early adopters of innovative cybersecurity practices. The auto industry has things in play but could fortify them for even better protections, including:

- **Stricter protocols for consumer data sharing**: This is important because you have to send PII to other systems for credit pulls and lender qualification.
- **Access controls on top of encryption**: Instituting and continuing to improve access controls helps you comply with the GLBA (Gramm-Leach-Bliley Act) while also working to prevent unauthorized access.
- **Managing third-party vendors**: The software you use could put you at risk, as demonstrated by the CDK attack. Vetting your vendors based on their cybersecurity and data privacy initiatives would be a good practice to establish.

By being security first, you have the opportunity to make this a differentiator. Consumers have reason to be distrustful about sharing PII since they've likely experienced a breach that included their data.

Prioritizing security and privacy could be a trust builder with consumers who will be less hesitant to use digital credit solutions. Emphasizing how you protect their information could be good for business and industry growth.

There are more considerations for building a cyber-secure digital credit solution. Innovations in Digital Credit Cybersecurity

Innovation is building secure digital credit solutions that can adapt to new threats. The most promising are AI (artificial intelligence) and machine learning. There is great potential for this technology to revolutionize digital credit cybersecurity.

Using AI to analyze real-time data for threats is becoming a common practice. It can identify patterns that cause concern. It helps you take action immediately instead of after a breach has occurred.

In addition to exterior threats, AI could be a tool to find insider threats. It could look at transactions or activities by your staff if they don't follow the rules.

AI can also play a part in protecting data storage, specifically the cloud. AI, as a monitoring tool within the cloud, can uncover anything that seems abnormal or suspicious.

If AI locates a threat, it could be the first response to deflect low-risk threats. Another possibility is AI delivering useful advice to security professionals on what actions to take.

Machine learning, a subset of AI, can be valuable in your cybersecurity plans, as well. Machine learning algorithms have the capacity to review massive amounts of data quickly. The outcome is the ability to detect and predict security issues.

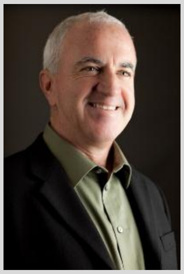
Embracing this innovation allows dealerships to scale cybersecurity measures, take advantage of intelligent automation, and stay ahead of attacks.

Achieving Proactive Consumer Data Protection

With these best practices, learnings from other industries, and new innovations, dealerships have a collection of tools to protect consumer data. However, threats evolve, so you must, as well.

You'll never be 100% risk free, but you can be consistent and continuously enhance your cybersecurity program. These efforts are worth it, as they work to protect your reputation and your operational framework. Stay informed, vigilant, and ready to pivot at the intersection of cybersecurity and digital credit solutions.

About the Author



Pete brings 40+ years of experience in Automotive Finance and Technology as Founder and CEO of eLEND Solutions™, an automotive FinTech company providing a middleware solution designed to power transactional digital retailing buying experiences. The platform specializes in hybrid credit report, identity verification, and 'pre-desking' solutions, accelerating end-to-end purchase experiences - helping dealers sell more cars! Faster!

Best Practices and Risks Considerations in Automation like LCNC and RPA

By Jordan Bonagura, Senior Security Consultant at Secure Ideas

Technologies such as **Low-Code/No-Code (LCNC) and Robotic Process Automation (RPA)** have become fundamental in the digital transformation of companies. They continue to evolve and redefine software development, providing new possibilities for different organizations. It allows users with no programming experience (citizen developers) to create applications and automate processes, simplifying complex tasks and optimizing business operations.

Application platforms for these technologies offer intuitive visual interfaces. These allow anyone, from a business professional to an IT employee, to develop customized applications and automate repetitive processes quickly and efficiently.

Despite their advantages, the use of these technologies has challenges, especially regarding information security. These platforms, which aim to simplify and speed up development, can introduce risks related to controlling and protecting corporate data. The agility these tools provide tends to reduce development time and costs compared to traditional models significantly. However, the lack of centralized control, especially in environments where non-technical teams are free to create applications, can generate vulnerabilities and ultimately lead to higher costs.

After conducting several penetration tests and risk assessments in environments using LCNC, RPA, or other forms of automation, I thought it crucial to offer more detailed security considerations for these technologies. Companies must understand the potential risks and impacts that adopting these solutions can bring, ensuring that the benefits of automation do not compromise security and regulatory compliance.

A common use of LCNC and RPA is related to automating data retrieval processes, a technique known as scraping. In many of the instances, I have observed these tools scraping data from both internal environments (such as corporate databases) and external ones (API sites, among others). Based on this data, the automated "robot" makes decisions, following the configured workflow, such as carrying out new searches, saving information in files or databases, sending emails, generating alerts, etc.

Although scraping is a widely used data collection practice, it can have legal implications, so I recommend that companies consult their legal or risk management department.

As you can imagine, this external dependence can become an absolute nightmare, especially when the organization has no direct control over these services. If the way the data is made available changes unexpectedly, whether the data host alters the addressing, data format, presentation, or removes the data completely, the automation can become vulnerable to critical failures. This external dependency makes the problem even worse if the automation process is based on this data - unavailability can generate errors and allow the "robot" to continue executing the process with incorrect data in a more critical scenario. This can result in damaging actions, such as wrong decisions in sensitive financial or operational processes, potentially severely impacting the organization. Mishandled failures in the automation can also lead to organizational decisions being made with outdated data, or the loss of data by overwriting good records with bad ones.

Therefore, solutions developed with automation must be designed to deal robustly with data unavailability. Automation must be able to detect and handle these scenarios, including the appropriate use of exception and error handling. This will ensure that even when data sources fail, the system can behave safely and predictably, preventing further damage.

Another crucial point, especially in organizations where the developers of LCNC solutions often lack formal programming experience, is the need to establish internal policies that guarantee the auditing and traceability of automated processes. A best practice is to implement detailed logs of all automation steps. Recording this information will not only allow the IT team or those responsible for security to investigate and correct any faults but will also be essential in resolving future problems, guaranteeing greater transparency and control over automated processes.

By default, automation processes are run by a specific user account, meaning they are directly linked to the permissions and privileges associated with that account. This is a critical point and must be constantly monitored to avoid risks. In this context, the recommendation to adopt the principle of least privilege is fundamental: to grant the user only the minimum level of permissions necessary to carry out their task. This limits access privileges and helps mitigate the impact if the account is compromised.

In the case of organizations that use automation processes involving scripts and command execution, such as CMD, Python, VBScript, or PowerShell. I recognize that they can be indispensable in some situations, however the recommendation is to reconsider using these technologies whenever possible, as they increase the overall risk considerably. A malicious user could exploit this capability to create harmful scripts and efficiently carry out malicious activities quickly. A good practice is implementing strict access controls in the infrastructure, limiting access to these functionalities, and constantly monitoring their use.

As always, I can't stress enough the importance of security training for users and developers of LCNC platforms and other automation processes, such as RPA. In addition to basic information security training, companies must include secure coding practices and emphasize adherence to general security best practices. This ensures that everyone involved in developing and operating automated solutions understands the risks and how to mitigate vulnerabilities.

Consider Low-Code/No-Code (LCNC) platforms as a potential insider threat vector in your network. Historical experience shows that many cyber-attacks begin with the introduction of malicious agents inside corporate networks. These attack vectors can exploit vulnerabilities in internal systems, which happens often enough that you should exercise due care in the design and implementation of any system that handles sensitive data. It is, therefore, prudent to assume that any internal automation, especially those handling confidential information, should be always viewed with the same security caution applied to internal threats.

As mentioned, although LCNC and RPA technologies allow many companies to speed up their development processes and reduce costs, it is essential to remember that security is often overlooked. When this happens, the risks can outweigh the benefits. Organizations must adopt robust and continuous security measures to protect these solutions, preventing security costs from rising exponentially and risks from becoming irremediable.

About the Author

Jordan Bonagura, Senior Security Consultant at Secure Ideas
Principal Security Researcher
Cybersecurity Specialist
Professor and Speaker

If you have any further questions, contact Jordan Bonagura at jordan.bonagura@secureideas.com, or you can find him on LinkedIn or Secure Ideas https://www.secureideas.com.

Guardians of AIoT: Protecting Smart Devices from Data Poisoning

By Manav Mittal, Sr. Project Manager, Consumers Energy

What if the smart thermostat in your home decides that winter is the perfect time for you to experience tropical heat or your self-driving car interprets a stop sign as a green light? These unstable situations sound scary like science fiction, but it highlights the threats that surround artificial intelligence of things (AIoT) systems.

Numerous devices today that shape modern life, such as smart homes, industrial machines, smart gadgets, healthcare systems, etc., are powered by AIoT (AI and IoT) devices. The technological advancements undoubtedly promise unmatched convenience and efficiency, but at the same time expose us to complex vulnerabilities. In this article, I will be highlighting the threat of data poisoning where attackers manipulate the datasets used to train or deploy AI models and cause them to behave in unpredictable ways. Let's dive deeper into why data poisoning attacks are so dangerous, how they take advantage of the unique features of AIoT systems and, most importantly, what we can do to defend against these attacks.

Understanding Data Poisoning

We first need to understand how AI models learn. Machine learning algorithms rely on datasets to identify and predict patterns. The quality and completeness of this data determines the performance of the model is determined by the quality and completeness of this data. Data poisoning attacks tamper the knowledge of the AI by introducing false or misleading information and usually following these steps:

The attacker manipulates the data by gaining access to the training dataset and injects malicious samples

- The AI is now getting trained on the poisoned data and incorporates these corrupt patterns into its decision-making process
- Once the poisoned data is deployed, the attackers now exploit it to bypass a security system or tamper critical tasks.

For example, Tay chatbot, launched by Microsoft in 2016, was designed to imitate the patterns of human conversation. On the contrary, attackers infiltrated the training content with offensive content and within hours inappropriate tweets were posted! Similarly, the spam-filter' feature of Gmail was manipulated by malicious actors to classify illegitimate emails as novice.

The addition of AI into IoT ecosystems has intensified the potential attack surface. Traditional IoT devices were limited in functionality, but AIoT systems rely on data-driven intelligence, which makes them more vulnerable to such attacks and hence, challenge the security of the devices:

- AIoT devices collect data from different sources which increases the likelihood of data being tampered.
- The poisoned data can have catastrophic effects on the real-time decision making.
- Many IoT devices possess limited computational power to implement strong security measures which makes them easy targets for these attacks.

Sector	**AIoT Application**	**Potential Impact of Data Poisoning**
Healthcare	Remote patient monitoring	Misdiagnoses, treatment delays
Transportation	Autonomous vehicles	Accidents, traffic disruptions
Smart Homes	Energy-efficient devices	Incorrect energy usage patterns, increased costs
Industrial IoT	Predictive maintenance systems	Equipment failures, production delays

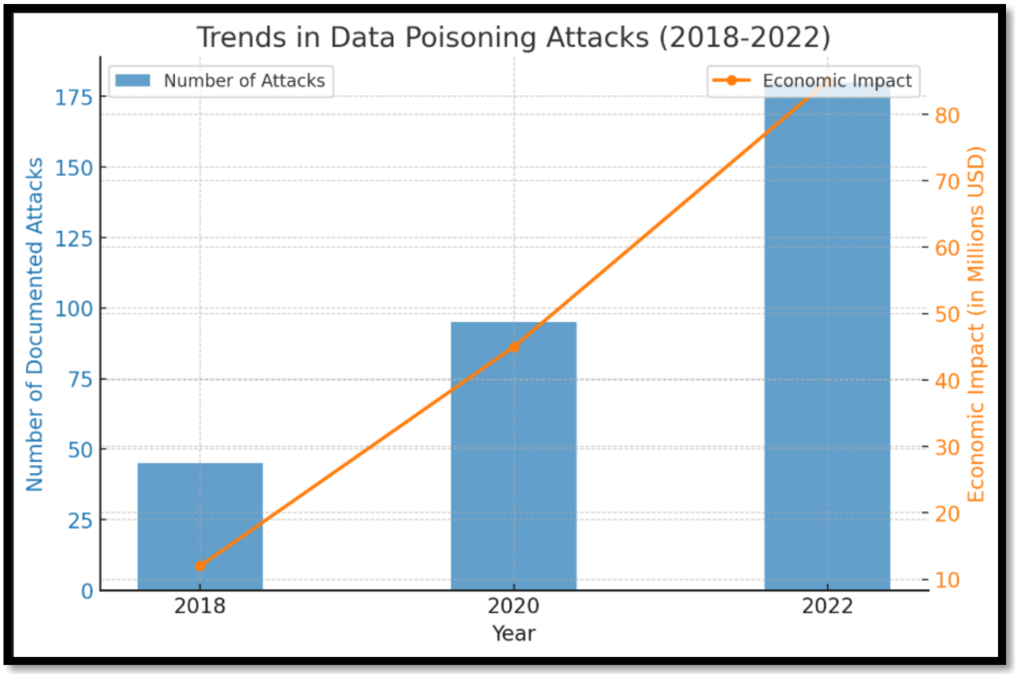
Detect and Mitigate Data Poisoning

The strategies range from technical mediations to policy-level safeguards:

- The first line of defense is to ensure the **training data is of good quality**. Data validation can be done by:
    - Removing the anomalies/outliers from the dataset prior to training.
    - Cross checking the integrity of data through hashing techniques
- Datasets can be examined for **unusual patterns** with the help of unsupervised learning algorithms which can indicate the poisoning of data. Dynamic environments such as smart grids or autonomous vehicles are more suitable for real-time anomaly detection.
- AI models can be taught to recognize and resist malicious inputs with the help of **adversarial training** which consists of simulating real time attacks. This proactive approach will build resilience against known and emerging threats.
- Every technical measure needs a strong data governance policy. This can be achieved by:
- ○ Enforcing strict access controls for data sets.
- ○ Maintaining audit logs of data usage and modifications.
- ○ Regularly monitoring the AI models for vulnerabilities.

Nisos cybersecurity conducted a thorough study and revealed that from a theoretical concern, data poisoning has now advanced to a pressing reality! The analysis focuses on trends over the past several years and depicts a sharp increase in the number of recorded attacks and their economic consequences.

Year	Number of Documented Attacks	Estimated Economic Impact (USD)
2018	45	12 million
2020	95	45 million
2022	180	85 million



The graph illustrating the trends in Data Poisoning Attacks (2018-2022). **Source**: Nisos Cybersecurity.

An upward trend in both attack frequency and economic damage, points out the critical need for dynamic security measures fitted to AIOT systems. To prevent the concerning trends, industry-wide alliance between cybersecurity organizations, policy makers and technology partners is required.

Most attacks in 2018 involved simple methods, such as adding mislabeled data to publicly available datasets and often targeted less critical systems, like conducting minor financial fraud. or spam filtering. Eventually, by 2022, attackers started to use advanced strategies such as inserting malicious samples that bypass anomaly detection systems. Industries like healthcare and automated transportation become the primary target where the repercussions of these threats can be life threatening.

According to the graph, the quickening financial impact reflects the increased dependency on AIoT systems across industries. By 2020, industrial IoT organizations experienced huge losses due to the poisoned data that tampered the algorithms. By 2022, cybersecurity organizations noted that the cost of managing toxic datasets included new training models, improving compromised systems and legal liability for affected customers.

Attackers usually target critical industries like healthcare and tamper patient tracking systems and introduce incorrect metrics. In one such instance, a hospital's AI powered diagnostic tool misclassified an emergency as non-essential due to data poisoning and lifesaving intervention was delayed for the patient. Similarly, in autonomous vehicle industry, tampering with the image recognition systems can cause traffic signs to be misinterpreted leading to recalls and costly security patches. These increased threats emphasize the importance of proactive measures such as adversarial training, real-time anomaly detection and a strong regulatory framework to protect the future of AIOT systems.

The Future of AIoT security

Looking ahead, avoiding data poisoning attacks requires alliance between developers, researchers, and policymakers. Evolving technologies such as blockchain and federated learning are seeming beneficial for increasing data integrity and minimizing the risk of data poisoning.

Blockchains can help with decentralized data storage by constructing tamper-proof records. This technique safeguards the accuracy of the dataset used to train the AI models. Federated learning technology trains AI models within the device and lowers the need for centralized data collection and hence, regulates exposure to data poisoning attempts.

The incorporation of AI with IoT devices has opened remarkable possibilities but at the same time has made systems more vulnerable and prone to sophisticated attacks like data poisoning. As industry leaders, it is our shared responsibility to predict these risks and reinforce our defenses. We can ensure that smart devices remain trustworthy and secure if we combine technical revolutions with robust governance practices.

Please feel free to reach out to me for more information and further discussion on this topic.

About the Author

Manav Mittal is a seasoned Project Management Expert specializing in Automation within the utility, oil, and gas industries. With over nine years of experience, Manav has honed his skills in delivering multi-million-dollar projects with exceptional precision and efficiency. His expertise is backed by PMP and CSM certifications, and he is known for his ability to seamlessly manage tasks, solve complex problems, and mitigate risks, all while fostering excellent communication and collaboration among his teams. He leads cross-functional teams on diverse projects, including construction, IT, strategy, and automation. Manav has extensive experience handling high-risk automation projects in the oil and gas industry. He has successfully implemented SCADA software, modem upgrades, smart metering, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), and Burner Management Systems. As a subject matter expert in automation, Manav excels at integrating these technologies with minimal disruption to day-to-day operations.

Manav Mittal can be reached online at mav.umich@gmail.com and at his LinkedIn https://www.linkedin.com/in/manav-mittal-project-manager.

Setting the Record Straight: Debunking Myths About Mainframe Security in Cyber Strategies

By Cynthia Overby, Director of Security at Rocket Software

Earlier this year, the modern mainframe celebrated its 60th anniversary, underscoring its ongoing significance. According to this 2024 Forrester report, 61% of global infrastructure hardware decision-makers confirm their firms still rely on mainframes, with more than half planning to expand their use in the next two years. As digital transformation accelerates across industries, the mainframe remains a critical backbone of operations; however, its security is often overlooked.

Cybersecurity strategies for mainframes should be top of mind for organizations especially considering mainframes are essential to the operations of leading enterprises: 45 of the world's top-grossing banks, 67 of the Fortune 100 companies, and 8 out of 10 major telecommunications and insurance providers depend on these systems. Given their role in maintaining key functions, from keeping planes in the air to trains moving to facilitating seamless financial transactions, a strategy which aligns a mainframe vulnerability management process to the organization’s requirements and critical success factors, as well as risk metrics are vital for protecting organizational assets and maintaining trust in organization's data security.

Understanding Current Threats

The cyber threat landscape is becoming increasingly dangerous as malicious actors gain access to an ever-expanding arsenal of tools and techniques. These attackers are also becoming more aggressive; in 2023 alone, over 3,200 data breaches in the U.S. impacted more than 350 million individuals. While familiar attack methods (like ransomware and DDoS attacks) remain prevalent, advances in technology have opened the door to even more harmful activities. According to the World Economic Forum's Global Cybersecurity Outlook 2024 report, Generative AI chatbots, for example, now allow cybercriminals to craft highly convincing phishing emails and custom malware with alarming ease. Despite built-in safeguards in commercial AI chatbots, some cybercriminals have turned to models like FraudGPT and WormGPT, which enable subscription-based services for executing complex attacks with minimal technical expertise.

The same leading-edge technologies used by bad actors, however, also offer new opportunities for defense. Applying advanced tools to strengthen foundational security measures can help address the long-standing challenges of reliability and availability many organizations face. Emerging technologies, when combined with an exposure management strategy, can fortify an organization's defenses against sophisticated threats – we'll cover this further down.

As technological advancements empower cybercriminals, they also underscore the need for companies to implement robust, layered cybersecurity strategies that encompass mainframe security. By integrating encryption, AI, and continuous monitoring into a comprehensive security framework, organizations can significantly improve their resilience against complex and evolving cyber threats.

Common Misconceptions About Mainframe Security

However, misperceptions around mainframe security can leave these critical systems exposed. One myth is that mainframes are inherently secure due to limited access and the architecture. While they do provide a solid security foundation, this belief can be detrimental. Mainframes are attractive targets for hackers, as they have IP addresses and are vulnerable to classic cyber threats, with attackers continuously adapting to exploit even minor oversights in security.

Another misconception is that mainframe security operates independently from broader IT security initiatives. However, mainframes must be integrated into an organization's overall cybersecurity strategy. The complexity of IT infrastructures can create security gaps, leading to delayed breach detection where organizations might remain unaware of attacks for months.

The rising threat of identity-based phishing attacks emphasizes the need for an integrated security approach, as these attacks can yield stolen passwords that grant access to critical business data on mainframes. It's pertinent for enterprises to recognize that mainframes can easily fall off the security radar, causing IT professionals to underestimate their risk. Ultimately, mainframes are among the most secure platforms, but only when equipped with the right tools, personnel and strategies.

Best Practices for Encryption, Threat Detection, and Employee Empowerment

Securing mainframe environments against cyber threats requires a proactive approach to encryption, early threat detection, AI, and investing in the upskilling and reskilling of cybersecurity teams. According to IBM Security's 2024 Cost of a Data Breach Report, the global average cost of a data breach in 2024 increased by 10% over the previous year, reaching $4.88 million (the US led the charge with the highest average cost at $9.36 million), revealing the financial stakes are high–underscoring the urgency of quick and effective threat detection. Beyond just the financial impact, these breaches can also inflict significant reputational damage, and once public trust is lost, it can be incredibly challenging to regain. Prioritizing these best practices strengthens defense capabilities and enhances organizational resilience against potential breaches.

Encryption: A Double-Edged Sword

While encryption is a vital defense against cyberattacks on sensitive data, it can also be exploited by malicious actors. Hackers often leverage encryption as an attack vector, infiltrating systems, initiating malicious encryption, and demanding ransom for decryption keys. To combat these threats, organizations must establish reliable methods for early detection of unauthorized encryption activities. However, excessive alerts can overwhelm support staff and hinder effective responses to genuine threats, making the implementation of automated response systems essential.

Investing in Cybersecurity Talent

Organizations should enable their teams to acquire new cybersecurity skills by investing in comprehensive training programs, including online courses, boot camps, and workshops led by industry experts. Leaders must first assess the team's current skill set and encourage employee participation, providing the necessary time and resources for learning. Creating safe environments for practical application, such as staging simulated cyberattacks, fosters a culture that values ongoing education. Recognizing employees who take the initiative to learn and apply new skills is also vital.

According to the 2022 (ISC)² Cybersecurity Workforce Study, found that the global cybersecurity workforce has grown to approximately 4.7 million professionals, yet there remains a staggering shortage of 3.4 million skilled workers. This gap has intensified the impact of breaches: in 2024, IBM reported that over half of breached organizations face severe security staffing shortages—a 26.2% increase from 2023—resulting in an additional average of $1.76 million in breach-related costs. This critical talent shortage presents a valuable opportunity for those interested in a cybersecurity career, offering competitive salaries, job stability, and the chance to play a key role in protecting essential infrastructure.

Leveraging AI and Automation

AI and automation are reshaping cybersecurity, streamlining threat detection and response while also enabling cybercriminals to execute attacks at unprecedented scales. According to IBM, organizations using these technologies saw a substantial reduction in average breach costs, from $5.72 million for those without AI and automation to $3.84 million for those extensively utilizing them—a savings of $1.88 million. These tools allowed organizations to identify and contain breaches nearly 100 days faster than those without them, highlighting their critical role with these threats.

To maximize these benefits, security teams need comprehensive visibility across hybrid and multi-cloud environments. Applying Data Security Posture Management (DSPM) and enforcing strong access controls can safeguard data across various platforms. However, as generative AI adoption accelerates, so do its risks. Implementing AI governance and securing training data from theft and manipulation are crucial defenses. Vigilance against AI-specific threats, such as prompt injection and data poisoning, strengthens an organization's resilience. Moving beyond outdated practices to advanced monitoring technologies can better protect an organization's critical infrastructure against a rapidly shifting threat landscape.

