The Cybersecurity Handbook

A Guide for Board Members and C-Suite Executives

Richard Gwashy Young, PhD

ROUTLEDGE

A Productivity Press Book

The Cybersecurity Handbook

The workplace landscape has evolved dramatically over the past few decades, and with this transformation comes an ever-present threat: cybersecurity risks. In a world where digital incidents can lead to not just monetary loss but also reputational damage and legal ramifications, corporate governance must adapt. *The Cybersecurity Handbook: A Guide for Board Members and C-Suite Executives* seeks to empower board members and C-suite executives to understand, prioritize, and manage cybersecurity risks effectively.

The central theme of the book is that cybersecurity is not just an IT issue but a critical business imperative that requires involvement and oversight at the highest levels of an organization. The argument posits that by demystifying cybersecurity and making it a shared responsibility, we can foster a culture where every employee actively participates in risk management.

This book aims to provide essential insights and practical guidance for corporate leaders on effectively navigating the complex landscape of cybersecurity risk management. As cyber threats continue to escalate in frequency and sophistication, the role of board members and C-suite executives in safeguarding their organizations has never been more critical. This book will explore the legal and regulatory frameworks, best practices, and strategic approaches necessary for fostering a robust cybersecurity culture within organizations. By equipping leaders with the knowledge and tools to enhance their oversight and risk management responsibilities, we can help them protect their assets and ensure business resilience in an increasingly digital world.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

The Cybersecurity Handbook

A Guide for Board Members and C-Suite Executives

Richard Gwashy Young, PhD

Routledge
Taylor & Francis Group
A PRODUCTIVITY PRESS BOOK

Designed cover image: Public Image

First published 2025
by Routledge
605 Third Avenue, New York, NY 10158

and by Routledge
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

Routledge is an imprint of the Taylor & Francis Group, an informa business

ISBN: 978-1-041-00074-7 (hbk)
ISBN: 978-1-041-00073-0 (pbk)
ISBN: 978-1-003-60805-9 (ebk)

DOI: 10.4324/9781003608059

Typeset in Garamond
by Apex CoVantage, LLC

This book, *The Cybersecurity Handbook: A Guide for Board Members and C-Suite Executives*, is dedicated to the countless individuals who have dedicated their careers to safeguarding our increasingly digital world. Their tireless efforts, often underappreciated and unseen, represent the bedrock of our collective security.

It is dedicated to the unsung heroes—the cybersecurity professionals, incident responders, and security analysts—who tirelessly work to detect, prevent, and mitigate threats, often facing overwhelming odds. Their expertise and commitment are essential, and their contributions deserve both recognition and ongoing investment.

It is also a dedication to the next generation of cybersecurity leaders. To those students, researchers, and aspiring professionals who are driven by a passion to protect our shared digital future, I offer this handbook as a resource and a call to action. Your knowledge, ingenuity, and ethical dedication will be crucial in addressing the ever-evolving challenges of cybersecurity in the years to come.

Finally, I dedicate this book to my family and loved ones—for their unwavering support, patience, and understanding throughout the long process of researching, writing, and refining this work. Their love and encouragement have been indispensable, reminding me that even amidst the complexities of cybersecurity, the human connection remains paramount.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Contents

Preface

In today's interconnected world, cybersecurity threats are no longer a niche concern; they pose existential risks to organizations of all sizes and across all sectors. The devastating consequences of even a single successful cyberattack—financial losses, reputational damage, legal repercussions, and operational disruption—highlight the critical need for proactive and effective cybersecurity governance. This handbook is born from that necessity.

For years, the responsibility for cybersecurity has often resided solely within IT departments, leaving boards of directors and C-suite executives underinformed and ill-equipped to oversee this crucial area. However, the sheer sophistication and frequency of modern cyber-attacks, as evidenced by the high-profile breaches detailed within these pages (Colonial Pipeline, JSB Meat Parker, SolarWinds, and countless others), underscore the vital need for leadership from the top. Cybersecurity is no longer an IT issue; it is an *enterprise-wide* risk requiring a holistic, strategic approach.

This handbook provides a comprehensive guide for board members and C-suite executives to understand and manage cybersecurity risks effectively. It is a practical resource meticulously structured to address the critical questions confronting leaders today:

- **Understanding Cyber-Risk:** This book dissects the fundamental concepts of cybersecurity, examines various attack vectors (web-based, system-based), and explains the crucial distinctions between vulnerabilities, threats, and assets.
- **Effective Governance:** We delve into the essential framework for building a robust cybersecurity governance structure, emphasizing the critical role of the board of directors in oversight and accountability. This includes establishing clear expectations, fostering a strong cybersecurity culture, and defining the roles and responsibilities of key personnel.

- **Navigating the Legal Landscape:** The intricate and ever-evolving legal and regulatory environment surrounding cybersecurity is addressed, including detailed explanations of relevant laws (Dodd-Frank Act, SEC regulations, FCPA, GDPR). Compliance is not just a box to check; it is an ongoing process demanding diligent attention.
- **Leveraging Expertise and Resources:** We discuss how boards and C-suites can effectively utilize internal and external resources—from cybersecurity experts to legal counsel—to build a culture of preparedness and proactively mitigate risks.
- **Addressing Insider Threats:** This often-overlooked threat is thoroughly explored, providing practical strategies for detecting, investigating, and remediating malicious insider activity.
- **Outsourcing Cybersecurity:** We offer guidance on best practices for working with third-party vendors, mitigating the risks associated with outsourcing crucial security functions.

This book goes beyond theoretical discussions; it provides actionable frameworks and clear steps to help leaders translate their understanding of cyber-risk into effective strategies. It is a call to action, urging proactive measures and a paradigm shift in how organizations view and manage cybersecurity. It is time to move beyond reactive responses to build a resilient organization that thrives in the face of ever-evolving cyber threats. This handbook will serve as your guide.

Acknowledgment

To my cohort “Mixed-Methods,” mentors and colleagues, whose wisdom and collaboration have enriched my journey in this field and higher education. Your guidance has shaped my understanding of the complexities of leadership, cyber-risks, and the transformative potential of artificial intelligence. Lastly, to my family whose support and encouragement have been my anchor throughout this endeavor. Your belief in my vision fuels my passion for advancing our collective knowledge and practices in cybersecurity. Thank you for being my greatest motivation.

About the Author

Richard Gwashy Young is a seasoned technology executive and academic leader with a distinguished career in the financial services industry. Based in New York City, he currently serves as a platforms engineering and technology risk executive at one of the top global financial institutions based on Wall Street, where he leads a team of technology and cyber-risk software developers and risk managers. With extensive experience in the global financial sector, Richard is recognized for his expertise in cybersecurity, technology risk management, and regulatory compliance.

In addition to his professional accomplishments, Rich is pursuing a doctoral degree in educational leadership, where he focuses on the intersection of technology and education. He is also an educator, teaching graduate courses on technology risk management and cybersecurity. Richard is deeply committed to fostering the next generation of technology leaders, particularly in underserved communities, and is in the process of establishing a Science, Technology, Engineering, and Mathematics (STEM) school for underprivileged youths in New York City and Johannesburg, South Africa.

Introduction

The digital landscape has fundamentally reshaped the global economy, offering unprecedented opportunities for innovation and growth. However, this interconnected world has also amplified the threat of cyberattacks, transforming them from a technological nuisance into a significant strategic risk for organizations of all sizes and sectors. The consequences can be catastrophic—financial losses, reputational damage, regulatory sanctions, and even operational disruption—underscoring the critical need for proactive and comprehensive cybersecurity governance.

This handbook addresses the urgent demand for informed and effective leadership in cybersecurity. It provides a practical, actionable guide for board members and C-suite executives, equipping them with the knowledge and strategic frameworks necessary to navigate this complex and ever-evolving threat landscape.

Unlike many technical guides, this book focuses on the crucial intersection of cybersecurity with business strategy, corporate governance, and fiduciary responsibilities. It translates complex cybersecurity concepts into clear, concise, and relevant terms for non-technical audiences. The content is supported by a rigorous review of relevant laws and regulations, case studies of major cyber incidents, and insightful analysis of emerging industry best practices.

In this book, you will find:

- **A deep dive into the fundamentals of cybersecurity:** Understand the core principles of confidentiality, integrity, and availability; explore the various types of cyberattacks, both web-based and system-based; and grasp the nuances of cybersecurity vulnerabilities and threats.
- **A comprehensive framework for board oversight:** Learn about establishing an effective cybersecurity framework, making crucial structural changes for appropriate risk oversight and management,

and understanding the internal roles and responsibilities of boards of directors.