Achieving Near Real-Time Monitoring

Organizations typically take an average of 258 days to identify and contain a breach, followed by an additional 100 days or more for recovery. During this time, attackers can infiltrate systems, establish backdoors, compromise backups, and encrypt data—all while remaining undetected. For mainframe operators, the risk of these malicious activities slipping through the cracks is significant, highlighting the necessity for early detection as a core component of business and security strategy.

To identify malicious encryption, organizations can implement a whitelist of authorized encryption processes. Regular updates to this whitelist are critical; however, reliance on human intervention can lead to errors. A more efficient approach is to use real-time alerts triggered by software that detects rogue processes. This system can differentiate between legitimate and malicious activities, allowing authorized processes to continue without unnecessary alerts while immediately suspending any unauthorized ones, thereby preventing further damage and enabling support staff to investigate the threat.

Adapting to Future Challenges

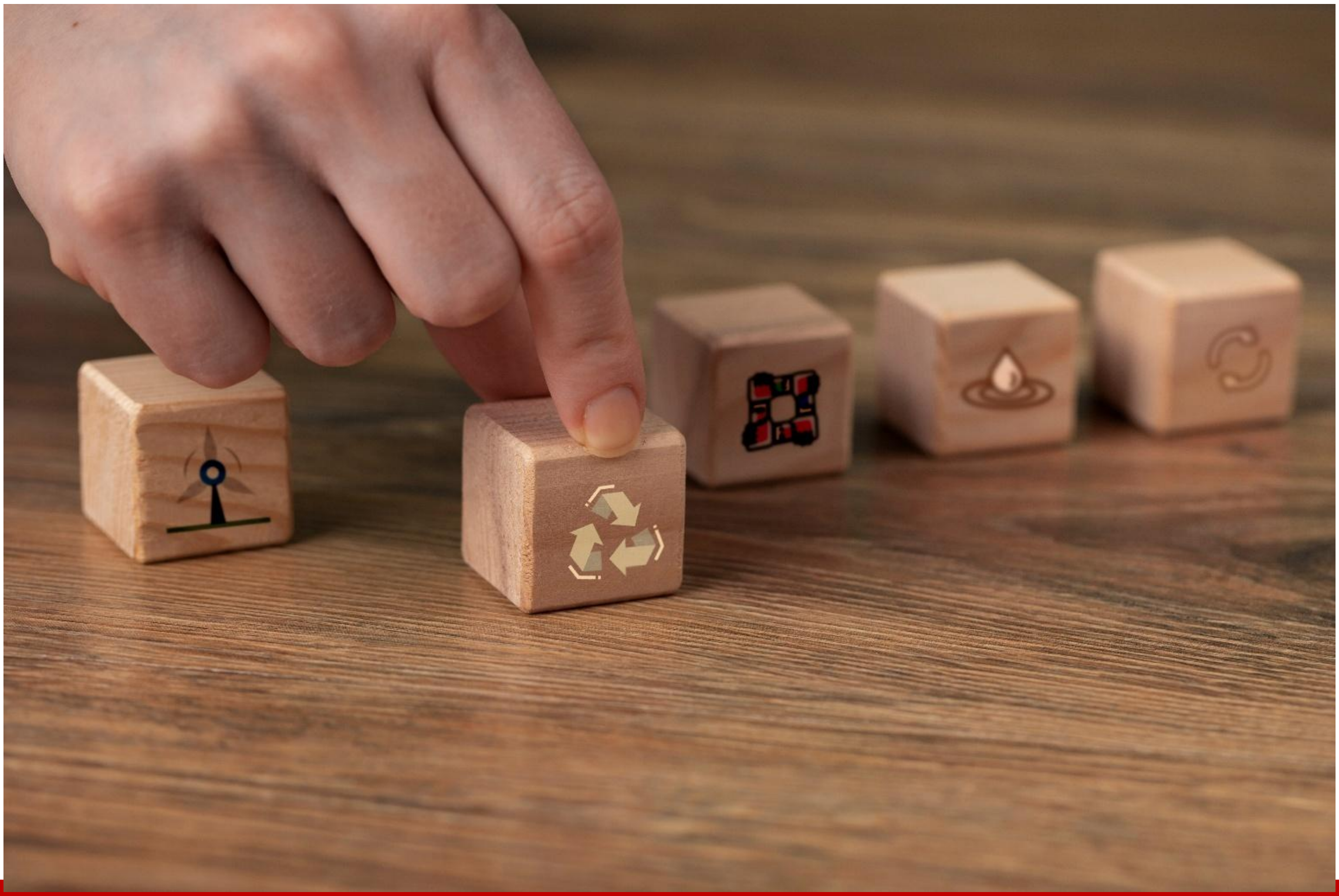
As cybersecurity changes in response to new threats and regulatory demands, organizations must shift from isolated security tools to integrated, risk-managed approaches. In 2025 and beyond, adapting to these challenges will require deep, organization-wide assessments that address the specific vulnerabilities of mainframes and other critical infrastructure. This includes minimizing privileged accounts to reduce identity-based attacks, as threat actors increasingly target identity and vulnerability scanning at the operating system layer.

The integration of mainframe security into comprehensive cybersecurity strategies is essential as cyber threats grow more sophisticated. Through understanding current threats, dispelling misconceptions, and following best practices for encryption and threat detection, organizations can build stronger defenses. Taking proactive steps to secure mainframes today will better position organizations to navigate the threats of tomorrow. The time to act is now—secure mainframes, protect your organization, and stay ahead of emerging threats.

About the Author

As Director of Security, Customer Solutions Engineering at Rocket Software, Cynthia leads the company's suite of solutions, focusing on mainframe security, cyber defense, and data protection, positioning Rocket Software as a leader in the compliance and risk management space. With over 40 years of industry expertise in sectors including financial services, healthcare, IT, and cybersecurity, she brings a wealth of knowledge in security strategy, executive leadership, and business case development.

As a dedicated advocate for women in cybersecurity and diversity in tech, Cynthia also serves on the Board of Directors at SHARE, where she led the Women in IT initiative, mentoring and developing the next generation of female tech leaders. With a career built on influencing sustained change and promoting leadership development, she strives to drive impactful solutions that enhance the security landscape across industries



Legacy Code: A Growing Threat to Public Sector Organizations

Modernizing legacy systems with GenAI

By Joel Krooswyk, Federal CTO at GitLab Inc.

Legacy code, a relic of past development practices, poses significant security risks and development challenges to public sector organizations. These outdated systems are often incompatible with modern security tools and create vulnerabilities that cybercriminals can exploit.

Beyond security, maintaining legacy code is a costly endeavor, requiring specialized skills and significant developer time. As a result, organizations are trapped in a cycle of technical debt, struggling to innovate and adapt to changing business needs.

By leveraging AI-driven testing, security capabilities, and code refactoring techniques, organizations can modernize their legacy systems, mitigate security risks, and empower development teams to focus on innovation.

What’s the problem with legacy code?

Legacy code refers to an existing code base that a team inherits from previous team members and continues to use and maintain. The codebase may function correctly, but its long history of modifications by various developers can obscure its original intent and introduce unintended consequences. The current team may struggle to distinguish between valuable and unnecessary changes. Furthermore, the code might rely on outdated frameworks or programming languages, increasing the risk of vulnerabilities and maintenance difficulties.

Organizations that choose to retain legacy code expose themselves to a multitude of risks. Because the code wasn’t designed for newer technologies, teams may be unable to integrate it with modern software, potentially impacting product performance, scalability, and customer experience.

A particularly significant concern is the lack of security scanners designed for legacy code. This leaves organizations exposed to undetected vulnerabilities, especially when updates are made by developers unfamiliar with the codebase or its underlying language. Moreover, legacy code frequently relies on memory-unsafe languages like C or C++, which are proven to host 70% of identified vulnerabilities.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has emphasized the heightened security risks associated with using unsupported software in critical infrastructure and the subsequent risk to national security. By continuing to rely on outdated code, organizations jeopardize their security posture and undermine their ability to innovate and adapt to the evolving technology landscape.

The solution is code refactoring

Code refactoring, a controlled technique for improving the design of an existing code base, allows the securing and modernizing of legacy code without obscuring its original functionality. There are many refactoring techniques – from inline refactoring, which involves simplifying code by removing obsolete elements, to refactoring by abstraction, where duplicate code is deleted.

What’s important to know is that code refactoring requires time and significant developer skills to do well. It also requires a lot of testing when developers are already busy working on their other tasks. While code refactoring is certainly the answer to bringing your legacy code into the future, making it readable, efficient, and secure, it is a project in and of itself, especially at scale.

How AI can help

AI is already accelerating software development, and there’s a lot that AI can do to help teams accelerate the refactoring process. AI-powered tools can decipher complex legacy code, generate new code, and bridge knowledge gaps for developers unfamiliar with specific languages. By automating tedious tasks and providing intelligent assistance, AI can speed up the modernization of legacy systems.

AI can further enhance refactoring by automating testing and security tasks. By analyzing root causes, generating tests, and identifying vulnerabilities, AI can help developers remediate vulnerabilities efficiently. With AI as a powerful ally, code refactoring is accessible and achievable for organizations.

According to GitLab research, 34% of all respondents using AI across the software development lifecycle already use AI to modernize legacy code. This is even higher in the financial services industry (46%).

While AI offers significant potential for accelerating code modernization, it also requires testing, guardrails, and human oversight. To ensure optimal security, teams should combine AI-powered tools with other security measures, such as creating a dynamic software bill of materials (SBOM). An SBOM provides a comprehensive inventory of software components, including legacy code, enabling organizations to identify and mitigate potential vulnerabilities.

Bring your codebase into the future

While the transition from legacy codebase maintenance to modernization may seem daunting, it is a crucial step toward ensuring organizational security and future-proofing operations. Organizations can streamline processes, reduce costs, and boost efficiency by embracing modern tools and techniques.

Instead of allocating valuable resources to deciphering outdated languages and frameworks, development teams can focus on innovative product development. AI-powered tools can automate the complex task of code refactoring, ensuring that legacy code is not only secure but aligned with modern best practices.

About the Author

Joel Krooswyk has over 25 years of experience in the Software industry. His end-to-end software development life cycle expertise benefits customers and employees alike. His leadership experience spans not only the U.S. Public Sector, but also small, mid-market, and enterprise businesses globally. Joel is an experienced leader, team builder, communicator, thought leader and researcher.

His experience spans development, QA, product management, portfolio planning, and technical sales, and he has written a half million lines of unique code throughout his career. On an average day, you'll find him discussing software modernization, cybersecurity, governance and compliance, AI, ongoing digital transformation, and automation.

Learn more about GitLab at https://about.gitlab.com/solutions/public-sector/ and follow Joel on LinkedIn at https://www.linkedin.com/in/joelrkrooswyk/.

Global Capabilities Centers in Cybersecurity: A New Era of Cyber Defense

Revolutionizing Security: How Global Capability Centers are Shaping the Future of Cyber Defense

By Roshan Patil, Research Associate at SNS Insider Pvt. Ltd

Cybersecurity today transcends the typical consideration of large enterprises or governments as a part of the global infrastructure of our digital world. An introduction to the problem Cyber sacred sipping, businesses, governments, and individuals are getting then more susceptible to cyberattacks as cyber threats expand more complex and twain more intensive. With this expanding threat landscape, a multitude of organizations have set up the Global Capabilities Center (GCC) in cybersecurity. GCCs are aimed at adopting a future-forward and responsive mindset around cybersecurity issues, employing international talent, advanced technologies, and cross-border partnerships.

What Are Global Capabilities Centers (GCCs)?

Global Capabilities Centers are strategic hubs that centralize top talent, tools, and know-how using their resources to work on some of the hardest problems in cyber. GCCs are a high-level structure that integrates all cybersecurity capabilities namely Threat Detection, Incident Response, Security Operations, Risk Management, etc. in conjunction with one another, unlike traditional SOCs which operate up to a functional level.

Such centers are tailored to both protect against current threats as well as innovating new state-of-the-art cybersecurity solutions. This mix of regional expertise allows them to approach cyber threats with a global mindset. Normally, Cybersecurity GCCs also act as research and development centers where experts do a lot of research on new security technologies; and threat analysis, along with simulating potential cyberattacks to ramp up preparedness.

The Growing Importance of Global Capabilities Centers in Cybersecurity

Cybersecurity Global Capabilities Centers are on the rise, thanks to the growing digitalization and the rise of cyber threats. Global costs of cybercrime are projected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015. It also stands as a testament to the necessity of resilient cybersecurity frameworks as this rise in cyberattacks averaging 1,636 attacks weekly in 2023 indicates. Most breaches (74%) originate from external actors, including a 13% rise in ransomware in 2022. To meet these growing threats, GCCs are central to managing and mitigating these risks. More than 50% of GCCs are in India, and many of them deliver cost-effective yet complete cybersecurity offerings. In addition, Artificial Intelligence and machine learning technologies are continuously improving the capabilities of GCCs. The agility and precision of AI-powered threat detection and response capabilities are now leading to 65% of GCCs integrating these systems within their cybersecurity architecture.

Organizations are compelled to strengthen their cybersecurity due to government regulations like GDPR and the Cybersecurity Information Sharing Act (CISA). For instance, the U.S. government has asked for $13 billion towards cybersecurity in fiscal year 2025, an increase from $11.8 billion in the previous fiscal year. An additional indication of the expanding need of expertise in this area is the 1.3 million people employed in the cybersecurity workforce here in the U.S. in 2023. Companies, governments, and even individuals will continue to benefit from Global Capabilities Centers (GCCs) as they remain in the frontlines of the cyber threat evolution spate, serving as the staunchest defense everyone could have against the growing sophistication of these attacks.

The Role of Global Collaboration in Cybersecurity

A hallmark of successful Global Capabilities Centers is their ability to harness global collaboration. Cybersecurity threats often transcend borders, with attackers operating across regions and time zones. A GCC can bring together talent from different countries, ensuring that the center operates around the clock, providing continuous protection and innovation.

Global collaboration within a GCC also enables organizations to stay ahead of emerging cyber threats. Different regions face unique cybersecurity challenges based on their geopolitical context, regulatory landscape, and industry-specific risks. By pooling expertise from diverse sources, a GCC can develop solutions that address a wide range of challenges, from compliance with data protection regulations in Europe to protecting critical infrastructure in North America or Asia.

Key Functions of Global Cybersecurity Capabilities Centers

1. **Threat Intelligence and Incident Response**: One of the primary roles of a GCC is to identify and respond to cyber threats. By leveraging real-time data from across the globe, these centers can detect anomalies and signs of potential attacks before they escalate. This proactive approach allows them to respond quickly to mitigate damages. Incident response capabilities within GCCs include managing cyber-attacks, investigating breaches, and implementing remediation strategies.
2. **Research and Development (R&D)**: Cybersecurity is an ever-evolving field, and GCCs are at the forefront of developing new defense mechanisms. They invest in R&D to create cutting-edge technologies like artificial intelligence-driven threat detection systems, next-generation firewalls, and advanced encryption methods. These innovations play a crucial role in staying ahead of increasingly sophisticated cyber adversaries.
3. **Security Operations**: GCCs serve as security operation hubs, ensuring that all systems are constantly monitored for potential vulnerabilities. They deploy a variety of tools, from endpoint detection and response (EDR) to intrusion detection systems (IDS), ensuring that any potential breach is detected and addressed quickly. Continuous monitoring is a crucial function, helping organizations maintain high levels of security in their operations.
4. **Compliance and Risk Management**: Cybersecurity is also about ensuring that an organization complies with relevant industry standards and regulations. GCCs play a crucial role in managing cybersecurity risks, ensuring that companies meet local, national, and international cybersecurity regulations. They help organizations avoid regulatory fines and reputational damage by ensuring they are following the necessary compliance protocols, including those related to data privacy (GDPR, HIPAA) and industry standards (ISO/IEC 27001).
5. **Data Protection and Privacy**: With data being one of the most valuable assets for businesses today, data protection is a top priority for GCCs. These centers develop policies and deploy technologies to ensure the confidentiality, integrity, and availability of sensitive data. This includes everything from securing data during transmission to ensuring that storage systems are encrypted and protected against unauthorized access.

Types of Websites Associated with Global Capabilities Centers in Cybersecurity

Website Type	Description
Interactive Dashboards	Real-time monitoring of cybersecurity threats, system vulnerabilities, and attack events.
Collaboration Platforms	Online hubs for global teams to collaborate, share information, and work on cybersecurity initiatives.
Incident Response Portals	Specialized portals for reporting breaches, tracking incidents, and coordinating response efforts.
Educational and Training Sites	Websites offering training programs, webinars, and resources for cybersecurity awareness and best practices.
R&D and Innovation Pages	Dedicated sections for sharing research, white papers, and new cybersecurity technologies.

Website Types of Global Capabilities Centers in Cybersecurity

- **Interactive Dashboards for Threat Monitoring**: These websites are equipped with interactive, real-time dashboards that allow cybersecurity teams to monitor threats, breaches, and security events in real-time. The dashboard typically shows key metrics such as system vulnerabilities, attack vectors, and ongoing incident investigations. This is essential for rapid decision-making and response to emerging threats.
- **Collaboration Platforms**: GCCs often have websites that serve as collaboration hubs for teams across the globe. These platforms allow cybersecurity experts from different regions to share information, conduct virtual meetings, and work on shared projects. Integration with cloud-based services makes these platforms highly scalable, enabling seamless global collaboration.
- **Incident Response Portals**: Some GCCs provide specialized websites dedicated to incident response. These portals allow clients to report breaches, track ongoing incidents, and receive real-time updates on remediation efforts. The site acts as a central hub for communication and coordination during cybersecurity incidents.

- **Educational and Training Websites**: Many GCCs offer websites dedicated to cybersecurity training and awareness. These platforms host webinars, online courses, and resources designed to educate organizations about cybersecurity best practices. The goal is to train employees to recognize potential threats and respond appropriately, reducing the likelihood of security breaches caused by human error.

Global Capabilities Centers in Cybersecurity: A Global Perspective

The role of GCCs in cybersecurity is rapidly growing, as they enable organizations to mitigate the increasing threat of cyberattacks. Their importance cannot be overstated, as they combine cutting-edge technology, global expertise, and collaborative solutions to provide robust protection. As cyber threats continue to evolve, the need for Global Capabilities Centers will only increase, helping businesses stay one step ahead of attackers.

About the Author

Mr. Roshan Patil is a Senior Research Associate at SNS Insider Pvt. Ltd., specializing in Market Research and Analysis. With a post-graduate degree in MBA and over 4 years of experience in the Healthcare Industry, he contributes to insightful reports that aid strategic decision-making, helping clients stay competitive.

Roshan can be reached on LinkedIn https://www.linkedin.com/in/roshan-patil-193ab2235/

Harnessing AI to Strengthen Security Controls

By Vassilis Papachristos, Head of Information Security Advisory Services, Netcompany-Intrasoft

The rapid development in the field of Artificial Intelligence during the last years brought significant changes to many areas, including information security. Security controls traditionally relied on human inspections and analyzes, nowadays they are taking advantage of possibilities given by AI to detect and counter threats more precisely and efficiently.

The Role of Artificial Intelligence in Information Security Controls

AI provides various tools and technologies that can considerably improve the effectiveness of controls. AI can analyze vast amounts of data through ML algorithms to find anomalies and potential threats. Applications include but are not limited to:

- **Anomaly Detection**: Machine learning algorithms can be trained on what normal behavior is on a network and detect anomalies that could indicate an attack.

- **Process Automation**: Automation of control processes reduces the need for human intervention, thus enabling faster and more frequent checks.
- **Analytics**: AI could use data to predict future threats and perform proactive actions.
- **Compliance Checking**: AI could help information security auditors to check systems compliance with various regulations, standards and frameworks and easily spot any discrepancies before these turn out to be significant issues.

Benefits of Using AI in Information Security Controls

The incorporation of AI in security controls provides the following benefits, among many others:

- **Increased Accuracy**: The ML algorithms analyze data more accurately than a human brain can, this reduces the occurrence of false positives and false negatives.
- **Speed and Efficiency**: AI can process huge amounts of information in real-time to provide timely detection and response in the event of any threat.
- **Continuous Learning**: With each passing day and every new information feed, machine learning becomes more intelligent and resilient, making it capable of handling newer and more complex threats.
- **Cost Reduction**: Automation of control processes decreases the cost associated with manual checks, requiring less human intervention.

Challenges and Issues

Even with all those advantages, integrating AI into security controls does not come without its challenges:

- **Algorithms' Security and Reliability**: ML algorithms are prone to different kinds of attacks, with adversarial attacks being one of them, where attackers feed deceptive data to deceive AI systems.
- **Ethical Issues**: The use of AI raises ethical concerns like privacy invasion and surveillance since continuous monitoring and data analysis may be perceived as intrusion into one's private life.
- **Need for Specialized Personnel**: Developing and managing AI systems require specialized knowledge and skills, which might not be readily available to all organizations.
- **Data Dependency**: The effectiveness of ML algorithms depends on the quality and quantity of data they are fed. Insufficient data may result in the algorithms failing to detect threats correctly.

Examples of AI Application in Security Testing

Many organizations have already started integrating AI into their security testing. Examples include:

- **SIEM Tools**: SIEM tools use AI to combine and analyse data from multiple sources to provide comprehensive security reports with real-time threat detection.

- **Malware Detection**: AI algorithms can detect new forms of malware not recognized by traditional detection systems.
- **Vulnerability Assessment**: AI can assist and support in identifying and evaluating vulnerabilities in systems and networks, suggesting corrective actions before these vulnerabilities are exploited by attackers.
- **Risk Assessment**: AI strengthens risk assessment through big data analytics to show impending threats and patterns. It can find emerging risks and anomalies in real time while offering actionable insights.

The Future of AI in Information Assurance Controls

The continued evolution of artificial intelligence is expected to bring even more changes into the field of information and cyber security. Trends anticipated to dominate in the near future include:

- **Advanced Automation**: The automation of control processes is set to grow further with the use of more advanced AI algorithms that will enable even more complex analyses and actions.
- **Human-Machine Collaboration**: AI will not replace humans but will collaborate with them, providing tools and information to help security professionals make better decisions.
- **Enhanced Privacy Protection**: As AI evolves, new methods will be developed to protect user privacy, ensuring that personal information remains secure and confidential.

Conclusion

The integration of artificial intelligence into information security controls represents a significant step forward in enhancing the security of information systems. Despite the challenges, the benefits AI offers are undeniable. Organizations that adopt it will be better equipped to handle modern security threats and complex cyber-attacks. The future of AI in this domain looks promising, with ongoing improvements and innovations in cyber security solutions that expected to provide even greater protection and efficiency.

About the Author

Vasilis Papachristos is the Head of Information Security Advisory Services at Netcompany-Intrasoft. With 15+ years of experience in information security, compliance, risk management and governance, he specializes in building robust security frameworks for diverse industries. His expertise spans in ISO 27001, NIS2, DORA, GDPR, risk assessments, policy development and client-focused consulting. Currently, he leads a team of skilled professionals while delivering strategic solutions and services that enable organizations to mitigate cyber risks and achieve regulatory compliance. Netcompany-Intrasoft provides tailored GRC and security advisory services, helping businesses safeguard their operations in an evolving threat landscape. Vassilis can be reached online at Linkedin and at our company website: https://www.netcompany-intrasoft.com

Email: vassilis.papachristos@netcompany.com

Key Cybersecurity Considerations for 2025

By Sailaja Kotra-Turner, Chief Information Security Officer at Brown-Forman

As we usher in a new year, it's crucial to focus on key areas in cybersecurity that demand our attention. While there's undoubtedly a long list of issues that all companies are dealing with, these are three topics - mitigating risks from vendors, navigating the complexities of AI, and combating phishing - that should be at the top of the list while planning for a successful 2025.

Mitigating risks from vendors. Relationships with vendors are constantly evolving as are the threats. Before the advent of cloud computing and SaaS there was a layer of separation between the vendor and customer. The vendor would have an update that could then be tested in-house to make sure it worked as intended before it was deployed, but with cloud computing, and more so with SaaS, there is no layer of separation now. If a vendor has an incident - cyber or otherwise - that incident is quickly and immediately passed on to the customer.