- **Guidance on effective risk management strategies:** Discover how to set the tone for cybersecurity within your organization, manage risks using a five-principle approach, and assess your company's risk appetite effectively.
- **Best practices for third-party risk management:** Understand the unique challenges of managing risks related to outsourcing cybersecurity functions and how to mitigate these risks effectively.
- **Essential considerations for environmental, social, and governance (ESG) factors:** Learn how to integrate ESG concerns into your company's cybersecurity approach.
- **A detailed guide to addressing insider risks:** Explore the steps to take when dealing with insider threats and how to create appropriate investigation procedures and policies.
- **Essential questions for the C-suite/CISO:** Utilize the specific questions highlighted in this handbook to drive a productive and insightful dialogue with your cybersecurity leadership team.

This handbook is not merely a resource; it is a call to action. The increased sophistication of cyber threats and the growing awareness of their potential impact on corporate value demand a proactive and well-informed approach to risk management. *The Cybersecurity Handbook* equips you with the tools and knowledge to meet this challenge effectively, protecting your organization and ensuring its continued success in the digital age.

Chapter 1

Background

1.1 Background

The menace of cybersecurity attacks has continued to plague diverse sectors in various parts of the world (Seema et al., 2018; Kalakuntla et al., 2019). Notable examples include the cyber-attacks launched against Colonial Pipeline, JSB Meat Parker, Toll group, Marriott International, Magellan, Twitter, and Software AG (Downs, 2020; BBC News, 2021; Turton & Mehrotra, 2021; Waldman, 2021). In April 2021, hackers gained unauthorized access to the networks of the largest fuel pipeline in the United States (Turton & Mehrotra, 2021). The security breach of Colonial Pipeline was due to a compromised password, which gave hackers entry to Colonial Pipeline's network. The cybercriminals used a virtual private network that allowed employees to access the company's computer network. The cyber-attack led to the shutdown of Colonial Pipeline and the theft of 100 gigabytes of data from the company (Turton & Mehrotra, 2021). A week after the security breach occurred, the cybercriminals demanded a ransom of $4.4 million to be paid in cryptocurrency to avoid the leak of the company's confidential data. Eventually, Colonial Pipeline paid the ransom to prevent the leak of the company's data (Turton & Mehrotra, 2021).

Similarly, in June 2021, the computer networks of the largest meat processing company in the world, JSB Meat Parker, were hacked by cybercriminals (BBC News, 2021). The launch of this cyber-attack led to the shutdown of the company's business operations in Canada, Australia, and the United States. The cybercriminals threatened to delete the files and disrupt the business activities of the company if a ransom in cryptocurrency

DOI: 10.4324/9781003608059-1

was not paid within the stipulated deadline. Although the majority of the company's plants were operational, JSB Meat Parker was forced to stop cattle slaughtering in all its plants in the United States for 24 hours. This disruption of business activities threatened the availability of food supplies and posed risks of higher food prices for consumers. In order to put an end to the ransomware attack, JSB Meat Parker paid a ransom of £7.8 million in Bitcoin, which is equivalent to $11 million to the cybercriminals (BBC News, 2021).

Toll group also experienced two incidents of a cyber-attack within three months in 2020 (Downs, 2020; Waldman, 2021). The cybercriminals launched ransomware against Toll group, which disrupted the business activities of the company. In that same year, Marriott International suffered a data breach that gave cybercriminals unauthorized access to the personal information of 5.2 million clients (Downs, 2020; Waldman, 2021). Magellan, a renowned healthcare insurance industry, also suffered a ransomware attack that led to the successful exfiltration of the personal data, tax information, and login credentials of about 365,000 patients (Downs, 2020; Waldman, 2021). Similarly, Twitter accounts were hijacked that same year by three cybercriminals via social engineering cyber-attacks. The cybercriminals gained unauthorized access to the internal management system of the social media company, including the private information of former United States President Barack Obama, Tesla CEO Elon Musk, and Amazon CEO Jeff Bezos (Downs, 2020; Waldman, 2021). Other notable cyber-attacks that occurred in the same year and their impacts include the following:

1. Microsoft. In January, a spokesperson of Microsoft announced to the public that the database for internal customer support, which was designed to store the analytics of anonymous users, was exposed online. The breach of the database led to the exposure of 250 million customer records without encryption. The data breach led to the exposure of the IP addresses, email addresses, and other personal details of Microsoft users (Aria Cybersecurity Solutions, 2021).
2. Estee Lauder. An online database that belonged to Estee Lauder was exposed online.
   This data breach resulted in the exposure of the confidential information stored in more than 440million customer records. Many customer records were left unprotected in cyberspace. Some of this information are IP addresses, pathways, email addresses, ports, and storage data. Security experts emphasized that the exposure of the confidential information of customers is largely due to the poor security

measures implemented to prevent cyber-attacks in the cosmetics company (Aria Cybersecurity Solutions, 2021).