This also adds another layer of risk, as now hackers can go after a company by going after its vendors. This can cause collateral damage to companies that may not have been the intended targets. We're now seeing third, fourth and even-fifth party risk getting a lot more complicated. The best way to combat this new threat is by using a tried-and-true tactic - trust.

Part of building trust includes thorough evaluation of your vendor's environments by various means - questionnaires, audits, security ratings. These evaluations must assess both security and operational posture, and be repeated periodically to make sure they're up-to-date. Trust can also be built through contractual agreements that transfer and/or assign liability to the right party through data agreements and service letter agreements.

All that said, no matter what the level of trust that is built, you still need a robust incident response plan and business continuity plan those accounts for potential disruptions and security incidents caused by a vendor.

Navigating the challenges of AI: The first thing to remember with AI is that the risk is still the underlying data. An AI system is a tool that exposes the underlying data to a potentially different type of risk, or exacerbates existing risk. In short, secure AI starts with secure data.

The combination of AI and cloud creates potential for unauthorized and unintended disclosure of data. Without appropriate data agreements, any data entered into an AI could potentially be used to train the system, thus compromising the confidentiality of the data.

Another area of concern when it comes to AI is the potential for misuse. Whether it's the use of deepfakes to spread misinformation, crafting better phishing emails, or lowering the technological threshold for hacking - AI can be a very powerful tool that has the potential to work against your organization.

The area of AI regulation can also be challenging at times as it is still in its infancy, but is growing fast. Staying on top of upcoming regulations and ensuring we all meet said regulations will be a moving goalpost for some time.

At Brown-Forman we are focusing on data governance and enhanced data security first. Understanding who owns what data, and minimizing visibility to an as-needed basis helps us build AI systems that will only access the right data and present it to the right people.

Because of this, we are very focused on education and awareness. These spans opportunities presented by AI, how to use AI, and the risks of AI. The more our employees understand and learn how to use AI safely, the better we can make sure of the opportunities provided by AI while minimizing the risks.

Combating Phishing. Phishing has evolved over the years from mass emails - send a 1000 or more and hope someone "bites," to spear phishing - more targeted emails that require research. Today, the targeting has continued to get better and generative AI has added another layer. We used to tell people to look for spelling and grammar errors, but with generative AI there are no such errors. Phishing emails look very, very similar to real emails.

Recognizing phishing emails for scams requires muscle memory. It's not necessarily difficult to spot a phish, but you need to be vigilant about repeated training so you remember to check on a regular basis. You also need to be realistic and accept that people will fall for phishing one time or another. It is important to have layers of protection in place for when that does happen. Quick reporting helps activate those layers faster, and should be a focus of education and awareness efforts.

In 2025 we will continue to focus on "role-based training" for phishing, because the level of risk faced by and posed by different roles is different. For example, a salesperson who consistently receives external email that may or may not include attachments is more vulnerable, whereas a HR person likely has access to information that's more valuable and faces more risk. We're working with each team to see how we can better help them craft processes that minimize risk and impact of being phished.

As technology advances, so must our strategies for improving security. Sometimes the solutions are as simple as trust and training, and other times it's a matter of implementing new governance, technology and strategies. In 2025 focus on the security issues that pose the largest threats and find the right solutions for your organization to be successful.

About the Author

Sailaja Kotra-Turner is the Chief Information Security Officer at Brown-Forman. Sailaja has been with Brown-Forman since September 2020 as Chief Information Security Officer. She has been instrumental in shaping Brown-Forman's security posture and controls to date. Prior to joining Brown-Forman, Sailaja's leadership focused on IT Security teams in the areas of security engineering, operations and strategy, security awareness, and identity management. Sailaja holds a Bachelor of Technology in computer science and systems engineering from Andhra University and a master of business administration from Southern Methodist University. Our company website is https://www.brown-forman.com/

Make the Most of Your Holiday Cybersecurity Awareness Efforts

By Jatin Mannepalli, Information Security Officer, IMC Trading

The holiday season is a time for joy, celebration, and, unfortunately, an uptick in cyber threats. From phishing scams that mimic festive deals to exploitation of end-of-year operational freezes, cybercriminals are particularly active during this time of year. Having navigated these challenges in my professional journey, I've come to appreciate the importance of a well-tailored holiday cybersecurity awareness program—one that resonates with the people it's designed to protect. Here are some practical strategies to ensure your program stands out and delivers lasting impact.

Understanding the Holiday Threat Landscape

The holidays bring unique vulnerabilities. Increased online transactions, particularly in retail and tech sectors, attract phishing scams disguised as holiday offers. A recent Proofpoint's State of the Phish Report revealed that 75% of organizations experienced phishing attacks in the last year, with a noticeable spike during the holiday season. "Peak freeze" periods, where system changes are restricted to maintain stability, can inadvertently limit security updates, creating a ripe environment for attackers.

Cybersecurity teams often struggle to cut through the seasonal distractions and make users vigilant. The key is to adapt your approach to your organization's specific context and the varied roles within it. A generic one-size-fits-all strategy rarely works.

Tailor Messaging for Maximum Impact

To resonate with your audience, tailor your awareness program based on roles, individual preferences, and your organization's unique context.

1. **Role-Based Messaging:** Each department faces distinct cybersecurity risks. For instance:
    - **Accounting Teams**: Target them with messaging about invoice scams and fraudulent wire transfers.
    - **Customer Service**: Focus on social engineering tactics they're likely to encounter.
    - **Executive Teams**: Highlight threats like business email compromise (BEC) attacks, which the FBI estimated caused (Report) over $2.9 billion in losses in 2023.

The core message should emphasize "security as everyone's responsibility," while tailoring examples and action items to specific risks each group faces.

2. **Individualized Messaging:** People engage more when they see how cybersecurity impacts them personally. Share real-life incidents from your industry to illustrate the stakes. For example:
    - Educate employees on protecting their families' online accounts, then link these practices to workplace security.
    - Use relatable, seasonal scenarios like fraudulent delivery notifications or fake charity drives to drive home key points. There was a 30% surge in cyberattacks during the holiday season, according to Cyberint.

3. **Business Context:** Your program should reflect your company's risk landscape and goals. For example:
    - Address vulnerabilities arising from peak freeze periods.
    - Engage global teams with culturally relevant content.
    - Educate temporary holiday hires and third-party vendors on security protocols.

Keeping Content Engaging and Fresh

In my experience, the biggest challenge in cybersecurity awareness is sustaining interest. Here's how to keep your program dynamic:

- **Timely Topics**: Relate lessons to current events and recent threats.
- **Diverse Media**: Mix up formats with videos, infographics, emails, and interactive sessions.
- **Gamification**: Turn learning into friendly competitions with rewards for phishing-spotting champions or cybersecurity quiz winners.
- **Humor**: Lighthearted messaging can make lessons memorable without diluting their importance.
- **Leadership Involvement**: Messages from the CEO or other leaders underscore the program's priority.

Tackling Phishing Head-On

Phishing attacks peak during the holidays, leveraging themes like holiday deals, shipping notifications, and charity appeals. One of the most effective ways to address this is through simulated phishing exercises. Customize these scenarios based on your organization's history and evolving threats, ensuring they mirror real-world tactics. According to Proofpoint's 2024 report, phishing simulations improved awareness by 46% when tailored to an organization's specific context. Post-simulation feedback is invaluable in turning mistakes into learning opportunities.

Managing Risk During Peak Freeze

Many organizations impose operational freezes during critical holiday periods to ensure system stability. While this practice minimizes disruptions, it can also delay essential security updates. To navigate this:

- Communicate evolving risks to leadership so informed decisions can be made about mitigation or acceptance.
- Incorporate lessons from accepted risks into your awareness content.

Beyond the Holidays: Creating a Year-Round Security Culture

A successful holiday security awareness program lays the groundwork for a culture of vigilance that extends throughout the year. Carry the momentum forward by:

- Regularly updating training to reflect new threats.
- Maintaining open dialogues between security teams and other departments.
- Celebrating and rewarding ongoing engagement with cybersecurity practices.

Final Thoughts

The holiday season is a time for celebration, but it’s also a prime opportunity for cybercriminals. By tailoring your awareness program to your organization’s unique challenges and fostering a culture of engagement, you can empower your team to navigate this season securely. From my own experiences, I can share that the value of making cybersecurity personal, relevant, and above all, actionable. Let’s make this holiday

About the Author

Jatin Mannepalli CISSP, CCSP, is an Information Security Officer (ISO) at IMC Trading, with over 10 years of experience in the InfoSec field. He has led information security and risk management teams, and worked as a security consultant for major firms like McKinsey & Company. Jatin specializes in security governance, risk management, and creating customer-centric, technology-driven security strategies. His approach focuses on aligning security with organizational goals. He is a published author on DarkReading and SecureWorld, and contributes to cybersecurity by developing ISC2 exams and volunteering to raise security awareness in local communities. Jatin’s expertise and passion for holistic security management make him a prominent figure in the field, and he is known for his dedication to organizational success and client satisfaction.

Linkedin: https://www.linkedin.com/in/jatin-mannepalli-7a7b05a5/

2025 Cyber Security Predictions: Navigating the Ever-Evolving Threat Landscape

By Glen Williams, CEO, Cyberfort

As we look ahead to 2025, the world of cyber security is set to undergo significant changes. Attackers are becoming increasingly more sophisticated with the use of AI, making phishing emails even more convincing and enabling the daunting creation of cloned personal identities.

This shift from traditional identity theft to much more complex techniques poses new challenges on both individuals and businesses. Additionally, the landscape of identity and permissions management is evolving, underscoring the importance of a proactive and comprehensive approach to cyber security. This includes leveraging advanced technology, maintaining continuous monitoring, and fostering a strong culture of security awareness within organisations.

By understanding these emerging threats and preparing accordingly, we can better protect our organisations and ensure a safer digital future. But what will those key trends be as we enter 2025 and how we can all stay ahead of the threat in this ever-changing digital world?

Human Error to Increase as Attacks Get “Less Dumb”

In the past six months, we’ve seen an alarming increase in the use of generative AI by attackers, mirroring techniques that achieve 80% success rates in real world testing. This technology is being leveraged to craft highly targeted phishing emails, integrating social media and work personas to deceive recipients more effectively. Additionally, the use of deep fake technologies to clone senior individuals and demand tasks to be completed has become more prevalent.

This combined with machine learning will provide attackers with ‘more likely to succeed’ target lists in 2025, which we will then start to see offered at a premium through marketplaces and associate programs. As attacks become more sophisticated, the margin for human error will increase, making it crucial for organizations to enhance their security measures and training programs.

Identity Theft to Be Replaced by Cloning

2024 saw a significant rise in the use of Open-Source Intelligence (OSINT) and advanced data tools to create clone identities. This trend is expected to continue into 2025, posing a major challenge for identity verification processes.

As these cloned identities grow increasingly comprehensive, verifying legitimacy and ownership will become more challenging. Even traditional challenge-response methods may fail, as both the original and the clone are likely to provide accurate answers. Continuous and rigorous monitoring of identities will be essential to detect and mitigate these threats before they cause harm.

Evolution of Identity and Permissions

The concept of ‘zero trust’ has been a hot topic in cybersecurity discussions. However, most organizations are still in the strategy development stage and have not fully implemented zero trust across their IT environments. Even those that have adopted a zero-trust strategy often have not extended it to their cloud and SaaS environments.

As we move into next year, we will start to see hidden permissions assigned manually or explicitly at the account level, becoming an even bigger opportunity for attackers. Attackers will focus on these exceptions, leaving organizations vulnerable despite a 98% success rate in other areas.

Moreover, the complexity of modern IT environments, with a blend of on-premises, cloud, and hybrid infrastructures, adds to the challenge. Organizations must ensure that their zero trust policies are comprehensive and cover all aspects of their IT landscape. This includes continuous monitoring and validation of user identities and access privileges. Additionally, the integration of zero trust with other security frameworks and tools will be crucial in creating a robust defense mechanism. As cyber threats evolve, so must the strategies to counter them, making zero trust an ongoing journey rather than a one-time implementation.

Preparing for the Future

To prepare for these evolving threats, organizations must adopt a proactive approach to cyber security. This includes investing in advanced threat detection technologies, enhancing employee training programs, and continuously monitoring and updating security protocols.

The key to staying secure in 2025 will be a combination of advanced technology, continuous monitoring, and a culture of security awareness within organizations. By understanding these predictions and taking proactive steps, organizations can better protect themselves against the sophisticated threats that lie ahead.

About the Author

Glen Williams is the CEO of Cyberfort. Glen is responsible for leading the business, driving organic and inorganic growth and developing key customer relationships. Prior to joining Cyberfort he held CEO roles at North and Damovo. Earlier in his career, Glen was a senior leader at Dell, Computacenter and Lenovo.

Glen can be reached online on LinkedIn and at our company website https://cyberfortgroup.com/

Not Just Another List of Top 10 Metrics You Should Measure

By Shirley Salzman, CEO and Co-Founder, SeeMetrics

In the world of cybersecurity, we've all encountered those articles: lists that tell us the top ten metrics to track to improve performance, strengthen security posture or communicate and impress the board. Many of these lists include metrics such as MTTD, MTTR and Average Vendor Security Rating as a few examples. The purpose of these lists is to help us understand where we are, map where we are heading, and work with our peers to reduce risk and exposure to threats.

The cybersecurity industry is still grappling with the rather new challenge of finding the right recipe for the right metrics. We see a range of leading firms and cybersecurity leaders intensively debating and writing on this topic. From Google security leadership to metrics aficionados and naturally the risk rating leadership, all are well focused on “what needs to be measured”.

While it’s a good start to know WHAT metrics to measure, the real challenge is understanding HOW to streamline continuous measurements.

Metrics can’t stand alone.

Metrics need to be interconnected to provide a dynamic view of our organization’s security landscape and how we’re performing against a range of parameters, among them risk tolerance and policies. But in todays’ reality there’s a major gap between cybersecurity measurements and a real-time, comprehensive understanding – such an understanding would allow the cybersecurity leadership to see what's actually happening, proactively spot gaps, prioritize the most critical risks to the organization and execute an action plan accordingly.

So, even if I would share in this article the top ten metrics, I think are the most important to measure, it would only be the first step and would depend on the particular purpose and audience of your particular organization. The real power comes from correlating your metrics—understanding how one variable influence another and creating a dynamic, comprehensive narrative about the organization's security performance.

Why current methods for metrics are failing

In my work with security organizations, I’ve encountered three common (yet inefficient) approaches to measuring cybersecurity effectiveness. First, there’s the overwhelming reliance on spreadsheets—a sea of endless rows and columns, with metrics meant to represent the organization’s security posture, but often only add to the complexity.

Second, there’s the attempt to integrate analytics tools with cybersecurity tools, which creates a disconnect, as data professionals typically lack the nuanced understanding of security, while cybersecurity experts may not fully grasp the data analytics side. Finally, many organizations turn to the Big Four consulting firms, only to receive yet another massive spreadsheet.

Each of these approaches reveals the same core issue: they lack real applicability, leaving security teams in the dark rather than equipped to act. These methods yield static results; they are cumbersome, manual and stand-alone whereas security is constantly evolving and interrelated.

Security leaders cannot capture something so fluid and complex with tools that are frozen in time. They need something agile that connects the dots and places measurements (of performance, risk, threats) in context.

I have also learned from customers who have spent years and millions of dollars building their own metric automation programs that these are the key challenges: (1) Identifying which data is truly important (2) Continually collecting and maintaining the data (3) Incorporating the security context when it’s the data analysts in charge of managing the data. It is no wonder that so many customers give up on inhouse metric programs after investing so much time and money.

You need real-time data that goes beyond being static numbers. This data needs to be flexible, showing historical trends as well as being adaptable to the perspectives that matter most today. Only then can your organization truly grasp what’s happening, identify gaps, and take meaningful, prioritized action.

A key example: Vulnerability Prioritization

There are countless examples of how correlating metrics can make a real difference. Here's one that I see our customers find especially valuable – Vulnerabilities. A vulnerability management solution might flag 1,000+ endpoints as critical. But how do you know which ones to address first?

By correlating vulnerability data with asset management information, you can gain key insights into which business units those endpoints belong to.

You can take it a step further by adding identity security data: Which users are connected to these endpoints? Are they admins? Do they have access to sensitive financial or intellectual property data? Have any of these users been targeted by phishing attacks?

This automated lens of enriched context (rather than a siloed list of metrics) allows you to prioritize vulnerabilities based on their actual risk to your business, ensuring your actions align with the most critical objectives and business impact.

The same would be true when prioritizing the endpoints without any coverage (by correlating data from Crowdstrike and Kandju), or prioritizing unscanned projects (by correlating data from Skyk and GitHub), or prioritizing which users haven't offboarded properly (by correlating data from Workday and Azure).

Unlocking the Full Potential of Security Metrics

The true power of metrics lies in their ability to help prioritize. Only by moving beyond isolated "top ten metrics to measure" lists can security leaders and teams identify interrelated patterns that span multiple layers of their security stack. This shift not only unlocks deeper insights but also drives more efficient workflows and leads to more impactful outcomes.

About the Author

Shirley Salzman, CEO and Co-Founder of SeeMetrics, a data fabric for risk management allowing security teams to measure the performance of people, processes, and technologies against various security policies, risks, and threats. Empowered by SeeMetrics, security organizations reduce risk, improve collaboration, enforce policies and govern cyber security with confidence. Shirley brings over a decade of experience in commercial leadership (Percepto, Contguard, and Logic Industries). Prior to her high-tech career, Shirley worked for global policy and strategy firms such as the German Marshall Fund of the U.S. and the Institute for Policy and Strategy at the Interdisciplinary Center, Herzliya, Israel. Shirley holds an MA with honors in International Security and Non-Proliferation from King's College, London.

Shirley can be reached online at https://www.linkedin.com/in/shirleysalzman/?originalSubdomain=il and at our company website https://seemetrics.co/

Now Is Not the Time to Cut Back on Security Teams

By Dr Nick New, CEO and Co-Founder of Optalsysys

Generative artificial intelligence (AI) is revolutionising the way businesses operate. The widespread adoption and integration of models, such as OpenAI's ChatGPT and Google's Gemini, into everyday organisational processes has resulted in the seismic growth of the global market, which is expected to reach $1.3 trillion in 2032.

The rapid advancement of AI models has created a highly competitive environment where companies are channelling unprecedented resources into AI development. However, the extreme pressure to keep up and innovate is overshadowing an equally critical priority — AI safety.

Security is the backbone of companies

Despite the immense potential and excitement over generative AI, its adoption has yet to be universal. A recent study by CIO found that 58% of organisations haven't adopted AI due to cybersecurity concerns.

As AI technologies evolve, so do the types of cyber-attacks capable of disrupting businesses. Yet, many companies are scaling back their security teams — the very units tasked with protecting sensitive data.

Mass layoffs within information security departments have become alarmingly common. Demand for cybersecurity professionals has fallen by 32%, and even large corporations, such as ASDA, have cut their internal security teams.

These cuts come at a time when data breaches linked to AI are becoming a growing risk. For example, ChatGPT has been manipulated into generating Windows 10 and 11 keys, leading to significant security breaches. User prompts can also reveal sensitive business information, which may be stored without encryption. Studies reveal that 24.6% of employees have entered confidential documents, and 5.4% have input payment card information when asking generative AI models a question.

Such mismanagement of AI can damage an organisation's trust and credibility and expose it to legal liabilities and regulatory fines. In the UK alone, businesses have incurred over £44bn worth of damages relating to cybersecurity breaches.

Technology holds the key to next-level security

Governance policies, compliance measures, and education programmes are critical for companies looking to combat generative AI's potential security threats. However, organisations must also invest in privacy-enhancing technologies (PETs) to strengthen their defences.

Most companies handle sensitive and financially valuable information, which means the risk associated with a potential cybersecurity breach is staggering. PETs can act as a powerful complement to existing security measures.

PETs enable secure exchanges among organisations while ensuring confidentiality and compliance without exposing vulnerabilities. For instance, Fully Homomorphic Encryption (FHE) allows computations on encrypted data without the need to decrypt it. This means that data can remain confidential throughout AI processing, preventing sensitive data from being exposed even during complex computations. Other tools, such as Data Loss Prevention (DLP), can monitor and control the movement of sensitive information, which helps prevent data leaks and ensures that sensitive data is not shared or lost.

Whilst no solution can guarantee complete security, especially given AI's constant evolution, the integration of PETs represents a positive step towards protecting sensitive data. The future of cybersecurity in the AI era lies in organisations combining robust internal security measures with these advanced technologies.

The case for security teams

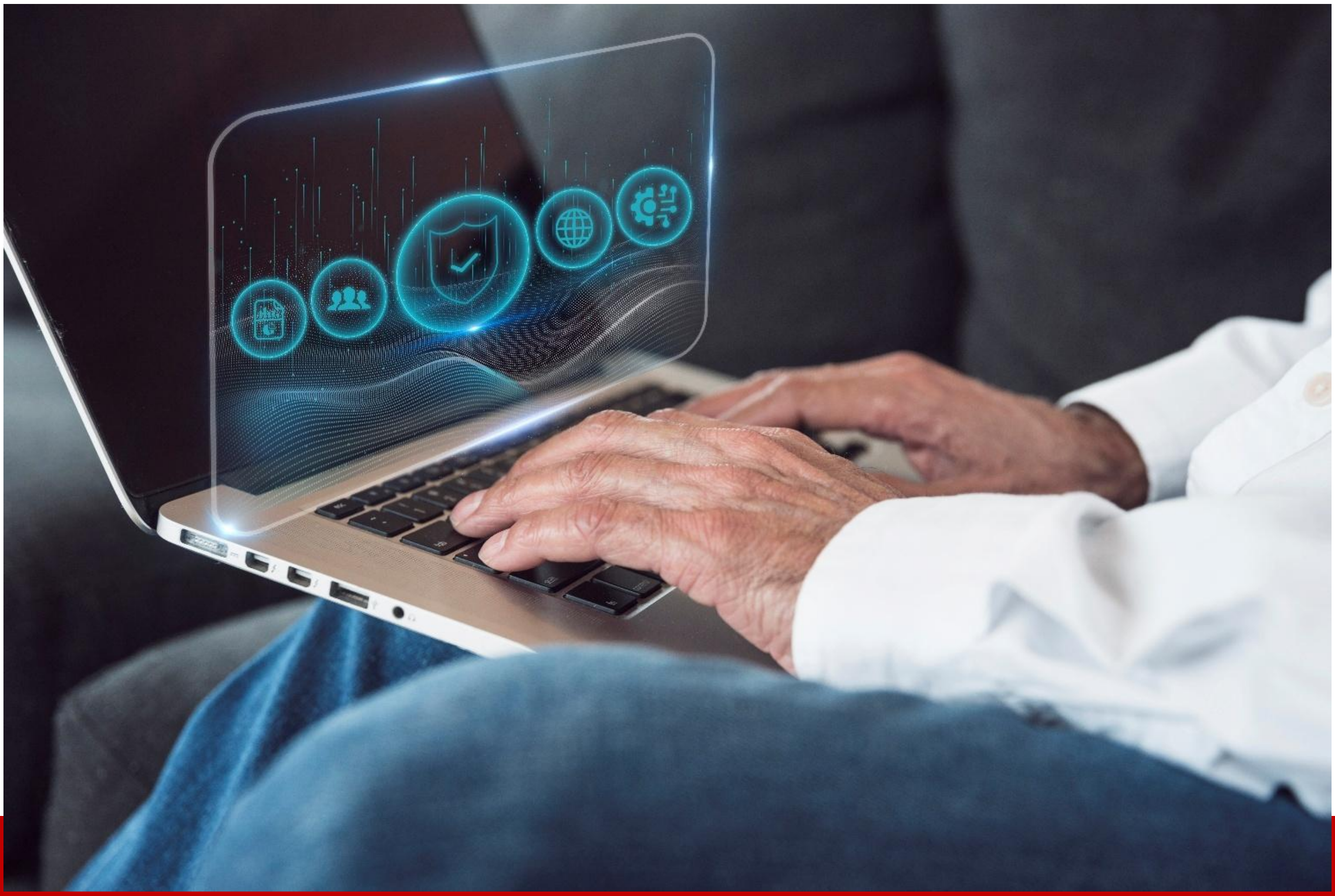
The challenge when deploying generative AI is ensuring the confidentiality of sensitive data whilst leveraging AI's capabilities. To tackle this, organisations need to take a multidisciplinary approach, employing and retaining key security personnel and using innovative PETs. This ensures businesses can enjoy the benefits of AI whilst keeping valuable data secure and private.

Organisations should view the role of CISOs and their teams not as an expense but as investments. The cost of a dedicated security team is minimal compared to the reputational and financial damage caused by a cyberattack. In the ever-changing technological landscape, CISOs and their supporting team have never been more critical to business success. Now is the time for organisations to focus on safeguarding their users' data rather than focusing on AI growth at all costs.

About the Author

Dr Nick New, CEO and Co-Founder of Optalysys. With a PhD in Optical Pattern Recognition from Cambridge, Nick has a strong foundation in optical technology. Before Optalysys, he led Cambridge Correlators, shaping their technical development and international growth. At Optalysys, Nick is pioneering advancements in silicon photonics and FHE.

Nick can be reached at our company website https://optalysys.com/



One Vendor Delivers 100% Protection And 100% Detection Visibility in MITRE ATT&CK Evaluation

Cynet achieved these results without configuration changes.

By George Tubin and Michael Newell, Cynet

Priority number one for cybersecurity leaders across small-to-medium enterprises (SMEs) and managed service providers (MSPs) is to ensure IT environments are up and running. To proactively minimize the risk of a data breach, it's crucial to keep tabs on a rapidly evolving cybersecurity vendor landscape and continually reassess which solutions are most effective. The recent release of the 2024 MITRE ATT&CK Evaluation — cybersecurity's most trusted vendor assessment — offers an answer key. This practical guide distills performance insights and guidance to interpret the results.

Cynet was the sole vendor to deliver 100% Visibility and 100% Protection in the 2024 Evaluation. The All-in-One Cybersecurity Platform detected every threat tested in the Detection Phase and blocked all attacks simulated in the Protection Phase of the Evaluation. Plus, Cynet achieved the 100% detection with zero false positives.

“These 2024 MITRE ATT&CK Evaluation results reflect our entire team’s commitment to secure success for Cynet partners, customers, and end users,” says Cynet Founder & CEO Eyal Gruner. “Achieving 100% Detection Visibility and 100% Protection is a motivating milestone that affirms the compelling advantages Cynet’s All-in-One Cybersecurity Platform is enabling for organizations around the world.”

These 2024 results build on Cynet’s record-breaking performance in the 2023 MITRE ATT&CK Evaluation when, for the first time ever, a vendor achieved 100% Visibility and 100% Analytic Coverage with no configuration changes. It should be noted, however, that MITRE does not rank vendors or declare “winners.” Instead, cybersecurity leaders must interpret the data to determine which solution best fits their organization’s unique needs.

What is the MITRE ATT&CK Evaluation?

MITRE is a nonprofit foundation that supports private sector companies “solving problems for a safer world.” Their annual ATT&CK Evaluation is regarded as the most rigorous and unbiased technical trial of cybersecurity platforms.

- MITRE emulates real-world attacks in a controlled lab environment to evaluate how vendor solutions behave against a set of threats introduced in the exact same manner.
- Vendor solutions are tested consistently, without external, extraneous variables to influence the results as in real-world deployments.

This methodology is designed to evaluate the efficacy of a solution at detecting the discrete steps an adversary could take to execute a cyberattack. Because MITRE emulates the techniques of prominent threat groups, each technique presented represents what is plausible to play out in a real-world scenario.

For vendors, the Evaluation is an opportunity to demonstrate how their solution detects the threats presented and provides useful information for each detection.

2024 RESULTS

Cynet delivered 100% Detection Visibility, perfectly detecting every attack action using no configuration changes and no delays.

Threat detection is the core competency of an endpoint protection solution. Detecting attack steps across the MITRE ATT&CK sequence is critical for protecting the organization. Missed steps can allow an intrusion to expand and ultimately lead to a breach or other catastrophic outcomes.

In 2024, the attack sequence was executed over 16 steps, which were broken out into 80 malicious sub-steps. During Cynet’s testing, 3 of the sub-steps were not executed due to technical reasons and are considered N/A (not counted) which resulted in 77 total sub-steps executed. **Cynet detected every single one of the 77 sub-steps**. Cynet had ZERO misses in this year’s MITRE testing and detected 100% of attacks over Windows and MacOS devices as well as Linux servers.

All 77 detections were performed without the need for configuration changes. Leaders reviewing vendor outcomes can see which vendors could accomplish detections only *after* they were allowed to make configuration changes.

Cynet delivered 100% Protection, blocking every attack sequence attempted. Around half of the participating security vendors were unable to test all 10 attack steps planned for the Protection tests due to technical issues. MITRE was able to execute all 10 attack steps for Cynet. **Cynet blocked every one of the 10 attacks steps — allowing no malicious activity to execute**.

The chart below shows each participant's Protection rate as well as the volume of steps blocked and the volume of steps executed (steps blocked/steps executed).

Cynet delivered 100% Prevention, blocking every attack in the first step attempted. Protection measures whether any sub-step in a Protection step was blocked. For example, if a step consisted of 5 sub-steps, a vendor could miss the first four, block the fifth and consider the entire step blocked. Cynet defines Prevention as how quickly (early) in each of the 10 attack steps the threat was prevented.

Prevention measures the percentage of sub-steps that were blocked from executing. Ideally a vendor would block the first sub-step in every step tested so that every subsequent sub-step in the step was considered to be blocked. By this measure, Cynet is the only vendor to achieve 100% Prevention - blocking every one of the 21 Protection sub-steps from executing.

Cynet is the leader in Overall Threat Visibility and Protection

This chart compares each vendors overall visibility with prevention rate. Prevention rate is used as it's a more rigorous measure of the solutions ability to block malicious attacks.

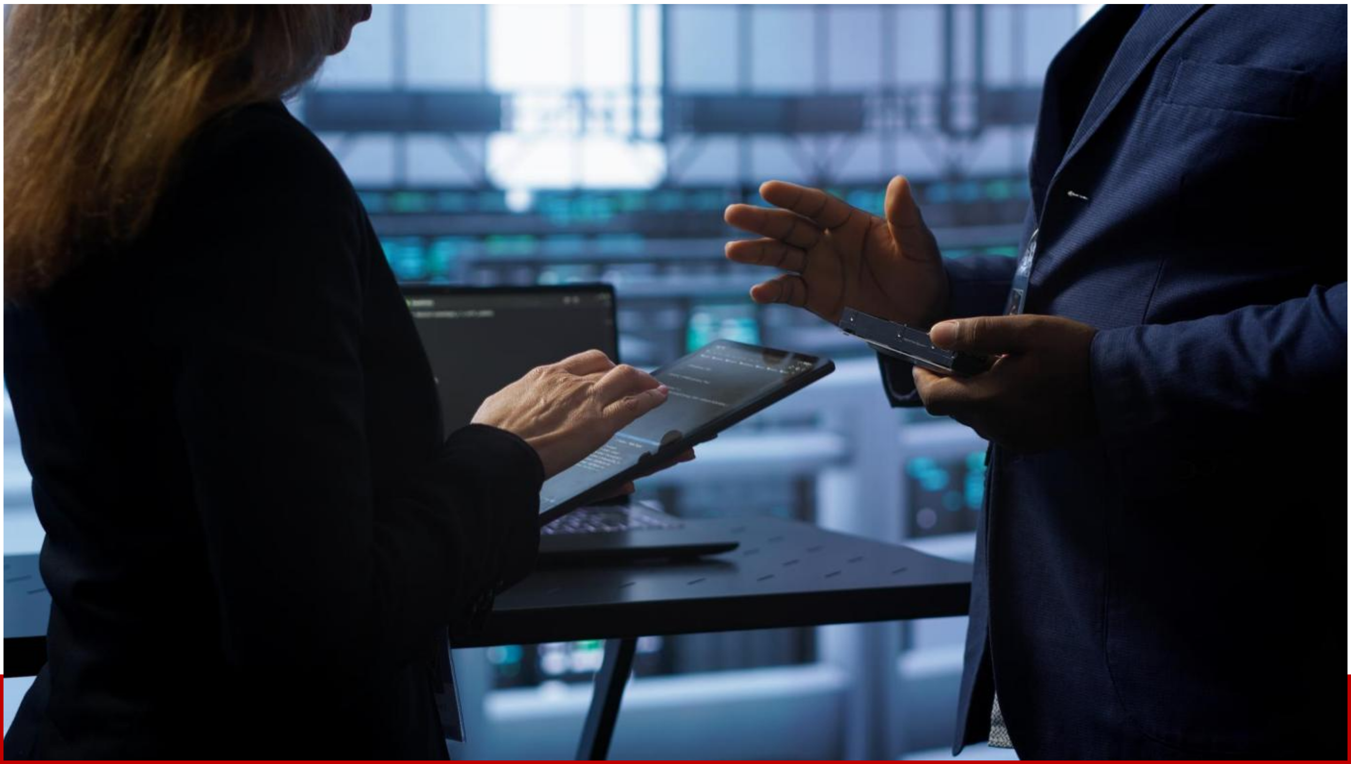
Conclusion

Identifying which cybersecurity vendor can best protect your business or your clients is one of the first and most impactful steps a cybersecurity leader can take. The 2024 MITRE ATT&CK Evaluation results substantiate why Cynet's All-in-One Cybersecurity Platform is an increasingly popular solution for fast-growing SMEs and MSPs. By demonstrating that highly effective protection can be also be intuitive and affordable, Cynet has set a standard that competing vendors must strive to emulate.

Sign up to see Cynet in action today.

About the Authors

George Tubin and Michael Newell are teammates at Cynet. Cynet’s All-in-One Platform unifies a full suite of cybersecurity capabilities on a single, simple platform, backed by 24/7 SOC support. For more info, visit: https://www.cynet.com



How CISOs Can Master Operational Control Assurance — And Why It Matters

By Dale Hoak, Senior Director of Information Security at RegScale

Chief Information Security Officers are facing rising pressure to ensure robust security and compliance across globally distributed environments. Managing multiple security tools and platforms while avoiding inconsistencies and gaps in coverage is an ever-growing challenge.

Digital transformation and the shift to the cloud introduces even more areas of concern. With sensitive data distributed across multiple cloud providers, CISOs struggle to maintain visibility into these complex and ephemeral environments. As both the technology and threat landscapes continue to change, it's all but impossible for CISOs to manage security and risk using traditional, manual approaches.

Dynamic operational control assurance offers a way forward. It's an approach that offers both automation and visibility into different security controls and management areas across the distributed environments. It's particularly valuable in complex, rapidly changing environments where traditional methods just aren't sufficient to address evolving risks and diverse compliance requirements.

Below, we'll explore in depth how dynamic operational control assurance makes it easier for CISOs to manage security, risk, and compliance effectively.

First, What Is Dynamic Operational Control Assurance?

Dynamic operational control assurance is an approach that leverages both AI capabilities and Open Security Controls Assessment Language (OSCAL) to implement compliance as code in the continuous integration/continuous delivery (CI/CD) pipeline, ensuring operational readiness and legal defensibility.

Dynamic operational control assurance offers several key benefits, including:

- Real-time monitoring and assessment of control effectiveness
- Integrated security measures throughout the dev lifecycle
- Proactive risk management through continuous controls monitoring (CCM)
- Visibility across the enterprise, empowering CISOs to make data-driven decisions

Essentially, dynamic operational control assurance enables organizations to identify risk-relevant events during runtime, aggregate information to meet local or global requirements, and assess the system's security capabilities. This enables security teams to optimize security and compliance and act proactively instead of reactively.

How To Implement Dynamic Operational Control Assurance

To adopt a dynamic operational control assurance approach, organizations must embed compliance as code (the practice of codifying compliance controls into machine-readable formats) into their CI/CD pipeline. This in turn will help them achieve proactive risk management, increased visibility, and stronger security.

1. Adopt OSCAL

First, CISOs need to adopt OSCAL. OSCAL provides a standardized, machine-readable format for data in order to facilitate consistent communication across various platforms and tools. By representing security controls, profiles, implementations, and assessments in standardized formats (XML, JSON, and YAML), OSCAL makes it possible to automate security control documentation, implementation, and assessment tasks.

Implementing OSCAL also improves interoperability among security management and assessment tools, streamlining compliance with a wide variety of cybersecurity frameworks and standards. It's an essential step for any successful dynamic operational control assurance plan.

2. Map Controls and Update Rules

To effectively manage different frameworks — for instance, FedRAMP, GDPR, and PCI DSS — companies must be able to map compliance controls easily. OSCAL can help with this, enabling automation and improving consistency.

Having a clear process for mapping controls will in turn make it faster and easier to update code-based rules when compliance requirements change, and it will help CISOs adapt quickly to evolving regulations. It also establishes a clear, machine-readable audit trail that demonstrates ongoing compliance for auditors and other stakeholders.

3. Implement Compliance as Code

Implementing compliance as code transforms traditional manual compliance checks into automated, repeatable processes that can be integrated directly into the CI/CD pipeline — which in turn enables continuous validation of security and regulatory requirements at each stage of software development. By embedding compliance checks into their pipeline, organizations can also reduce the risk of non-compliance and minimize the costly, reactive work that's often required when compliance is treated as a separate, end-of-cycle activity. This approach not only accelerates the development process but also ensures a consistent approach to maintaining security standards across different projects and teams.

Additionally, by incorporating compliance checks into Infrastructure-as-Code (IaC) templates, organizations can also be sure that newly provisioned resources will meet security and compliance requirements. The result? Automated enforcement, reduced manual work, and consistent compliance across an organization's entire infrastructure and application landscape.

4. Leverage AI

While OSCAL and compliance as code play essential roles in automating compliance, AI is also integral. AI and machine learning (ML) power advanced threat detection systems that can identify patterns and potential risks more quickly and accurately than traditional methods. These systems are able to detect and respond to compliance risks in real-time, making it easier to maintain security and compliance standards.

AI also enables predictive modeling, which allows organizations to anticipate and mitigate potential threats before they materialize. This proactive approach enhances overall security posture and strengthens compliance efforts.

Coupled with OSCAL and compliance as code, AI will help CISOs build a more robust, adaptive, and efficient security ecosystem from code to cloud.

Operational Readiness and Legal Defensibility

Many CISOs are concerned about operational readiness and legal defensibility in distributed environments — and rightly so. Luckily, dynamic operational control assurance provides real-time visibility into control effectiveness through continuous monitoring, allowing organizations to swiftly identify and address compliance issues.

D operational control assurance also enables evidence-based decision-making and ensures that compliance with all relevant regulations is documented. This makes it simpler to demonstrate compliance and justify security choices, strengthening defensibility for a CISO and their organization. It also increases operational readiness and minimizes risk and liability for organizations faced with a compliance issue or lawsuit.

Maintain Robust Security from Code to Cloud

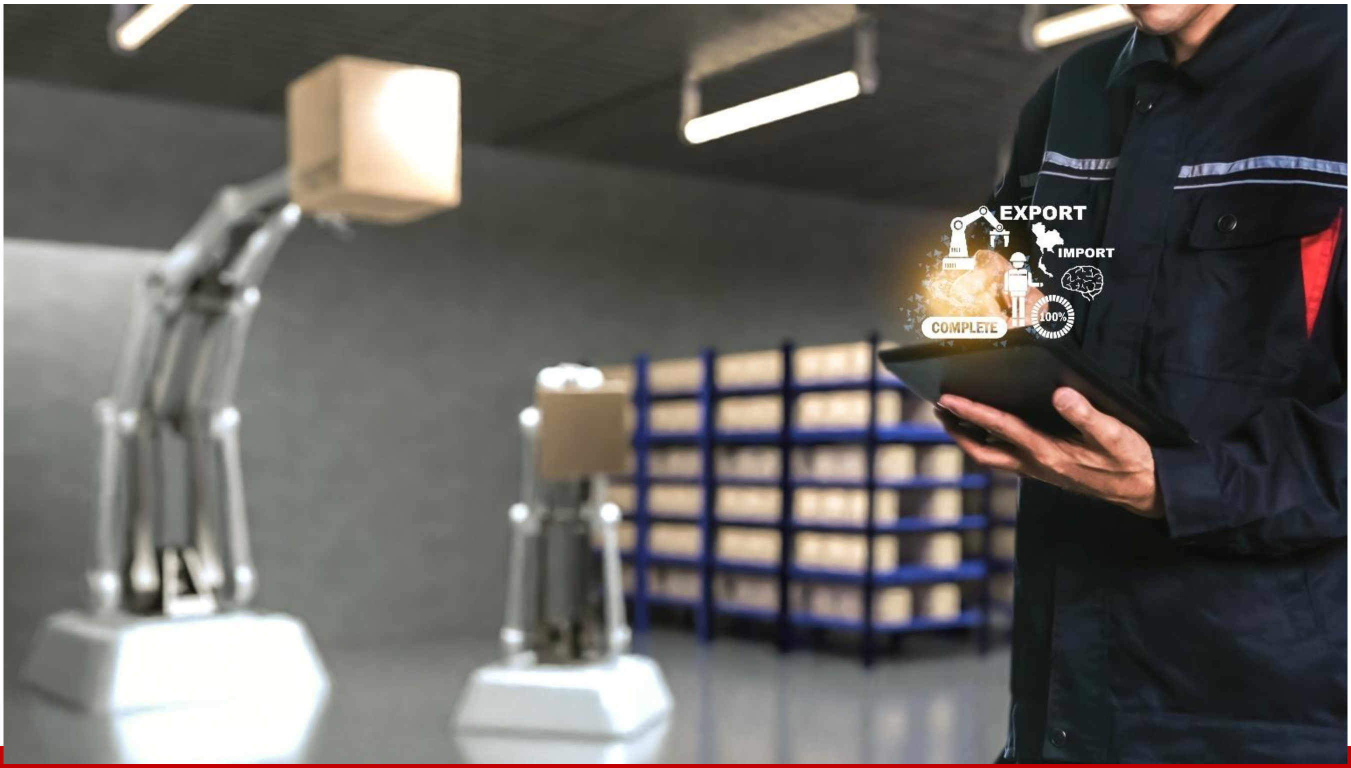
The bottom line on dynamic operational control assurance? It's a way for CISOs to maintain robust security from code to cloud by implementing and automating comprehensive security and compliance measures throughout the entire software development lifecycle.

Dynamic operational control assurance also integrates security practices from the initial planning and design stages to deployment and maintenance, guaranteeing that security is a fundamental component of the development and deployment process. By leveraging automation tools and integrating security checks into CI/CD pipelines, CISOs can ensure consistent application of security measures across all environments.

Ultimately, dynamic operational control assurance results in more secure software and infrastructure, as well as improved security posture and compliance. It might even return some of those weekends and late nights to resource-strapped GRC teams. And who wouldn't want that?

About the Author

Dale Hoak is a seasoned Cybersecurity and Technical Operations Leader with a distinguished career in the U.S. Navy, where he designed secure, mission-critical systems. Currently the Director of Information Security at RegScale, Dale built RegScale's security program from the ground up, enhancing compliance, risk management, and operational effectiveness. Recognized for his excellence in building Security Operations Centers and Threat Intelligence programs, Dale's tactical leadership has led to significant achievements, including disaster recovery and business continuity planning for the DoD, rapid deployment of communication packages for Navy Seal Teams, and the creation of training programs for system administrators. His hands-on approach and commitment to efficiency have made regulatory compliance faster and more accessible. Dale can be found on LinkedIn here.



The Cyber Resilience Act: How Manufacturers Can Meet New EU Standards and Strengthen Product Security

By Eystein Stenberg, CTO, Northern.tech

Cybersecurity has become a leading priority for manufacturers of embedded systems and IoT devices. The rapid proliferation of these technologies, combined with their increasing integration into critical infrastructure, has made them prime targets for cyberattacks. In response, the European Union created the Cyber Resilience Act (CRA) as a landmark regulation to protect the digital ecosystem and ensure security by design throughout the entire lifecycle of products with digital elements (PDEs).

The CRA establishes stringent requirements for manufacturers, addressing the entire lifecycle of connected products, from development to end-of-life. These measures exist to protect all users by minimizing vulnerabilities, fostering transparency, and ensuring the secure deployment of updates. For global manufacturers, aligning with these regulations is essential, as sweeping noncompliance penalties drastically affect business success. Adherence to the CRA's security requirements is necessary to remain competitive in an increasingly regulated market.

Given the complexity and unique scope of the CRA, the regulation presents key challenges requiring proactive, actionable strategies to remain compliant throughout its enforcement. Successful industry players will adapt its processes to ensure security and transparency are at the forefront of every stage of the product lifecycle, and thereby, achieve compliance.

Essential requirements and key mandates of the CRA

The EU Cyber Resilience Act (CRA) establishes comprehensive requirements to enhance the cybersecurity of products with digital elements (PDEs), ensuring their security from design to decommission. These essential requirements, detailed in the annexes, outline measures that manufacturers must implement, including:

- **Continuous monitoring:** Manufacturers must continuously monitor its products for vulnerabilities, including conducting regular security tests and reviews.
- **Transparency through SBOMs:** A detailed, machine-readable Software Bill of Materials (SBOM) is required, providing an inventory of all software components and dependencies. This level of transparency enables full disclosure and timely vulnerability identification for any interested parties.
- **Vulnerability disclosure mechanisms:** Manufacturers must establish accessible and reliable channels for publicly reporting vulnerabilities, ensuring accountability and expediting resolution processes. Disclosure measures must report vulnerabilities through a single point of contact.
- **Timely remediation via secure updates:** Vulnerabilities must receive prompt remediation through secure software updates, made available to the general public immediately upon identification. Robust over-the-air (OTA) update systems are essential to deploy these patches quickly and efficiently without exposing devices to additional risks.

Together, the CRA measures emphasize a lifecycle approach to cybersecurity, mandating manufacturers integrate security throughout its products to maintain integrity and safety long after initial production. These requirements enhance the resilience and reliability of connected products while safeguarding the end user.

Classification of products

The CRA focuses on all “products with digital elements (PDEs)” sold in the European Union. Differing from other cybersecurity efforts, the CRA **mandates** its sweeping regulations to ensure the safety of these offerings. For products that perform a security function, Annex 3 delineates specific categories of PDEs with additional compliance requirements. Including a conformity assessment and auditing regulations, these categories fall under two classes:

- **Class I** products include software and hardware-software combinations essential for everyday cybersecurity and network management at the consumer level. Class I products encompass solutions like VPNs, antivirus software, password managers, and smart home security devices.
- **Class II** products include software and hardware-software combinations focused on critical cybersecurity functions at the enterprise level. Class II products focus on securing virtualized

environments and ensuring robust system protection through means such as firewalls, intrusion detection systems, and tamper-resistant microprocessors.

The CRA's expansive legislation lays the foundation for securing all products with digital elements through the aforementioned requirements. These security requirements are substantial lift, demanding preparation and further understanding of the scope and, most importantly, a manufacturer's responsibility to achieve compliance successfully.

Scope of the CRA and its impact on different industries

The CRA’s scope is vast, covering a wide range of products, including:

- Internet of Things (IoT) devices, such as smart home systems and wearables.
- Embedded systems used in industrial automation and critical infrastructure.
- Software and firmware integral to connected devices, especially those concerning remote data processing.

The CRA focuses on ensuring that security measures are baked into products at every level, from hardware to software. Products with digital elements (PDEs) are everywhere in today’s consumer market, inadvertently creating possible attack vectors. Bolstering comprehensive security protects end users.