3. MGM Resorts. In February, a hacker leaked the personal information of over 10.6 million guests of MGM Resorts hotels. These records included the personal information of celebrities like Justin Bieber, the CEO of Twitter, Jack Dorsey, and some government officials. Although MGM Resorts insisted that no financial information or passwords were exposed during the data breach, the personal information of clients exposed online may be used to foster spear-phishing campaigns. The data breach experienced by the corporation suggests the failure of the company to implement adequate cybersecurity measures to ensure the protection of their client's personal information (Aria Cybersecurity Solutions, 2021). According to Aria Security Solutions (2021), a similar data breach occurred in 2019, which also led to the online exposure of the private information of clients.
4. Facebook. In April, over 267 million Facebook profiles were available for sale at $600 on the dark web. The online exposure of the Facebook profiles was due to a data breach that occurred in December 2019. The data breach led to the disclosure of personally identifiable information such as email addresses and mobile numbers. This information can be used by cybercriminals to launch spear-phishing campaigns to retrieve user passwords and other sensitive data.
5. Zoom. During the COVID-19 lockdown, many people used the Zoom app to schedule video calls. However, the launch of a cyber-attack led to a data breach in which more than half a million Zoom teleconferencing accounts were exposed online. These accounts were available for sale on the dark web at $0.02 (Aria Cybersecurity Solutions, 2021). This data breach gave unauthorized users access to disrupt formal and informal meetings scheduled on the Zoom app. Notable ways in which cybercriminals created chaos in the Zoom app include the sharing of shock videos and pornographic videos. These cyber-attacks may be attributed to the absence of scalable cybersecurity measures to meet the growing demands of a large number of users and sudden changes in users' behaviors (Aria Cybersecurity Solutions, 2021).
6. Cognizant Technology Solutions. In April, a ransomware attack was launched against Cognizant Technology Solutions by the Maze group. The Maze group demanded the payment of a ransom to prevent the online exposure of the breached data. This cyber-attack led to the disruption of services provided to the clients of the company. Two

months later, one of the information technology management services business enterprises disclosed that the ransomware attack led to the theft of clients' information such as financial account information, names, social security numbers, tax identification numbers, passport information, and driver's licenses. Eventually, Cognizant had to pay a ransom of almost $70 million to Maze to retrieve the personal information of its clients (Aria Cybersecurity Solutions, 2021).

7. Nintendo. In April, Nintendo publicly announced that about 160,000 users were victims of a mass account hijacking carried out by cybercriminals. The data breach gave hackers unauthorized access to the payment services that were linked to this account. Such payment services are PayPal accounts and credit cards. The cybercriminals used this information to make unsolicited purchases for several weeks. The data breach led to the exposure of private information such as nicknames, gender, email addresses, and date of birth (Aria Cybersecurity Solutions, 2021). Two months later, Nintendo indicated that about 140,000 user accounts were compromised (Aria Cybersecurity Solutions, 2021).
8. Whisper. In March, cybercriminals exposed the content of a database that stored 900 million Whisper posts and the metadata of anonymous users from various social networking sites (Aria Cybersecurity Solutions, 2021). Although Whisper always referred to its cyberspace as the safest place on Earth, the cybercriminals exposed all the personal information of Whisper users. This information includes the location, personal confessions, ethnicity, gender, nickname, hometown, and age of the users. The online exposure of the content of the database allowed individuals to access the information tied to different anonymous users (Aria Cybersecurity Solutions, 2021).
9. Software AG. In October, Software AG was the victim of a double extortion attack that led to the mandatory shutdown of internal systems. The cyber-attack also resulted in a data breach that led to the theft of encrypted files (Waldman, 2021). The cybercriminals demanded a ransom of $20 million, which the software giant company refused to pay. Consequently, the decision of the company resulted in the online exposure of confidential information such as the financial information and passport details of employees (Waldman, 2021).
10. Vastaamo Psychotherapy Centre. Despite being the largest physiotherapy center in Finland, Vastaamo Psychotherapy Centre was a victim of a data breach in October 2020 (Waldman, 2021). The cyber-attack resulted

in the theft of confidential information of patients. The cybercriminals chose to blackmail the patients directly rather than demanding a ransom from the organization. About 25,000 patients were blackmailed by cybercriminals (Waldman, 2021).