Excluded industries

While the CRA has broad applicability, some industries are exempt due to existing regulatory frameworks. These include:

- Medical Devices: Governed by the EU Medical Devices Regulation.
- Military Equipment: Subject to defense-specific legislation.
- Automotive: Already regulated under the UNECE WP.29 cybersecurity framework.

By carving out these exemptions, the CRA avoids redundancy and allows specialized regulations to handle industry-specific security challenges.

Although an EU regulation, the CRA’s implications extend far beyond Europe. Companies operating outside the EU must still ensure compliance in order to maintain access to the EU’s lucrative consumer base: the regulation applies if a company sells products in the EU. Perhaps similar to GDPR, this will, in turn, create a ripple effect, encouraging the adoption of CRA-aligned practices across the globe and setting a higher standard for cybersecurity worldwide.

Challenges in complying with the CRA

The CRA's requirements center around providing security and traceability throughout the lifecycle of a PDE; the legislation outlines key points that present challenges to manufacturers looking to comply, including:

Secure by default

The CRA mandates a *secure by default* approach, requiring manufacturers to prioritize security at the design stage and throughout the product lifecycle. Manufacturers must build products that are inherently secure, with configurations optimized for cybersecurity rather than user convenience or time-to-market, for example. While requiring design-level security ensures a stronger baseline of protection, it can significantly increase development time and costs, especially for organizations without adequate security practices. Balancing functionality, usability, and security is particularly challenging for resource-constrained manufacturers.

SBOM maintenance

Compiling a machine-readable Software Bill of Materials (SBOM) is a pivotal requirement of CRA compliance. Notably, maintaining an accurate and up-to-date SBOM across complex supply chains requires substantial preparation. Software components often originate from multiple vendors, open-source libraries, or third-party suppliers, each with its own update cycles and vulnerabilities. The fragmented software ecosystem creates difficulties in tracking component changes, ensuring compatibility, and responding promptly to emerging threats.

Vulnerability disclosure

The CRA requires transparent and timely vulnerability disclosure processes, enabling stakeholders to identify and report risks effectively. However, managing this process without compromising proprietary information or customer trust can be challenging. Manufacturers must establish secure communication channels, balance speed with accuracy, and coordinate with affected parties to resolve issues without introducing new risks.

Secure updates

Delivering reliable over-the-air (OTA) updates is critical for addressing vulnerabilities and maintaining compliance. However, ensuring the security and integrity of these updates is no small feat. Manufacturers must implement robust mechanisms to authenticate updates, protect against tampering, and provide seamless deployment across diverse devices and environments. Any lapse in these areas could lead to compliance violations or, worse, expose devices to further exploitation.

Proactive strategies for CRA compliance

Manufacturers must adopt a proactive and integrated approach to device security to overcome CRA compliance challenges. While pushing to align with the CRA, common security best practices stand to bolster compliance, including:

Proportionate security processes to cybersecurity risk

As the crux of the CRA, integrating security into the product development lifecycle is the core proactive success strategy. A *shift-left* approach, where security considerations are embedded early in the design and development phases while there is an ongoing process to test and remediate, ensures that vulnerabilities are addressed before they reach production. Proportionate security processes and policies like security assessments, automated testing tools, and secure coding practices must be defined compared to the product cybersecurity risk level. Doing so lowers the risk of vulnerabilities in design and shortens the time to remediate them when they occur while products are in production.

System and process integration

Compliance efforts often fail due to fragmented systems and misaligned processes. By integrating tools and aligning teams, manufacturers can work to create a unified security ecosystem. Centralized dashboards for tracking SBOMs, vulnerabilities, and update deployments provide real-time visibility, enabling faster decision-making and reducing the likelihood of errors or oversight.

Adopting secure by default practices

Building *secure by default* products involves adopting security best practices at every stage of development. These include secure boot processes, encryption, access controls, and minimizing the attack surface of devices. Additionally, regular security audits and penetration testing ensure that products maintain high-security standards throughout their lifecycle. A *secure by default* approach not only meets CRA requirements but also builds customer trust and reduces long-term maintenance costs and brand risk.

Leveraging robust OTA solutions

Professional over-the-air (OTA) update solutions are necessary for efficient security and compliance management of PDEs. These solutions are the backbone of device security, providing a secure and scalable way to deliver patches, feature updates, and configuration changes. By leveraging robust OTA platforms, manufacturers can ensure updates are cryptographically signed, tamper-proof, and deployed seamlessly across diverse device fleets. A proactive approach to software updates addresses vulnerabilities promptly and reinforces trust in connected products.

Strengthening security in a connected world

The Cyber Resilience Act (CRA) is a comprehensive initiative toward fostering a secure and trustworthy global digital ecosystem focused on security and transparency. By adhering to its mandates, manufacturers play a crucial role in advancing cybersecurity standards, safeguarding consumer interests, and driving innovation across industries, in addition to avoiding severe noncompliance penalties that have the potential to fully remove an offering from the European market.

The CRA sets a clear roadmap for integrating robust security practices into every stage of a product’s lifecycle. Overall, it presents an opportunity to demonstrate leadership in building resilient and secure products that meet rising global expectations. Aligning with the CRA ensures regulatory adherence while strengthening an organization's market position, establishing it as a pioneer in creating a safer, more resilient, connected world.

About the Author

Eystein Stenberg is the CTO of Northern.tech, a leader in Device Lifecycle Management, and the creator of Mender, the market-leading solution for robust, secure, and customizable over-the-air (OTA) software updates.

Eystein can be reached online at:

Email: eystein.maloy.stenberg@northern.tech
LinkedIn: https://www.linkedin.com/in/eysteinstenberg/
Company Website: https://northern.tech/

The Illusion of Truth: The Risks and Responses to Deepfake Technology

By Rohit Nirantar, Cybersecurity Professional

Abstract

In the age of information, where the line between reality and fiction is increasingly blurred, deepfake technology has emerged as a powerful tool with both immense potential and significant risks. Deepfake technology, utilizing sophisticated artificial intelligence (AI) and machine learning techniques to generate hyper-realistic audio and video, poses significant security threats alongside its innovative applications. This article provides an in-depth exploration of deepfake technology, illustrates its potential for misuse in various domains including misinformation and identity fraud, and proposes a comprehensive framework for mitigating these risks through technological, educational, and legislative measures.

How Deepfake Works

Deepfake technology relies on a complex process involving artificial neural networks. These networks are trained on vast amounts of data, such as images and videos, to learn patterns and recognize features. Once trained, the network can generate highly realistic contents, often indistinguishable from the original. To understand the technical foundations of deepfake technology, one must look at the fields of machine learning and artificial intelligence. At the core of this technology are Generative Adversarial Networks (GANs) and Deep Learning.

Generative Adversarial Networks (GANs)

GANs consist of two neural networks—the generator and the discriminator—engaged in a continuous loop of competition. The generator creates images or sounds that mimic the real data, while the discriminator evaluates their authenticity. Over time, the generator learns from the discriminator's feedback, improving its outputs until they are indistinguishable from authentic data.

Deep Learning:

Deep learning has been pivotal in the advancement of deepfake, with convolutional neural networks (CNNs) being extensively used to analyze and replicate the minute details of human expressions and voices. These models are trained on extensive datasets containing millions of images and audio files, which they use to learn and replicate human features with startling accuracy.

The Dark Side of Deepfake

The increasing accessibility of deepfake technology due to advancements in AI presents both significant opportunities and considerable risks. On one hand, it facilitates creative content generation, enhances artistic expression and improves educational experiences. On the other hand, it poses serious threats, including fraud, the proliferation of misinformation, and social manipulation. Here are some of the most concerning applications of deepfake:

- **Disinformation and Propaganda:** Deepfake can be used to create false information that can alter public opinion, influence elections, and incite violence. For example, a deepfake video of a politician making controversial statements could damage their reputation and undermine their credibility.
- **Personal and Corporate Fraud**: Deepfake can bypass facial recognition software or imitate voices in voice-activated systems, which can compromise safe access or personal banking systems. Corporations face threats of espionage with deepfake used in phishing attacks to obtain sensitive information or manipulate stock prices through fabricated announcements from influential figures.

- **Harassment and Cyberbullying:** When people are portrayed in deepfake videos without their consent, it may lead to psychological distress, social rejection, and legal issues.
- **National Security Threats:** Deepfake has the potential to destabilize countries, foster international conflict, and produce misleading intelligence.

Mitigating the Risks of Deepfake

Combating the misuse of deepfake technology involves a multi-faceted approach that integrates technological solutions, legal frameworks, public awareness initiatives, and international cooperation. Various methods have been developed, each addressing different aspects of the deepfake detection challenge. Here are some of the key measures that can be applied to mitigate the risks associated with deepfake technology:

- **Technological Detection Techniques:**
    - **Digital Forensic Techniques:** These involve analyzing the digital fingerprints left behind by deepfake algorithms. By examining pixel-level characteristics, inconsistencies like unnatural blinking or distorted backgrounds can be detected.
    - **AI-Driven Detection:** AI-powered tools can analyze videos frame by frame, identifying inconsistencies in lighting, shadows, and facial expressions that may indicate manipulation.
    - **Blockchain for Verification**: To ensure the authenticity of digital content, blockchain technology can be used to create an immutable ledger of media files. Several companies utilized blockchain to verify the integrity of images and videos at the point of capture, making unauthorized alterations easily detectable.

- **Educational Initiatives and Public Awareness**

Increasing public awareness and education is pivotal for the early detection and resistance against misinformation spread by deepfake:

- **Media Literacy Programs:** Programs like MediaWise, a project funded by Google and run by the Poynter Institute, aim to educate young people and the general public on how to identify fake news, including content manipulated by deepfake technologies. They use real examples from recent elections where deepfake videos were employed to create confusion and spread misinformation.
- **Workshops and Training:** The prominent media outlets have organized workshops that teach journalists and content creators how to spot deepfake. These sessions often use real-life examples, such as manipulated speeches of political figures, to train attendees on the telltale signs of fabricated content.

- **Policy and Regulation**

Legislative action can also play a significant role in controlling the spread and impact of deepfake:

  - **Legal Frameworks:** The European Union's GDPR has been adapted to include rights against unauthorized use of biometric data, which can be extended to govern the use of personal images and videos in deepfake. Similarly, in the United States, the DEEPFAKES Accountability Act was introduced in Congress to criminalize the malicious creation and distribution of deepfake content.
  - **Corporate Policies:** Social media platforms like Facebook and Twitter have implemented specific policies to handle deepfake content. For example, Twitter's approach involves labeling tweets that contain synthetic media, whereas Facebook collaborates with third-party fact-checkers to identify and reduce the circulation of deepfake.

- **Industry and Academic Partnerships**

Developing and deploying technology solutions in partnership with various stakeholders is essential for a robust defense against deepfake:

  - **Industry Collaboration:** In response to the deepfake threat, major technology firms such as Microsoft have developed tools like Microsoft's Video Authenticator, which analyzes a video's content and gives a score indicating the likelihood it's been artificially manipulated.
  - **Academic and Industry Research:** Universities and tech companies are collaborating on new research initiatives to stay ahead of deepfake technology. For instance, partnerships like the Deepfake Detection Challenge (DFDC) launched by Facebook aim to spur the development of deepfake detection tools through global competitions.

- **International Cooperation:**
  - **Global Frameworks:** Promote international collaboration to develop unified legal standards and cooperative measures to prevent the global spread of malicious deepfakes. This includes sharing technologies, strategies, and intelligence across borders.
  - **Cross-Border Enforcement:** Work towards agreements for cross-border enforcement of laws against the creation and distribution of harmful deepfake content, recognizing that digital media transcends national boundaries.

Conclusion

Deepfake technology is a double-edged sword. While it presents significant risks, it also offers potential benefits. To harness the positive aspects of this technology while mitigating its negative impacts, a multi-faceted approach is necessary. This includes developing robust detection tools, educating the public about deepfake, and establishing strong legal frameworks to regulate their use. By working together, governments, technology companies, and individuals can ensure that deepfake technology is used responsibly and ethically, ultimately benefiting society as a whole.

As deepfake technology continues to evolve, it is imperative to remain vigilant, adapt to emerging threats, and promote the ethical and responsible use of this powerful tool.

Endnotes:

1. Chesney, R., & Citron, D. (2019). Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics. Foreign Affairs. https://www.foreignaffairs.com/

2. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Bengio, Y. (2014). Generative Adversarial Nets. Advances in Neural Information Processing Systems.

3. Paris, B., & Donovan, J. (2019). Deepfakes and Cheapfakes: The Manipulation of Audio and Visual Evidence. Data & Society Research Institute. https://datasociety.net/

4. Verdoliva, L. (2020). Media Forensics and Deepfakes: An Overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 982–992. DOI: 10.1109/JSTSP.2020.3002101

5. Microsoft. (2020). Video Authenticator Tool to Combat Disinformation. Microsoft AI Blog. https://blogs.microsoft.com/

6. Deepfake Accountability Act. (2019). U.S. Congress. https://www.congress.gov/

7. Sample, I. (2019). What Are Deepfakes – And How Can You Spot Them? The Guardian. https://www.theguardian.com/

8. Facebook AI. (2020). Deepfake Detection Challenge. https://ai.facebook.com/

9. Vincent, J. (2020). Deepfake Detection Algorithms Will Never Be Enough. The Verge. https://www.theverge.com/

10. General Data Protection Regulation (GDPR). European Union. https://gdpr-info.eu/

11. Nguyen, T. T., Nguyen, C. M., Nguyen, D. T., Nguyen, D. T., & Nahavandi, S. (2019). Deep Learning for Deepfakes Creation and Detection: A Survey. ArXiv Preprint. https://arxiv.org/abs/1909.11573

12. Kietzmann, J., Paschen, J., & Treen, E. R. (2020). Artificial Intelligence in Content Marketing: A Synthesis and Research Agenda. Journal of Business Research, 116, 273–285. DOI: 10.1016/j.jbusres.2020.05.001

13. Maras, M.-H., & Alexandrou, A. (2019). Determining Authenticity in the Age of Post-Truth Politics. International Journal of Information Management, 48, 43–50. DOI: 10.1016/j.ijinfomgt.2019.01.017

14. Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M. (2019). FaceForensics++: Learning to Detect Manipulated Facial Images. Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV). https://openaccess.thecvf.com/

15. Pogue, D. (2019). Deepfakes Are Getting Scary Good. How Do We Tell What's Real? Scientific American. https://www.scientificamerican.com/

16. Schick, N. (2020). Deepfake Videos: How to Protect Yourself and Fight Back. Consumer Reports. https://www.consumerreports.org/

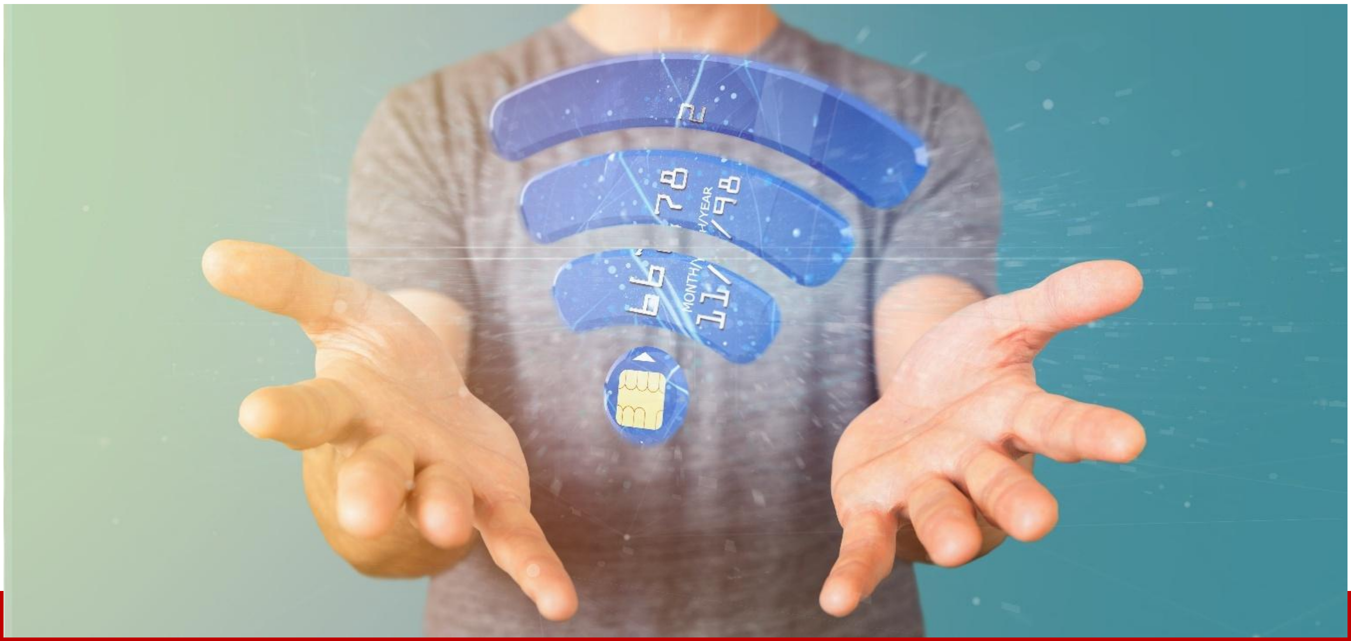
17. Citron, D. K. (2019). Sexual Privacy. Yale Law Journal, 128, 1870–1960. https://www.yalelawjournal.org/

18. Floridi, L. (2020). AI and Deepfakes: The End of Trust? Philosophy & Technology, 33(3), 385–389. DOI: 10.1007/s13347-020-00417-7

About the Author

Rohit Nirantar | CISM, PMP, Azure Security Engineer Associate, DevOps Engineer Expert

Rohit Nirantar is a Project Manager at Deloitte with over 18 years of experience in IT, specializing in application security, cybersecurity, and cloud security. He has successfully managed and implemented security solutions for global organizations, leveraging his expertise in secure cloud practices, threat management, and compliance frameworks. Rohit holds a diverse range of certifications in Information Security, Project Management, and Cloud Security. He is passionate about promoting cybersecurity awareness and fostering collaboration within professional communities. Rohit can be reached online at rohitnirantar@gmail.com.



The Internet of Things Design Challenges

By Milica D. Djekic

Developing an engineering project is a challenge by itself. In the practice, dealing with some product or service is very requiring and it can take a couple of phases from an initial idea unless the final solution. The Internet of Things (IoT) is a cyber-physical system which needs both – the good understanding of the hardware and software configuration, as well as the great management of the web service, so far. As a cutting-edge technology, the IoT has revolutionized the global high-tech industry landscape which thanks to such an endeavor has become much more accessible to many consumers across the world. The fact is the internet service is cheap, but in the majority of cases less reliable as those relying on that signal need to take care about safety and security of such a communication. In other words, the current tendencies dictate a demand for a better cyber defense which is extremely hard realizing in a reality as those projects are also a technological problem that must be tackled carefully, so far.

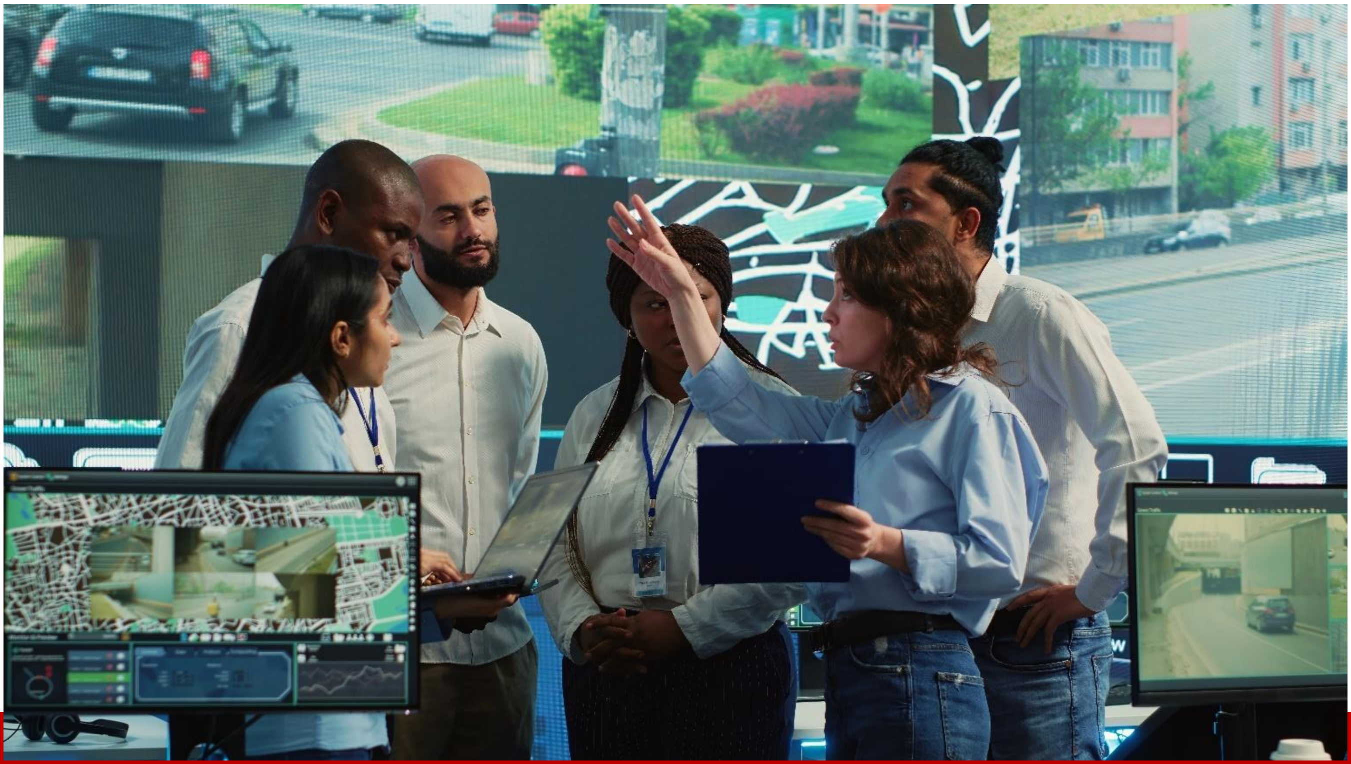
From this point of view, it's quite unthankful talking about all pluses and minuses of the IoT system design as some engineers believe that the web connectivity as a part of the internet as a critical infrastructure could be the main challenge, but – on the other hand - working on the software and hardware development and deployment might need an outstanding technical skill and some sorts of the deeply trickery adaptations, adjustments and brand-new ideas, so far. Serving in an R&D IoT department is something that seeks a big deal of creativity and intelligent approaches, because even if many industrial players have mastered to make such a technology yet need to learn a lot as any new project is a challenge requiring a new innovative and ingenious perspective in order to be resolved and launched on the marketplace, so far.

In so many cases, the IoT systems are truly a digital technology that looks for vetting engineers and coders who can meet demands of such a project. Apparently, sometimes it is needed to begin with skilled research that can make a road to the rest of the design phases suggesting how the project should appear at the end and responding on the very starting points of such a concern, so far. The majority of the high-tech security experts indicate that the cyber assurance requirements should be initial as they are well-aware about all the constrains of the messy prepared projects which can be deeply unsafe and unsecure in a technological fashion. Some experiences in the IoT industry show many marketplace actors especially in Asia deal with a pretty straightforward assembly industry purchasing fully developed semi-products, complying them and after making some program pushing such a solution through a testing phase practically not coping with any kind of the R&D at its genuine level, so far. Indeed, in the developed economies – it is common to start from nothing going step-by-step from one stage to the next for a reason those industries can offer something very novel and completely generated offering a progress to the entire humankind.

Indeed, the 4th industrial revolution came from the East as a response to the wiring issue and need for a better understanding of the wireless transmission of the information and as those two questions have been opened a couple of decades ago some ideas have come then, but as a very fast answer to such emerging attempts the majority of the Western countries have agreed those systems are not secure enough running the entire new trends in the technological ever-evolving ecosystem, so far.

About The Author

Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books “The Internet of Things: Concept, Applications and Security” and “The Insider’s Threats: Operational, Tactical and Strategic Perspective” being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert’s channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.



Unlocking Tension Between Security and Networking Teams With SASE: A Leadership Perspective on Balancing Performance and Safety

By Stephen Amstutz, Director of Innovation at Xalient

The demand for highly performant networks has risen exponentially as organizations seek to empower employees with fast, anywhere access to key applications. At the same time, the threat environment continues to escalate, and the consequences of breaches and disruption become increasingly severe. Networking teams are striving to deploy increasingly distributed, complex network solutions, and security teams are faced with the challenge of securing them.

Xalient's latest research report 'Why SASE is the Blueprint for Future-proofing Your Network in 2025 and Beyond' reveals that gaps in organizational networks present a significant and persistent threat to security, with 90% of research participants reporting that emerging cybersecurity attack vectors are taking advantage of gaps in their network. With this dual challenge of performance and security to solve, both security and networking teams are turning to Secure Access Service Edge (SASE) in a bid to strengthen the security posture across a highly distributed environment and drive network performance through reduced latency. Correctly implemented, a SASE solution can address several aspects of both the networking and the security requirements with a single solution rather than a bolt-on approach, making it more secure and less complex.

However, choosing and implementing a SASE solution needs careful thought. There are multiple stakeholders involved with different – sometimes competing – objectives. Consequently, there is an important role for leaders in working with teams to discern the right approach to identifying requirements and vendors selection that balances the drivers, risks and barriers to achieve the best outcome for the business. SASE allows security and networking teams to address zero trust principles like least privileged access and micro segmentation by taking an identity-centric approach to connectivity.

Networking and Security Factors to Consider

Xalient's recent research polled 700 organizations that have already implemented a SASE solution. They shared valuable insights into the issues they were seeking to solve and the benefits achieved.

Resolving performance issues and reducing latency for business-critical applications is the primary network-focused driver for exploring a SASE solution, pushing securing remote access for the hybrid workforce into second place. This reflects the fact that commercial pressures often outweigh security factors in decision-making. Implemented correctly, a SASE solution should solve both challenges and our research bore this out, with improved performance of business-critical apps cited as the top benefit following SASE implementation.

Businesses are also reporting concerns about the rising cost of traditional network architecture – this was a commonly cited driver for SASE adoption. We have reached a point where legacy networks are creaking under the strain of rising traffic and a greater number of remote workers. They are simply not resilient enough to support modern business structures and processes. Now that there is greater certainty around the shape and demands on networks following the pandemic upheaval, this is a good time to invest in a future-ready architecture.

From the security team's perspective, key drivers include the secure remote access already mentioned. Fear of breach – including the regulatory, reputational and financial impacts – was another key stimulus and these two are closely linked, given that 44% of respondents said a recent breach had originated with a remote or hybrid worker.

Security teams also have strategic objectives in mind. Secure cloud adoption and migration was the third most-common driver for SASE adoption. This makes sense – SASE is typically delivered as Software-as-a-Service so it can seamlessly provide full zero trust access based on the identity of the device or entity. It can be combined with real-time context and security and compliance policies to solve another key challenge – that of securing the network without having to lock down large portions of it.

SASE implementation had answered many of these drivers for our research cohort, with many reporting that they had achieved strong threat protection without having to implement hardware and software upgrades. Being able to deliver consistent security policies was another notable advantage.

Leaders who are working to devise the right SASE approach can usefully conduct their own research among network and security stakeholders to identify the drivers that are specific to their business and ensure they are effectively addressed by the chosen solution approach. This is important because our study showed that the advantages differ depending on whether a multi-vendor or single-vendor solution is chosen.

Single- or multi-vendor SASE selection?

There are various pros and cons associated with single vendor versus multi-vendor SASE solutions. Our survey showed that those who had implemented a muti-vendor solution were more likely to report improved performance of business-critical apps than those who had adopted a single vendor approach. However, they raised concerns about the complexity of managing multiple vendors and lack of clarity on pricing.

On the other hand, single-vendor environments were associated with a more predictable return on investment, but challenges included controls not being as effective or configurable compared with a multi-vendor solution and vendor lock-in.

These pros and cons must be weighed in light of the network and security teams' priorities and bandwidth. If performance improvements are non-negotiable, it may be prudent to opt for a multi-vendor solution but ensure that there is enough resource – either internal or externally provided – to support and manage it. If ROI is the strongest driver, a single-vendor solution may be the best option, but more work may be needed to configure controls.

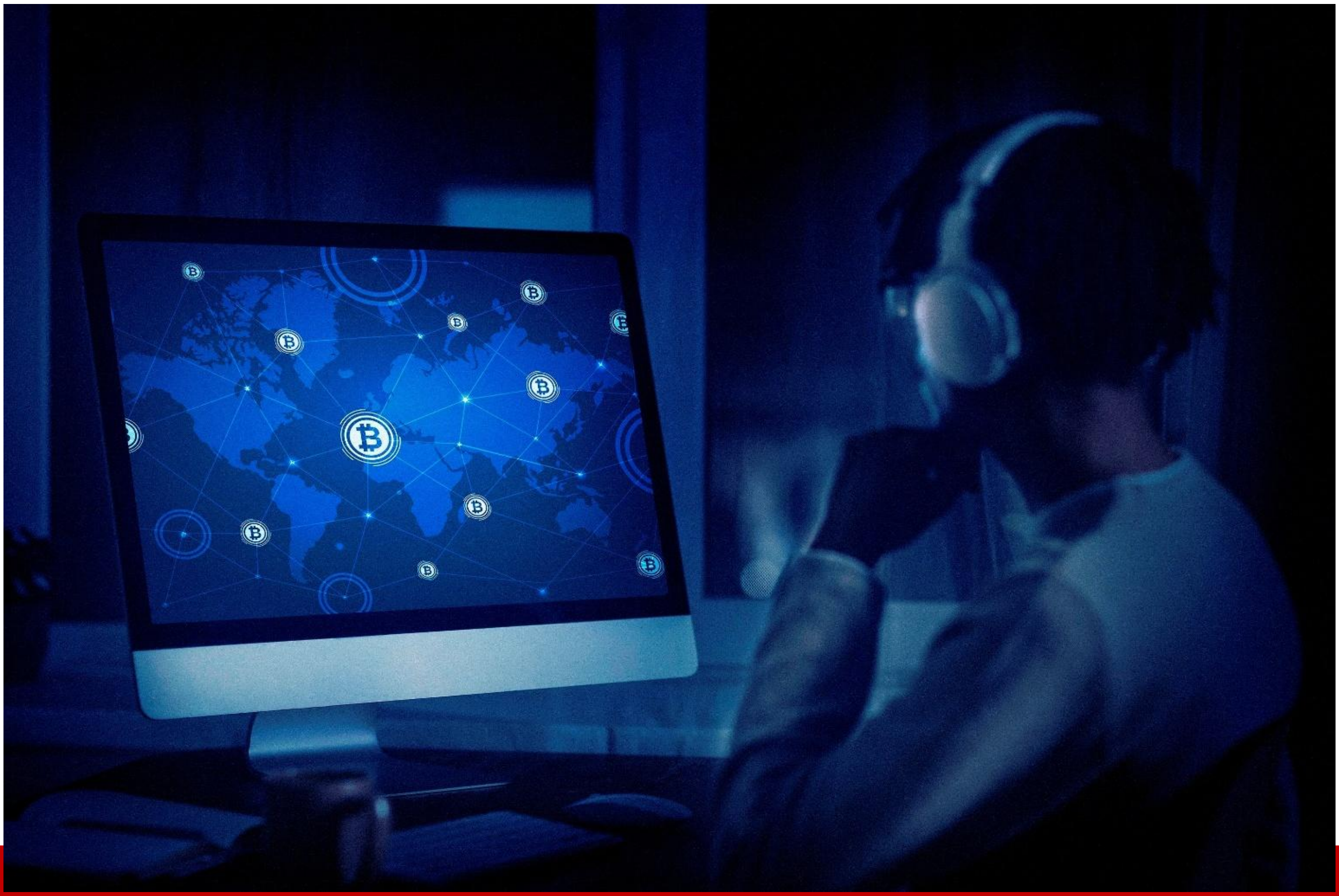
SASE is often deployed in phases, which is a prudent approach, however the selection shouldn't be made based on the first component to be deployed. It's important to consider requirements from both a network AND security perspective to ensure the end goal encapsulates the outcomes you want to achieve across both domains. Another common challenge we see is complexity; organizations have tens of monitoring tools in place with the associated alert fatigue. One objective SASE can address for all stakeholders is reducing complexity and thereby improving visibility.

What's right for one business may be wrong for the next, what leaders must do is ensure they have a complete picture from all stakeholders, and a sound understanding of what SASE offers in its different guises, before making the critical decision. Then the challenge is communicating back to stakeholders how the solution will solve their issues and set them up for a simpler, more secure, and more performant future system. This should unlock the tension and get teams working together to drive the business forward. This is where working with an experienced managed service provider that has undertaken multiple SASE implementations could help the organization determine what SASE solution is right for their requirements and provide leaders with the right balance of performance and security for the business.

About the Author

Stephen Amstutz is a results-driven, hardworking professional, capable of understanding complex matters outside his area of direct expertise. He has over 20 years' experience in design, implementation, and support of various IT infrastructures. Stephen is responsible for all technical pre-sales for Xalient. This involves designing a whole, end-to-end solution to meet the customer's needs, potentially including everything from networks and server infrastructure to applications and business processes.

Stephen can be reached online at xalient@c8consulting.co.uk and at our company website https://xalient.com/



Virtual Client Computing Market: Tapping on the Domain of Innumerable Opportunities

By Aashi Mishra, Content Developer, Research Nester

VCC or virtual client computing is an advanced IT approach with a comprehensive application and desktop virtualization solution. The system is fabricated to aid businesses in reducing IT costs and support a mobile workforce while maintaining data security.

Virtual Client Computing or VCC has gained prominent importance amongst the market players. This blog will explore various factors propelling the market's growth in the coming period.

Why are plenty of companies opting for VCC?

- **Rising demand for remote work solutions in the hybrid environment**

It has been estimated that almost 91% of employees globally prefer to work fully or almost completely remotely. Organizations have turned to numerous solutions to aid power remote work in the past few years. One of the most efficacious has been the adoption of virtual client computing infrastructure that allows organizations to centralize their Information Technology resources. Also, it provides users with remote access to a consolidated pool of computing power. Here are 3 remarkable benefits that organizations can achieve are as follows:

- **State-of-the-art performance**

The VCC model helps organizations run their desktops on data center infrastructure. This infrastructure is more efficient than laptops, where workers typically function. This type of performance is especially helpful for companies running legacy applications. VCC is an excellent fit for the application running in a client-server model.

- **Enhanced security**

Other various tools to operate remote work fabricate an extension of the corporate network to users' personal computers. These increase cybersecurity risks in an environment of distributed machines and create a management burden on IT departments. Also, VCC gives organizations a way to limit users' remote access.

- **Easy elasticity**

While end users have their personal computers, organizations may find it difficult to scale desktop resources up and down. However, including VCC can promptly scale up and down to accommodate business requirements. VCC appears as an efficient solution to increase elasticity.

Rising adoption of virtualization technologies for operational flexibility

The VCC is used by businesses efficiently and securely by lessening operational costs. Some of the technologies in VCC stand to enable organizations to optimize virtual client computing are as follows:

- Cost saving
- Contingency planning
- Improved scalability
- Better security

Some other growth-propelling factors for the market are strict cybersecurity requirements and advancements in cloud computing and mobile technology.

Other than this, the increased requirement for enhanced productivity and information security is one of the prominent factors that is fueling the market growth. VCC helps keep data and applications in a safe and managed closed setup, lowering the chances of data breaches.

Cost efficiency is also a big advantage of utilizing VCC

Virtual Client Computing Software Market Analysis:

The market is anticipated to have garnered USD 21 billion by the end of year 2024 and by 2037 revenue is projected to reach USD 55 billion by the end of 2037. Some of the key market players in the domain are Microsoft Corporation, Fujitsu Limited, VMware Inc, Ericom Software Inc, Dell EMC, Huawei Technologies Co Ltd, Hewlett Packard Enterprise Company, NEC Corporation, Hitachi Ltd, and Others.

The United States is among the substantial markets for virtual client computing all across the world. The growth in the market can be attributed to the rising adoption of cloud computing technologies and the presence of numerous key players in the region.

Similarly, the adoption of virtual client computing is projected to rise remarkably across Small and Medium Enterprises and large revenue-generating businesses across East Asia. The region is expected to remain the highest-growing market during the coming years due to the presence of flourishing economies and the rising adoption of virtual client computing in data centers.

In a nutshell,

The market is projected to garner a significant share during the forecasted period. Various entrepreneurs are willing to take a plunge in the pool of numerous opportunities offered by the burgeoning market. However, it is prudent to understand the market parameters in detail so that market leaders can make judicious decisions for their businesses and excel in the competition. Availing an exhaustive market research report is an efficacious solution as it contains regional analysis, growth driving factors, key market players, etc.

About the Author

Aashi Mishra is currently working as a content developer with the Research Nester. An electronics engineer by profession, she loves to simplify complex market aspects into comprehensive information. She has experience of 3 years in this domain where she has mastered in tech writing, editing, copywriting, etc. https://www.researchnester.com/

AI-powered Vishing

Get ready for the next phase of social engineering attacks

By Thomas LE COZ, CEO, Arsen

First, there was phishing. The goal: To trick targets into revealing information or completing unauthorized actions. Around since the 1990s, this attack vector remains the top internet crime reported to the FBI, partly because of its effectiveness in exploiting human emotions when pretexting.

After all, you can’t simply issue a patch or apply a firewall to human instinct. For example, how a new starter may feel under pressure to skip usual security procedures after being told, ‘You need to download this file for your onboarding.’ Or how a junior payroll administrator is unlikely to challenge someone who says they’re the regional finance director and needs an invoice to be paid immediately.’

There’s huge power in manipulating people’s feelings and responses to trust, fear, and urgency. These forms of social engineering threats are going nowhere. In fact, they’re becoming more advanced, as shown by the rise in voice phishing, otherwise known as vishing.

In the past, vishing may have been identified by its use of automated robotic voices, or that the actual voice on the phone didn't sound like the person they were impersonating. That's all changing because of AI.

How AI is accelerating vishing use cases and capabilities

Vishing has traditionally been labor-intensive. First, selecting the target, and applying various psychological techniques to verbally encourage them to fulfill the attack request. This needs a skilled manipulator of human emotions. Someone capable of improvising during a live call, and knowing when to threaten, coerce, or even impersonate a colleague or third-party contact.

You'd also need supporting tactics and technologies, such as caller ID spoofing to use a phone number the target would recognize. Or crawling the target's social media channels, to look for clues that would help build rapport during a call. Maybe referencing their favorite sports team, or a recent holiday destination.

Of course, vishing also relies on the target believing and trusting a voice they probably have never heard before. At least, until AI technology started being used for vishing. Now attackers have a new threat vector, adding a new dimension to attacks, and asking new questions of enterprise defenses.

Advances in deception methods with AI technology

It's now possible to clone someone's voice with as little as 15 seconds of audio, whether that's taken from online videos or recorded on a live phone call. Enough time for the AI to capture and learn from their vocal nuances, inflections, and tones.

Cyber criminals can then use the cloned audio for text-to-speech vishing attacks during real-time two-way conversations. Our voices are about as unique as fingerprints, plus we've had thousands of years of evolution where we're used to listening out for voices we recognize, without thinking, 'Is that really who I think it is?' So, it's not practical to expect people to suddenly stop trusting voice as an authentication factor.

That's because AI can also be deployed to bring context to conversations. Attackers can scrape the web in real-time, often using a mix of OSINT techniques and capabilities, to feed the results into an LLM. This allows the AI to communicate with relevancy and recency, such as mentioning recent news to add an authentic-sounding layer to requests.

You can see the impact of this in a study of an AI-automated vishing attack simulation, which extracted sensitive data from 77% of participants. This was in part due to the chosen LLM offering 'advanced capabilities in context understanding, response generation speed, and fluency in conversation, which is crucial in giving the illusion of a real-time conversation in a phone call.'

Scaling attacks with AI-powered vishing

This AI-driven approach is a long way from traditional vishing call centers, with human agents making calls from physical workstations. Cyber criminals can now launch hyper personalized 1:1 attack at scale, personalizing messages to multiple targets at once if needed. And then simply update language based on the AI's learned inputs, rather than needing to be reprogrammed if an attack is unsuccessful.

Many of these AI voice cloning tools are open source, opening up free or low-cost access to a wider range of malicious actors across the world. As development accelerates, the nature of vishing is evolving too, with AI allowing attackers to deploy with what the FBI describes as 'unprecedented realism'. In Q4 of 2023, vishing attacks rose by a reported 260% year-on-year. Meanwhile, in early 2024 a deepfake video led to a finance worker paying out $25 million to someone they thought was their CFO.

Attackers may often gain a first-mover advantage with emerging technologies, leaving defense teams racing to catch up and build systems to counter. However, they still rely on human vulnerabilities to breach successfully. So that's where businesses should start, by taking a people-centric approach to defending against AI-driven vishing.

How to tackle AI vishing's first-mover advantage

It starts with training the workforce to be aware of vishing and AI developments, helping them recognize when their emotions are potentially being triggered. Especially if that includes a request to share data, passwords, or other sensitive information.

Along with the theory, it also means giving them practice at being the subject of a vishing attack. After all, people may forget what a lecturer or online course says about AI vishing. They're more likely to remember the experience of AI vishing and thinking, 'What if that had been a real attack.'

This allows employees to reflect and learn new behaviors and thought processes. They don't have to repress emotions and thoughts that attackers want to exploit. They just learn to know when to take a step back during a call, and think: Am I being pressured to complete this action for this person? Am I being asked to believe something they say without any proof? Shall I end the call and call the person back on their main office number?

Simulation helps lighten the load on cybersecurity teams too. They can't always stay ahead of the latest vishing strategies, and developing protection systems such as voice biometrics takes time. Whereas educating employees with simulation and real-world training can be an effective and immediate defense alternative.

About the Author

Thomas LE COZ is the CEO of Arsen. He develops solutions to reduce the impact of social engineering in cyberattacks. By simulating attacks ranging from regular phishing to voice-clone vishing, Arsen provides a complete platform to evaluate, train and automate behavior improvements of the workforce with a "learn-by-doing" approach. Thomas can be reached online on LinkedIn and at our company website https://arsen.co

The Future of Third-Party Risk Management: Seven Key Predictions for 2025

By Alastair Parr, Executive Director, GRC Solutions at Mitratech

As organizations gear up for 2025, third-party risk management (TPRM) remains a top priority. The need to manage risks associated with vendors and partners has grown more urgent, driven by new regulations, geopolitical tensions, and supply chain vulnerabilities. In today's interconnected business environment, a partner's weak security posture can quickly become your organization's liability. Here are seven predictions for how TPRM will evolve to address these changing risks in 2025.

1. AI Will Drive Predictive Insights and Streamline Processes

Artificial intelligence (AI) is becoming a cornerstone of TPRM, enabling organizations to automate risk assessments, identify patterns in large datasets, and spot potential issues faster. Leveraging Large Language Models (LLMs) will help identify inconsistencies in documentation and responses. However, successful AI implementation will require robust data security, governance, and transparency frameworks. With only 5% of organizations actively using AI for TPRM in 2024, this number is expected to rise as businesses close governance gaps and embrace automation.

2. Regulations Will Tighten and Push for Elevated Due Diligence

Governments and regulatory bodies worldwide are strengthening third-party risk management requirements, particularly in data privacy, ESG (environmental, social, and governance), and operational resilience. Companies must assess third-party suppliers and partners more rigorously, emphasizing resilience and environmental impact to align with evolving regulations.

In the U.S., the EU Digital Operational Resilience Act (DORA) is emerging as a potential model for operational resilience standards, particularly within the financial sector. This aligns with efforts from regulatory bodies like the U.S. Office of the Comptroller of the Currency (OCC), signaling a broader push for stringent due diligence. Meanwhile, ESG mandates such as the EU's CSRD and CSDDD will require businesses to evaluate supplier practices, including carbon emissions, labor conditions, and ethical sourcing. These changes highlight the growing need for robust compliance strategies to meet regional and global regulatory demands.

3. Geopolitical Instability Will Demand Closer Monitoring

Political and regional instability—such as the ongoing crises in Ukraine and the Red Sea—is prompting organizations to scrutinize their extended ecosystems closely. Companies will focus on analyzing ultimate business owners (UBOs) and regional concentration risks to anticipate disruptions and avoid sanctions. Expanding vendor firmographic data will mitigate downtime and ensure operational continuity.

4. TPRM Will Be Embedded into Enterprise Culture

Organizations will adopt a more collaborative approach as TPRM shifts from an IT-led initiative to an enterprise-wide responsibility. Procurement teams, risk managers, and other stakeholders will play more significant roles in sourcing, due diligence, and vendor offboarding. This cultural shift will ensure that TPRM is fully integrated into broader business processes, fostering better coordination and risk mitigation.

5. Centralized Risk Reporting Will Become Essential

Boards and senior leadership increasingly demand consolidated views of internal and external risks. Organizations will integrate TPRM into their governance, risk management, and compliance (GRC) frameworks to meet this need. Unified key risk indicators will provide business-impact-focused insights that are accessible to both technical and non-technical stakeholders, enabling more informed decision-making.

6. Aggregated Risk Monitoring Will Strengthen Resilience

The rise in third-party cybersecurity incidents underscores the importance of assessing interconnected risks across ecosystems. Continuous monitoring across multiple domains—cyber, operational, reputational, ESG, and financial—will become standard practice. Real-time data insights will enable organizations to respond more effectively to emerging threats, bolstering supply chain resilience.

7. Third-Party Data Breaches Will Reach a Critical Point

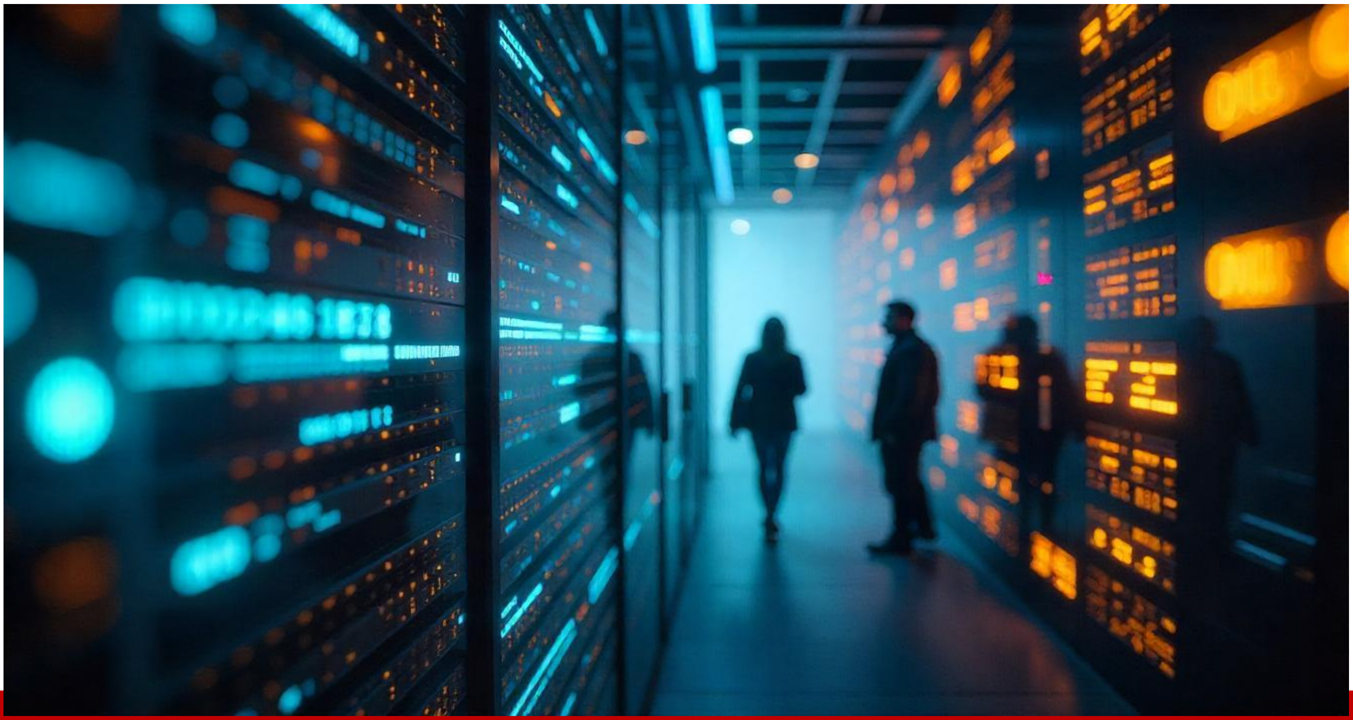
Third-party cybersecurity incidents have surged in recent years, affecting over 60% of companies in 2024. These breaches are also growing in severity, with millions of people impacted. In 2025, cybercriminals are expected to target third parties supporting high-profile industries such as healthcare, finance, and education. Proactive risk management will be critical to mitigating these threats.