11. SolarWinds. In December, it was announced that nation-state cybercriminals launched a massive cyber-attack against the supply chain of SolarWinds (Waldman, 2021). This attack was due to the insertion of a backdoor in SolarWinds software updates for the Orion platform. The insertion of a backdoor led to a breach in the security system of FireEye. As a result, the hackers gained unauthorized access to various enterprise and government networks worldwide. This security breach led to the infiltration of Microsoft's network and disruption of other activities on the Orion platform. Other major companies such as Intel, Cisco, and Nvidia also disclosed that malicious SolarWinds updates were sent to them after the security breach occurred (Waldman, 2021). This security breach is considered one of the biggest attacks in 2020 due to the high profile of victims and sophisticated execution of the cyber-attack.

The theft of confidential data is the most costly and fastest-growing segment of cyber-related crime (Tunggal, 2021a). The high incidence of this cybercrime has been attributed to the increase in the exposure of personal data to the web through cloud services (Kalakuntla et al., 2019; Tunggal, 2021b). Other factors that have contributed to the rise of cyber-attacks are the proliferation of smartphones and the Internet of Things (IoT), the ease of conducting e-commerce activities on the dark web, and the ability of cybercriminals to maintain anonymity while launching cyber-attacks outside a specific jurisdiction (Tunggal, 2021b). The aforementioned factors have led to an 11% increase in the average number of data breach incidents worldwide (Tunggal, 2021a). It is estimated that the average financial cost of cybercrime for a company has increased from $1.4 million in 2020 to $13 million in 2021 (Singh, 2019). For instance, the prevalence of cybercrimes in Africa cost the continent about $3.5 billion in 2017. As a result, digital hubs in countries such as Kenya and Nigeria suffered financial losses that accrued to $210 million and $649million, respectively. Even though many nations and organizations have continued to explore effective ways to address cyber threats, most emerging markets in different parts of the world currently operate below the cybersecurity poverty line (Singh, 2019). As a result, these markets cannot protect themselves from various vulnerabilities that are exploited by cybercriminals and are exposed to the risks of cyber-related losses (Singh, 2019). Despite the large economic costs incurred due to cybercrimes in continents like Africa that operate below the cybersecurity poverty line, about 96% of the security incidents were neither documented nor investigated (Singh, 2019).

Even though the successful execution of cyber-attacks has been attributed to the increase in the availability of sophisticated digital tools and technology, the high incidence of cyber-attacks is largely due to the ignorance of boards of directors about the importance of their cybersecurity oversight responsibilities (Cheng & Groysberg, 2017; Metivier, 2018; Vittorio & Holland, 2021). The low focus of these boards of directors on cybersecurity has resulted in economic, reputational, and regulatory costs for affected organizations. As a result, a series of lawsuits have been brought against organizations and boards of directors who chose to ignore the importance of their cybersecurity oversight responsibilities (Vittorio & Holland, 2021). For instance, the directors of Equifax Inc. had to compensate investors for the data breach experienced by the credit rating company. The sum of $149 million was paid to resolve the claims that the company misled investors about the vulnerabilities and cybersecurity defenses of the company (Vittorio & Holland, 2021).

According to Metivier (2018), the effective prevention of cyber-attacks depends on the understanding of the board of directors about cyber-risks management. The author further explained that the active involvement of the board and the establishment of a cyber-risk committee also determines the ability of a corporation to address cybersecurity-related issues. The role of various board committees on the prevention and mitigation of cyber-attacks should also be reviewed to make sure that the oversight role of the board of directors is comprehensive and well-coordinated (Lipton et al., 2018). The failure of members of the board of directors to carry out their oversight roles may lead to the issuance of an enforcement action. For instance, the inability of the members of the board in Wells Fargo to carry out the aforementioned oversight roles led to the issuance of an enforcement action by the federal reserve in 2018. The federal reserve claimed that the compliance breakdown in Wells Fargo was due to poor oversight and governance of risk by the board of directors. Furthermore, the federal reserve emphasized that the duties and responsibilities of the board of directors published in Well Fargo's corporate governance guidelines were not fulfilled (Lipton et al., 2018). In view of this, the federal reserve expressed the following views:

1. Replacement of board members.
2. The composition, practices, and governance structure of the board of directors must align with the organization's corporate strategy and risk tolerance.
3. Growth strategies in an organization should be supported by risk-management systems developed to prevent improper practices and violation of compliance to risk mitigation measures.
4. Assurances of improved monitoring and handling of known misconducts in the company should be backed up with reports of detailed and concrete plans submitted to the board of directors by the senior management.