Preparing for the Future

The evolution of third-party risk management is accelerating. From adopting AI to stricter regulations and focusing on resilience, organizations must adapt quickly to the changing landscape. By embracing innovation and prioritizing governance, companies can turn TPRM challenges into sustainable growth and success opportunities in 2025.

About the Author

Alastair Parr is the Executive Director of GRC Solutions at Mitratech. He offers over 15 years of experience in product management, consultancy, and operations. He ensures that customer and market demands are considered and applied innovatively within the Prevalent solution portfolio. Parr comes from a governance, risk, and compliance background, developing and driving solutions to the ever-complex risk management space. Follow him on LinkedIn.



Déjà Vu: What Cloud Adoption Can Teach Us About AI in Cybersecurity

The insights gained from cloud adoption can effectively guide cybersecurity teams in their journey toward embracing and implementing AI technologies.

By Ashish Pujari, Security Specialist, Google

The launch of ChatGPT undeniably marked a turning point in the technological landscape, ushering in the era of readily accessible and powerful Large Language Models (LLMs). This new age has ignited widespread enthusiasm among individuals and organizations alike, who are eager to harness generative AI to revolutionize their daily routines and operations. This is particularly evident in the cybersecurity domain, where the adoption of AI is seen as crucial for gaining an advantage in the ongoing battle against cyber adversaries. However, this technological advancement has also spurred a parallel evolution in cyber threats, with malicious actors becoming increasingly sophisticated in their use of AI to automate attacks, craft highly convincing phishing schemes (including the use of deepfakes), and develop new strains of malware.

Many cybersecurity teams are wrestling with the implications of this new AI-powered landscape, striving to find the optimal path forward for their organizations. Caught between the imperative to innovate and the crucial responsibility of maintaining robust security, these teams often find themselves navigating a delicate balance. On one side, they face pressure from business stakeholders eager to embrace and experiment with cutting-edge AI technologies. On the other, they bear the weighty responsibility of ensuring these powerful tools are adopted in a manner that prioritizes security, mitigates risks, and safeguards the organization's valuable assets.

Navigating the AI revolution may seem daunting, but we've been here before. The shift to cloud computing presented cybersecurity teams with a similar challenge: embracing a transformative technology while managing its inherent risks. Looking back, we can glean valuable lessons from that experience to guide our approach to AI adoption. This article focuses on the often-overlooked "people" aspect of this challenge, drawing on proven strategies that empowered cybersecurity teams to successfully navigate the cloud transition. (We'll leave the deep dive into specific AI technologies for now, as there are already abundant resources available on that front.)

Executive Support

Having witnessed multiple cloud migrations one thing is clear: Team members, consciously or not, mirror their leaders. When executives champion technology – not just with words, but with a clear vision and tangible resources (budget for training, tools, infrastructure modernization, etc) – success rates skyrocket. This was true for cloud adoption, and it will be equally important for secure AI adoption.

Cybersecurity Leaders must actively drive secure AI adoption, just as they did with cloud technologies by fostering collaboration and breaking down silos, particularly between cybersecurity teams and other business units. In my experience, strong leadership is the single greatest predictor of successful technology adoption, whether it's migrating to the cloud or integrating AI securely.

Upskill Upskill Upskill

Yes, I know I wrote that three times because that's how important this is. In the rapidly evolving landscape of artificial intelligence, the axiom "you cannot defend what you do not understand" has never been more pertinent. Just as cybersecurity teams who successfully navigated cloud adoption ensured their personnel were thoroughly trained in cloud technologies, AI demands an even more rigorous approach to upskilling. The stakes are exponentially higher with AI, given its potential to revolutionize—or compromise—entire systems and decision-making processes.

Cybersecurity professionals must not only comprehend AI's underlying mechanisms but also stay ahead of its potential vulnerabilities and ethical implications. This upskilling initiative should not be viewed as a one-time effort; rather, it must be an ongoing, dynamic process. The AI field is advancing at an unprecedented pace, with new developments emerging almost daily. Continuous learning and adaptation are not just beneficial—they are absolutely essential for cybersecurity teams to effectively protect against AI-related threats, mitigate risks, and harness AI's potential for enhanced security measures. Organizations that prioritize this continuous AI education for their cybersecurity teams will be far better positioned to safeguard their assets, maintain trust, and leverage AI securely in this new era of digital transformation.

Fostering a culture of experimentation

Many cybersecurity teams have designed their security architecture as a castle with multiple levels of security. While this is an effective strategy it does not lend well to experimentation. The common way any new technology is adopted is by stopping it at the castle gate.This has many unfortunate side effects:

● Business stakeholders go outside the castle (often with corporate crown jewels) to experiment with any new technology unbeknownst to the security team.

● Security teams garner a bad reputation because they are always saying no to new technology adoption

● In the age of rapidly changing technology this approach can hamper business agility ● Team members can avoid learning about new technologies because they know they can get away with it.

Instead of acting like gatekeepers, cybersecurity teams should encourage business stakeholders to experiment with small scale pilot projects and get involved early in the process. Cybersecurity teams which operated this way saw better results with technology adoption when adopting cloud technologies.

This approach will increase business agility and allow security team members to gain critical experience with AI tools and processes.

Participating in the AI Center of Excellence

Cybersecurity teams shouldn't just be involved in an AI Center of Excellence (CoE), they should be at the heart of it. Especially when it comes to AI adoption, their early and continuous involvement is critical for several reasons:

● Baking in security from the start: Cybersecurity professionals bring a crucial security-first mindset to AI development. By embedding them in the CoE, security becomes an integral part of the AI strategy, not an afterthought. This proactive approach is far more effective (and cost-efficient) than trying to bolt on security measures later.

● Scaling limited resources: Cybersecurity teams are often stretched thin. Participating in a CoE allows them to efficiently influence AI standards and best practices across the organization, maximizing their impact.

● Fostering crucial collaboration: CoEs are hubs for cross-functional collaboration. This allows cybersecurity teams to understand the diverse needs and perspectives of

different business units, leading to more informed and effective security decisions around AI.

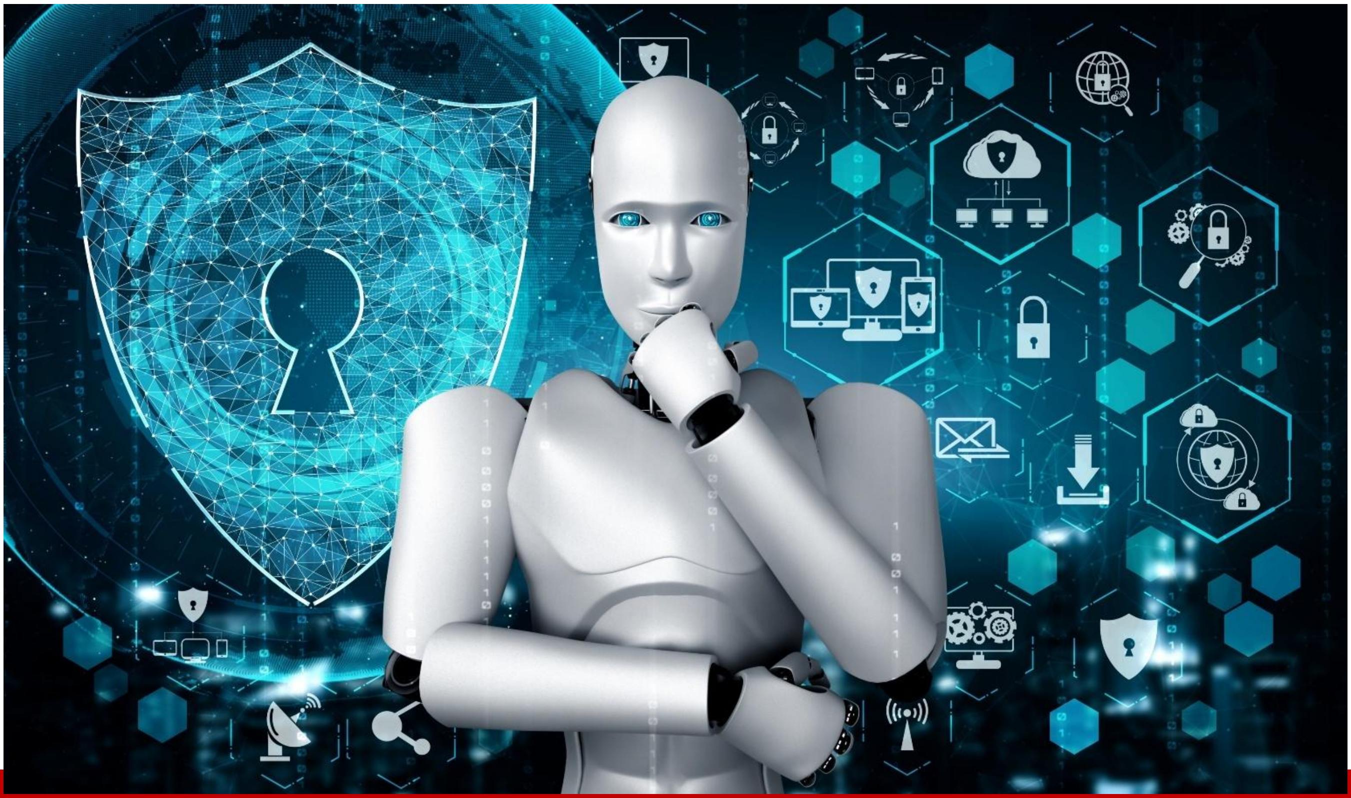
Ultimately, including cybersecurity in the CoE ensures that AI adoption is not just rapid, but secure and sustainable. This protects the organization from potential risks and fosters trust in AI solutions.

Conclusion

Having navigated numerous organizations through the complexities of cloud adoption, I can confidently say that AI adoption shares a striking resemblance. Just as we learned valuable lessons transitioning to the cloud, those same principles can guide us through the successful adoption of AI in cybersecurity. By embracing the above principles, security teams can use the transformative power of AI to strengthen their defenses, optimize operations, and proactively address the ever-evolving threat landscape.

About the Author

Ashish is a Technical Partner Manager at Google. He has 10+ years of professional work experience in Information security with expertise in cloud security, security architecture reviews and managing security operations in corporate and client facing environments. Ashish can be reached on LinkedIn https://www.linkedin.com/in/ashishpujari/



The Significance of Cybersecurity within AI Governance

Tackling Bias and Safeguarding Data Integrity

By Pooyan Hamidi, Cybersecurity Manager, Deloitte & Touche LLP

In everyday life, AI integration rapidly changes traditional consumers' shopping experiences, changes work scenarios at work spots, and health provision. With the impacts that AI strikes to the world, many changes develop due to its use; however, the involvement in decision-making attracts critical challenges on its ethical usage and data security. This article will examine the relationship between cybersecurity and the wider framework of governance surrounding AI, the importance of that link, and strategies through which this very important area-ethical, secure, and fair operation of AI systems-can be maintained.

Artificial Intelligence in Decision-Making: The Importance of Governance

Artificial intelligence systems are increasingly used in key sectors, including recruitment, financing, law enforcement, and healthcare. These systems make decisions based on data; when the underlying data is biased or tampered with, the output might perpetuate unfairness or cause harm. Example:

- **Recruitment algorithms** have been found to disadvantage women or minority groups unfairly because such algorithms are built from historical data that contains the previous biases themselves.
- **Facial recognition technology** has been historically prone to misidentifying individuals from marginalized racial backgrounds, resulting in wrongful apprehensions in certain cases.

This illustrates that in the absence of adequate supervision, artificial intelligence may exacerbate pre-existing disparities instead of alleviating them. The domains of cybersecurity and governance are essential in addressing these challenges by protecting the integrity of AI systems and ensuring that ethical standards inform their application.

The Convergence of Cybersecurity and AI Governance

Cybersecurity is often an afterthought when discussing AI governance, but the two are very deeply intertwined. AI systems are only as good as the data they process, and ensuring that data is accurate and secure is a cybersecurity challenge. Overlaps include the following:

1. **Data Integrity:** AI systems depend on a great deal of data to work. When that data is tampered with—either intentionally or accidentally—the decisions that result are wrong. Cyberattacks against datasets can skew the outcome, such as modifying medical AI models to misdiagnose patients.
2. **Model Security:** AI models are vulnerable to attack. The harmful data provided by an attacker can manipulate the AI framework to provide false output. For instance, in autonomous cars, a hostile interference could make the cars think a stop sign is a speed limit sign with serious consequences.
3. **Bias Mitigation:** Although bias is often considered an ethical issue, cybersecurity plays a significant role in identifying and preventing biased data from becoming integrated into AI models. Protecting data pipelines ensures that only vetted and quality data is used

Fairness in AI decisions is something that needs to be designed in, and that requires collaboration by technologists, ethicists, policymakers, and cybersecurity experts. Here's how to get it right:

- Algorithmic Transparency: AI systems must be designed so that independent review is possible. When AI decision logic is clear, biases are more easily detected and avoided. Open-source models are one good way to do this: allowing a large community to analyze and improve the technology.
- Diverse Teams: Bias often enters AI because the teams building the systems lack diversity. A diverse team brings a range of perspectives, reducing the likelihood that biases go unnoticed during development.
- Regular Audits: AI models should undergo frequent evaluations to check for bias and accuracy. Audits can catch problems before they affect real-world decisions.

The financial industry has embraced ethical AI practices to reduce bias in lending. For instance, many banks now use algorithms that avoid traditional credit scoring measures, instead relying on a broader set of financial behaviors to drive fairer outcomes.

Securing AI Systems: A Critical Cybersecurity Imperative

Ethics alone will not safeguard AI systems. Cybersecurity measures are also a must to protect these systems from manipulation. With federal initiatives such as the AI Bill of Rights, there is an increasing drive for AI systems to be not only fair but also secure.

Strategies for Securing AI Systems

- **Encrypting data that is used in AI systems** protects sensitive information such as medical records or financial data from unauthorized access.
- **Most endpoint protection** AI models rely on several systems and devices to function. Protection of these endpoints ensures that no weaknesses can be utilized by any attackers.
- **Monitoring of AI systems** should be done continuously to detect and prevent threats as soon as they occur. In this regard, intrusion detection systems can be used to identify unusual activities that may imply an ongoing attack.
- **The AI Bill of Rights,** which has been advanced by the White House, also speaks to the need for safe and ethical AI. This outlines guidelines for transparency, user protection, and the responsible use of AI systems. Organizations that comply with the recommendations ensure that their AI models are designed according to ethics and security.

Practical Guidance for Ethical and Secure AI Implementation

Practical Steps: For companies and developers who want to deploy the AI system responsibly, here it is:

1. **Start with a Risk Assessment:** Identify potential weak spots in your data and model, so you can fix those before hackers do.
2. **Invest in Cybersecurity Training:** Make sure your team knows how to lock down an AI system against everyday threats like data poisoning or adversarial attacks.
3. **Engagement Across Disciplines:** The integration of experts in cybersecurity, ethics, and artificial intelligence development engenders a holistic approach to governance.
4. **Engagement with Policymakers:** Knowledge of federal efforts like the AI Bill of Rights ensures legality and ethical concerns.

Practical Application: The healthcare industry has shown some leadership in this area. Artificial intelligence-based diagnostic tools, for instance, are increasingly being designed with ethical safeguards and cybersecurity measures. In one case, a hospital implemented AI systems that work only on encrypted patient data, thus ensuring both accuracy and confidentiality.

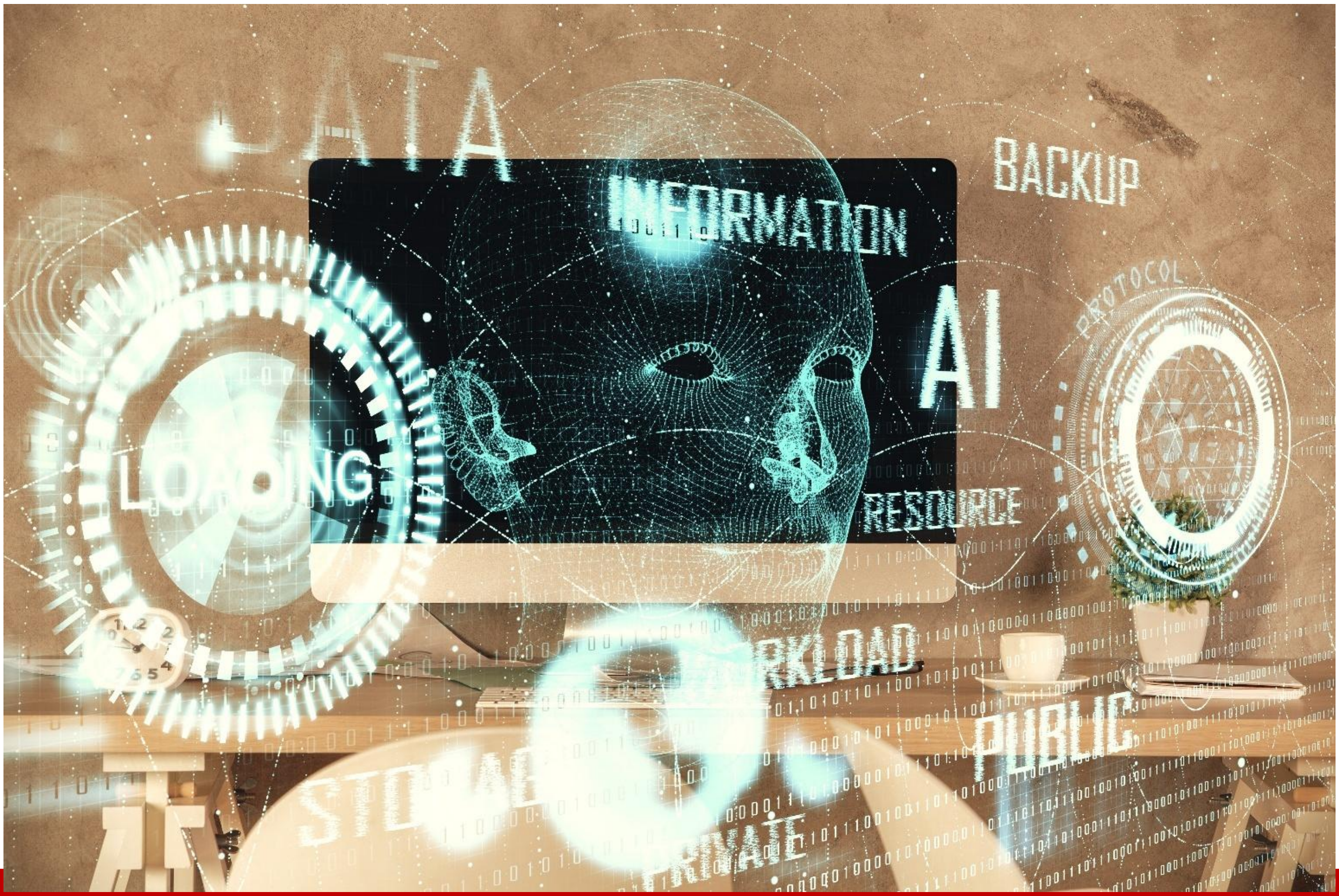
Future Directions

With AI only going to increase in importance, strong governance and cybersecurity will be required. It is not a purely technical challenge, but also a societal one: addressing bias and securing data integrity. Embed ethical principles within AI design and ensure strong cybersecurity to make AI beneficial for all, not just the few.

In all, AI governance and cybersecurity domains are pretty much interlinked. Together, they can work towards creating systems that are not only robust but fair, secure, and reliable. While the task may be intricate, the benefits justify the effort: a prospect in which AI acts as a positive influence.

About the Author

Pooyan Hamidi is a cybersecurity and AI governance enthusiast with a passion for exploring the intersection of technology, ethics, and security. With years of experience in the tech industry, Pooyan focuses on creating awareness about responsible AI deployment and its impact on society. You can reach him at pooyan.hamidi@gmail.com for inquiries, collaborations, or discussions on ethical AI and cybersecurity.



The Evolution of SOC: Harnessing Data, AI and Automation

By Abiodun Adegbola, Security Engineer, Systal Technology Solutions

The modern Security Operations Center (SOC) faces an ever-growing tide of data, fueled by the explosion of connected devices, cloud migration, and increasingly sophisticated cyberattacks while the growing impact of automation and artificial intelligence remains vital to achieving a robust and efficient SOC. SOC teams should aim to shift from conventional approaches filled with constraints and limitations; and actively look for opportunities to optimize processes, capabilities and outcomes. This article explores how these technologies can transform the SOC, enabling faster threat detection, incident response, and ultimately, a more proactive security operation.

Data: The Fuel of Modern Security

Data is key to providing visibility into any environment and vital for other SOC functions such as threat intelligence, analytics and incident response. Data originates from various sources, such as firewalls, intrusion detection systems (IDS), endpoint security tools, collaboration tools, directory services and cloud workloads. However, the sheer volume and complexity of this data can overwhelm some (traditional) systems while collecting everything is also considered a waste of time, money and resources. It is worth saying that logging too little restraints audit capacity and effective security monitoring. You want to ensure that you have all the data you need to act against risks and threats in your environment, while also ensuring that you're not paying to ingest more data than you need. To balance the need for proper level of visibility into the environment and ingesting data within the scope of what is required, it is paramount to prioritize critical assets, conduct log curation and configure the SIEMs to collect the most vital things.

AI: Augmenting Human Expertise

Artificial intelligence (AI) is emerging as a powerful tool to address the data deluge. AI algorithms can sift through massive datasets in real time, identifying patterns and anomalies that might escape human observation while generative AI models can be leveraged for advanced analysis of security incidents and malicious software. SOC teams face a mounting challenge with Cloudflare recent application security report claiming that around 7% of the global internet traffic is malicious and CVEs exploited as fast as 22 minutes after a proof-of-concept is made available. An AI-powered SOC could be transformative in this regard by supercharging threat detection and incident response. This allows SOC analysts to focus on other key tasks, which require actual human efforts, therefore, improving efficiency and productivity.

Automation: Streamlining Security Operations

Automation plays a vital role in enhancing SOC efficiency and can significantly transform many responsibilities and functions. Some repetitive tasks in incident response, threat intelligence gathering, and vulnerability scanning can be automated, freeing up analysts to focus on more complex and strategic tasks.

Automated workflows could be created on most modern security tools, such as SIEMs, EDRs, to perform various actions such as responding to threats, isolating devices, resolving known benign alerts and disabling user accounts. Automation can also be utilized in high-level situations such as the integration of threat intelligence feeds into SIEM solutions and monitoring of the dark web for organisation's sensitive data. SIEM tools, which is at the heart of security operations, have continued to be transformed for increased capabilities and this includes the infusion of SOAR features into modern SIEM tools.

Conclusion

Data, AI, and automation are not just trends; they are foundational pillars for a future-proof SOC. By harnessing these technologies, organizations can enhance threat detection, incident response, and achieve a more resilient/proactive security stance. While human inputs and operational procedures remain crucial, the impact of automation and artificial intelligence to process large data cannot be overemphasized. This helps to streamline security operations and improve the speed of threat detection and response.

About the Author

Abiodun Adegbola is a Security Engineer at Systal Technology Solutions, a global specialist in managed network, cloud and security services. He brings over seven years of various experience into the global security operations team within Systal. He is certified across various technologies and holds a BTech in Computer Engineering from LAUTECH, Nigeria and MSc in Advanced Security & Digital Forensics from Edinburgh Napier University, UK. Abiodun can be reached online at https://www.linkedin.com/in/abiodunadegbola/ and at company website https://systaltech.com/

Have The Last Word Against Ransomware with Immutable Backup

“It’s never going to happen to me.” Famous last words.

By Judy Kaldenberg, SVP Sales and Marketing at Nexsan

With incidences of ransomware on the rise, nobody should even be thinking that an attack is something that couldn’t happen to them, let alone speak those words into existence. And for organizations that believe a breach couldn’t happen to them because they store their data in the cloud are burying their heads in the sand.

All companies are vulnerable to ransomware. According to analyst estimates, cybercriminals were able to extort more than $1 billion in cryptocurrency payments from victims in 2023. What may have been a simple operational interruption 5 years ago has ballooned into millions of dollars per incident, loss of business reputation and a mystery as to how long it will take to return to viability.

Standard approaches to data security are no longer the answer

Even more disturbing is that ransomware attacks today have become more sophisticated than the “smash and grab” variety of the past. What was once regarded as a way to win a quick score has become increasingly sophisticated, with cybercriminals content to play a waiting game to find out what data is important, which files are being accessed the most and gaining access to passwords.

Typically, organizations would utilize a system of various storage, snapshots, replication, and backup to ensure business continuity. But because this has become such a standard approach, cybercriminals have begun targeting these systems to ensure greater success at securing a payday.

Ninety-three percent of ransomware attacks today target backups. These backups are being turned off, erased and encrypted. Seventy-five percent are successful in preventing recovery and forcing payment. In addition to impacting operations, successful attacks lead to additional penalties for companies in industries that must protect personal information due to industry compliance and legal requirements.

Having your head(ache) in the cloud

In an ever-increasing automated world, the ever-increasing shift to the cloud makes sense. Public clouds offer a plethora of benefits for organizations. Costs are shifted from upfront hardware purchases that will hopefully satisfy future capacity demands to only paying what is used as it is used. Scalability is easy. IT personnel can be utilized on tasks that directly support the business with managed cloud providers doing all the heavy lifting. One thing that it is not necessarily better at – despite the proclamations – is improved security.

Data is only as secure as employees at a company or at the cloud provider make it. The challenge of the cloud for financial organizations under SEC regulations or medical providers that must contend with HIPAA requirements is that data saved to the cloud is out of their control. There are plenty of instances where cybercriminals gain access to data stores because of human error. To what degree of accountability do cloud providers truly offer their customers? What happens when a cybercriminal gains passwords to a company's Microsoft Azure store or their AWS account? And to what degree are cloud providers made accountable for breaches that result in material loss?

Backups should be protected on an immutable platform

Vulnerabilities are almost certain to occur in any software, hardware or firmware release – including cloud providers' infrastructures as well. Though not a malicious attack, the recent CrowdStrike outage shows how widespread a disastrous event can be when it occurs as part of a cloud-native platform despite assurances that cybersecurity procedures are in place.

Well, if there are vulnerabilities everywhere, is everyone simply out of luck? Not so fast. Safeguarding a company's most valuable asset – their data – remains paramount despite the obstacles. Especially as data volumes continue to expand at an unprecedented rate. The challenge therefore is to manage growth while minimizing technological and/or human error to ensure data protection.

The primary goal of backup processes is to guarantee the ability to recover from any data loss or system failure within a predetermined timeframe. This necessitates a robust backup strategy involving automated processes across various applications, platforms and virtual environments. In the face of increasing ransomware threats, immutable storage has become a vital feature.

Rather than placing all of one’s proverbial eggs into a single basket, organizations can strengthen their data storage protection through a hybrid cloud approach that leverages the benefits of the full cloud with the control and security of on-premises solutions. There are several options for ransomware protection including immutable snapshots, S3 object-locking and platforms that provide unbreakable backup. Such solutions offer immutable storage that keeps backup data safe from ransomware attacks, accidental deletions or silent data corruption, while ensuring that backup data remains unaltered and recoverable to provide businesses a reliable defense against evolving cybersecurity threats.

Conclusion

There are many benefits to moving to the cloud – from saving money, to easy scalability and greater reliability – for both IT and end users than on-premises infrastructure. However, security is not one of those benefits. Ransomware has evolved to the point where it is no longer a “will I get hit?” scenario but rather a “when I get hit” one. And, unfortunately, companies rarely see it coming.

For businesses looking for better security of their data, having an immutable backup solution as either a standalone or as part of a hybrid cloud is a more attractive option. This is especially true for organizations with extremely sensitive information, such as healthcare or financial institutions. It can also be ideal for organizations that must comply with regulations that aren’t met by public cloud providers.

Want to have the last word in guaranteeing the safety, security and immediate availability of invaluable data? Ignore the public cloud and instead implement an immutable solution that provides the data integrity, ransomware defense, compliance and legal requirements, and historical data preservation that is needed to tell cybercriminals that they are wasting their time.

“That’s all, folks!”

About the Author

Judy Kaldenberg has been Championing Channel-Driven Data Storage and Ransomware Defense for many years. Her expertise encompasses all aspects of product and channel marketing with extensive experience in charting out sales strategies and contributing towards enhancing business volumes and growth. Prior to working for Nexsan, she held management positions at Kodak Alaris, Avtex Solutions LLC, The MACRO Group Inc., ACS Incorporation, Gauss Interprise, Optika, and Eastman Kodak Company.

Judy can be reached online at info@nexsan.com and at our company website https://www.nexsan.com/

Multi-channel Secure Communication

By Murat Guvenc, Managing Director, BeamSec

1.1 Emerging Cybersecurity Technologies

As we move into 2025, AI and machine learning are expected to play an even larger role in cybersecurity. These technologies will be used to enhance threat detection systems, automate incident response, and provide predictive analytics to preempt attacks. However, the increasing reliance on AI comes with its own risks. By 2025, it is predicted that 80% of organizations will fail to secure their AI-driven mechanisms, leading to a dangerous cycle where AI systems become both a defense and a vulnerability (CyberArk)(INCYBER NEWS). Cybercriminals will continue to leverage AI, not only to launch more sophisticated attacks but also to evade detection through AI-based malware and automated tools (Morefield)(INCYBER NEWS).

Generative AI, while a powerful tool for cybersecurity teams, also introduces new risks as cybercriminals adopt it to automate the discovery of vulnerabilities and craft sophisticated attacks (Gartner)(Morefield).

Organizations will need to adopt a more adversarial mindset in training their AI models, ensuring they test for both offensive and defensive scenarios. Embedding AI within secure environments and continuously stress-testing these systems will be essential to mitigate the rising cyber risks (CyberArk) (Gartner).

2.2 Key Threat Predictions

2.2.1 AI-Driven Attacks

By 2025, AI will be extensively used by cybercriminals to carry out advanced and highly targeted attacks. These AI-driven threats will include data poisoning, AI-enhanced phishing schemes, and automated malware production (Morefield)(Gartner). Hackers will increasingly rely on AI to scale their operations, making their attacks more personalized and harder to detect (CyberArk)(INCYBER NEWS). For example, AI will be employed to steal machine learning models, conduct automated vulnerability scans, and even develop deepfake technology to manipulate individuals or organizations (INCYBER NEWS)(Morefield). Defending against AI-powered attacks will require organizations to integrate AI into their cybersecurity strategies, continuously training their systems to counter evolving threats (INCYBER NEWS)(Gartner).

2.2.2 Ransomware Evolution

Ransomware attacks are predicted to become even more widespread in 2025, with attackers refining their techniques and focusing more on double extortion tactics. In double extortion, cybercriminals not only encrypt data but also threaten to release sensitive information unless a ransom is paid (Morefield) (CyberArk). The rise of Ransomware-as-a-Service (RaaS) platforms allows less experienced criminals to carry out these attacks, further exacerbating the problem (Morefield)(CyberArk)(INCYBER NEWS). Critical infrastructure sectors, including healthcare and finance, are expected to remain prime targets due to their high reliance on data and the potential for significant disruption (Morefield)(Gartner).

2.2.3 Enhanced Privacy and Security Measures

As regulations around data privacy tighten globally, organizations will need to adopt more robust privacy-enhancing technologies. Encryption will become even more critical, with end-to-end encryption and zero trust architectures expected to become standard practices in protecting sensitive data (Gartner) (INCYBER NEWS). These enhanced measures are crucial as cybercriminals continue to focus on exploiting vulnerabilities related to data privacy and security (INCYBER NEWS)(CyberArk).

2.3 Shifting Cybersecurity Strategies

2.3.1 Continuous Threat Exposure Management (CTEM)

With the growing adoption of cloud services, remote work, and SaaS applications, the attack surface for organizations is expanding rapidly. By 2025, businesses will increasingly rely on Continuous Threat Exposure Management (CTEM) to monitor their digital assets in real-time, identify vulnerabilities, and mitigate potential risks before they can be exploited (CyberArk)(Gartner). CTEM will help organizations adapt to the evolving threat landscape by providing continuous visibility into their security posture, enabling proactive responses to cyber threats(INCYBER NEWS)(Gartner).

2.3.2 Social Engineering and Identity-Based Attacks

Social engineering attacks, particularly those focused on identity theft, will remain one of the most prevalent threats in 2025. It is predicted that 80% of all breaches will involve compromised identities (INCYBER NEWS)(CyberArk). Attackers will continue to exploit human vulnerabilities, making social engineering a favored method for gaining unauthorized access to systems (Morefield)(Gartner). In response, organizations will need to prioritize identity protection strategies, including the use of passwordless authentication systems and robust multi-factor authentication (MFA) solutions (INCYBER NEWS)(Morefield). Continuous employee training will also be essential, as cybercriminals refine their techniques to deceive employees into divulging sensitive information (CyberArk)(INCYBER NEWS).

2.3.3 Cybersecurity Reskilling and Talent Shortages

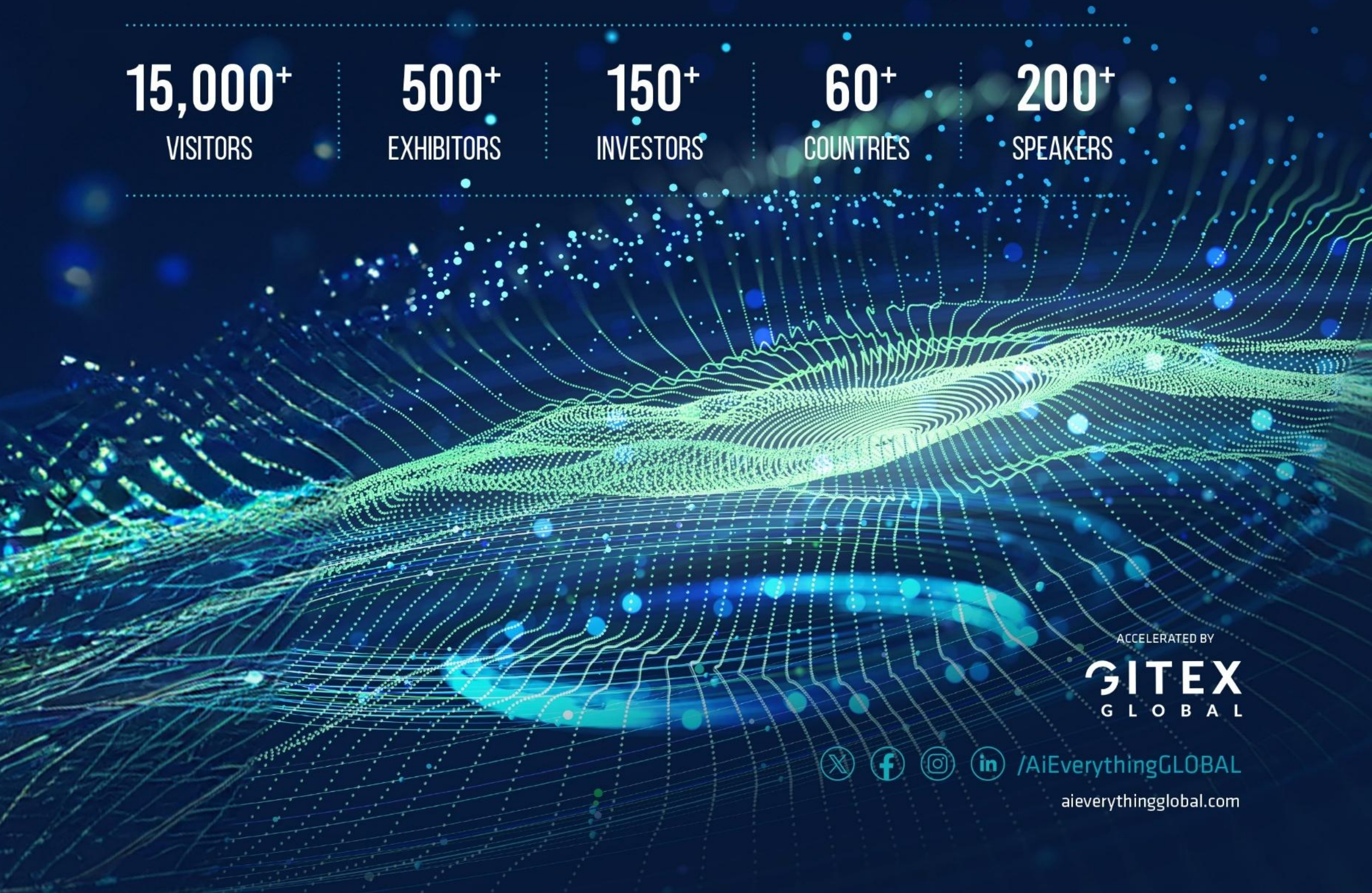
The global shortage of skilled cybersecurity professionals is expected to worsen, with the cyber skills gap projected to grow by 26.2%(Gartner)(INCYBER NEWS). Organizations will need to prioritize reskilling their workforce, focusing on expertise in areas like AI, cloud security, and privacy management (Gartner)(INCYBER NEWS). Cybersecurity training programs will become increasingly important to keep pace with emerging threats (INCYBER NEWS)(Gartner).

About the Author

Murat Guvenc is the Managing Director of BeamSec. Murat is a visionary and results-oriented IT executive with deep strategy, business transformation, and execution expertise. Murat has undertaken various leadership roles for global organizations in North America, Europe, and Middle East building and leading high-performing cross-functional teams, creating and implementing go-to-market strategies, and achieving substantial revenue growth. Murat's extensive leadership experience spans other key business areas such as organizational development, sales strategy, digital marketing, partner management, and operations. At his current role at BeamSec, Murat is responsible for the company's vision, strategic direction, and execution of the overall business strategy.

Murat can be reached online at https://www.linkedin.com/in/muratguvenc/ and at our company website https://www.beamsec.com/

EVENTS



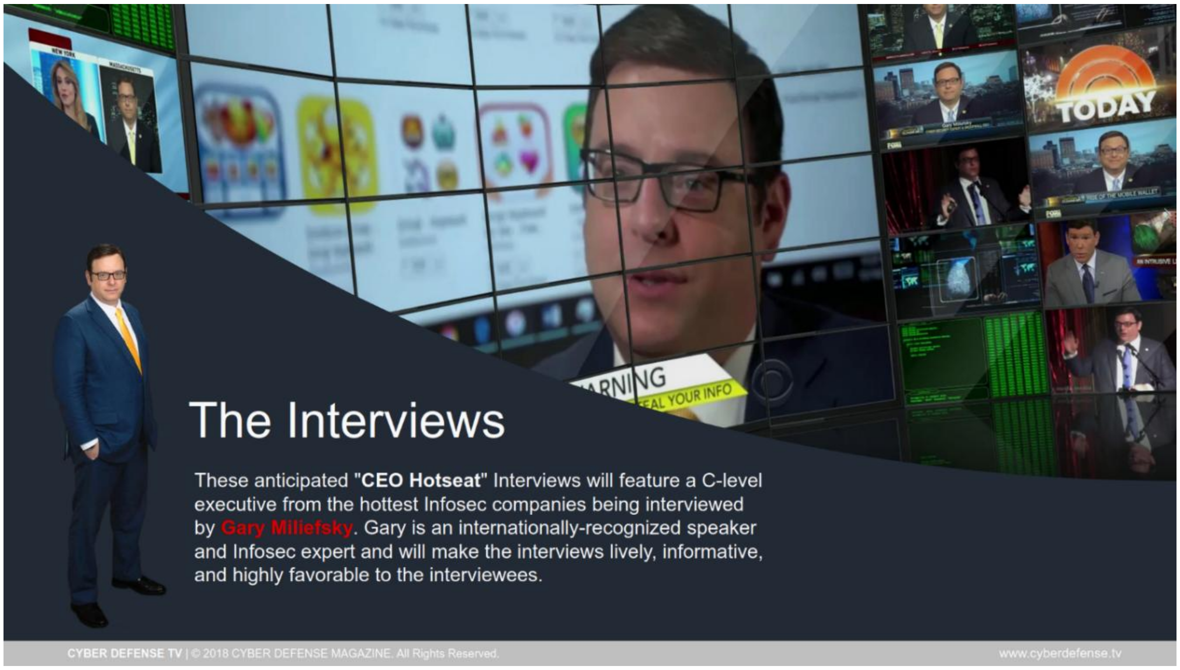
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



The Interviews

These anticipated "**CEO Hotseat**" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by Gary Miliefsky. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

---

Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them. Send us great content and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

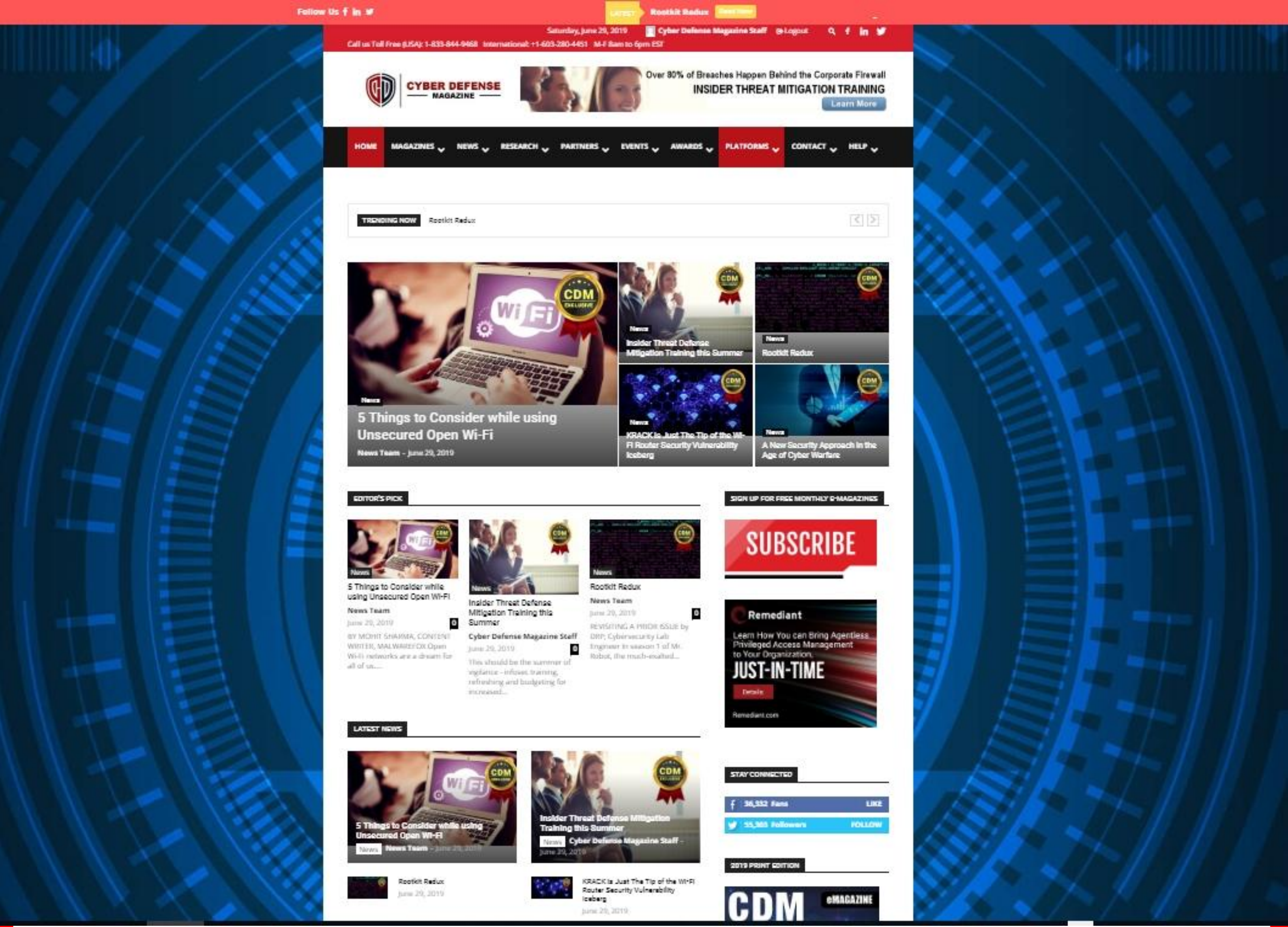
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

https://www.cyberdefensemagazine.com/

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 01/02/2025



5 Things to Consider while using Unsecured Open Wi-Fi
News Team – June 29, 2019

Insider Threat Defense Mitigation Training this Summer

Rootkit Redux

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg

A New Security Approach In the Age of Cyber Warfare

5 Things to Consider while using Unsecured Open Wi-Fi
News Team
June 29, 2019
BY MOHIT SHARMA, CONTENT WRITER, MALWAREFOX Open Wi-Fi networks are a dream for all of us....

Insider Threat Defense Mitigation Training this Summer
Cyber Defense Magazine Staff
June 29, 2019
This should be the summer of vigilance - infosec training, refreshing and budgeting for increased...

Rootkit Redux
News Team
June 29, 2019
REVISITING A PRIOR ISSUE by DRP, Cybersecurity Lab Engineer in season 1 of Mr. Robot, the much-exalted...

Learn How You can Bring Agentless Privileged Access Management to Your Organization.

5 Things to Consider while using Unsecured Open Wi-Fi
News News Team – June 29, 2019

Insider Threat Defense Mitigation Training this Summer
News Cyber Defense Magazine Staff – June 29, 2019

Rootkit Redux
June 29, 2019

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
June 29, 2019

Books by our Publisher: Amazon.com: CRYPTOCONOMY®, 2nd Edition: Bitcoins, Blockchains & Bad Guys eBook : Miliefsky, Gary: Kindle Store, Kindle Store, Cybersecurity Simplified, with others coming soon...

13 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites. We successfully launched https://cyberdefenseconferences.com/ and our new platform https://cyberdefensewire.com/

Don't risk it, secure your data today.

Ransomware disproportionately impacts small and medium sized businesses. NSA's no-cost cybersecurity services can help protect DOD contractor networks from threats.

Available to any company with an active DOD contract or access to non-public DOD information.

GET STARTED TODAY

NSA.GOV/CCC

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

CYBERSECURITY COLLABORATION CENTER

* with help from writers
and friends all over the Globe.