In view of this, the board of directors is advised to clearly articulate their expectations to the senior management about the importance of ensuring the efficacy of risk management systems that have been put in place in the organization. In addition to setting high expectations for compliance departments, internal and external counsels, members of the board must also request detailed and prompt inquiries from the senior management whenever there is any evidence of compliance breakdowns in the company (Lipton et al., 2018).

Other studies have also indicated that the role of the board of directors is critical to addressing cyber-risks, preventing and mitigating cyber-attacks, and protecting the confidential information of organizations and their clients/customers (Cheng & Groysberg, 2017; Metivier, 2018). Despite the negative impacts of cyber-attacks on business activities, some organizations and boards of directors still choose to ignore the importance of their fiduciary roles and cybersecurity oversight responsibility. Furthermore, most of the boards of directors do not have the skills, support, expertise, and experience required to undertake vital oversight activities. As a member of the board in your company, do you have an up-to-date understanding of the importance of cybersecurity? Do you know your fiduciary roles and oversight responsibility in ensuring the cybersecurity of your organization?

1.2 Role of Boards of Directors in Cyber-Risk Oversight

In different parts of the world, corporations are managed by boards of directors (Vittorio & Holland, 2021). This managerial model stems from a central principle of the modern corporation, which separates the control and ownership of a corporation. The individuals who manage the organization are subject to the shareholders of the corporation. The boards of directors are responsible for overseeing various aspects of the managerial activities in their companies. However, the recent increase in financial risks has increased the focus of stakeholders on how the boards of directors aim to effectively manage the risks their corporation is exposed to. As a result, the boards of directors assume greater responsibilities in overseeing the management of all forms of risks in their respective companies (Deloitte, 2016; Cheng & Groysberg, 2017; Metivier, 2018). Some of these risks include liquidity risks, operational risks, credit risks, and cyber-risks. The board of directors must ensure that the company's management has developed and implemented effective risk management strategies to address the aforementioned risks.

The increase in the sophisticated execution of cyber-attacks provides compelling evidence that small, medium, and large-scale companies are constantly exposed to threats that may result in catastrophic cyber-attacks. Some of the detrimental implications of cyber-attacks are response costs, harm to customers and the reputation of the company, and the disruption of business operations (Cheng & Groysberg, 2017; Metivier, 2018; Tunggal, 2021b). Moreover, litigation threats and sanctions may be brought against a company and the board of directors due to their failure to establish and implement adequate measures to protect the confidential information of its clients. In view of this, it is quintessential for the boards of directors to develop and implement proactive measures to effectively address all forms of cyber-risks to their respective companies.

Despite the known consequences of cyber-attacks, not all boards of directors and members of the senior management have developed proactive steps to address various cyber-risks (Cheng & Groysberg, 2017; Metivier, 2018; Vittorio & Holland, 2021). Some studies have indicated that there is a wide gap between the proactive measures taken by the board to prevent cyber-attacks and the exposure of various corporations to cyber-risks (Deloitte, 2016; Cheng & Groysberg, 2017; Metivier, 2018). According to Blonder (2014), the boards of directors are neither paying enough attention nor allocating sufficient resources to tackling the issues of cybersecurity. Similarly, Cheng and Groysberg (2017) indicated that boards were not assuming critical oversight responsibilities related to addressing cyber-risks in their respective companies. The authors also documented that most of the boards of directors do not have the required expertise to undertake vital oversight activities such as the annual review of budgets for privacy and cybersecurity programs, the documentation of reports on cyber-risks and data breaches, and the delegation of roles and responsibilities for cybersecurity and privacy. As a result, the boards are yet to develop adequate measures to prevent or mitigate cyber-attacks (Cheng & Groysberg, 2017). Although some boards of directors pay keen attention to cyber-risks, they often rely on the senior management to implement the measures developed to address cybersecurity issues (Aguilar, 2014; Cheng & Groysberg, 2017). In order to effectively address cyber-risks, the boards of directors to explore must have an in-depth understanding of their roles and responsibilities in cyber-risk management. In view of this, the cybersecurity framework and specific roles and responsibilities of the boards required to address cyber-risk-related issues in a corporation are discussed in the following sections.

1.3 Cybersecurity Framework

The first step in addressing cyber-risk-related issues is the establishment of a suitable framework (National Institute of Standards and Technology, 2014, 2020). In view of this, the National Institute of Standards and Technology (2020) released a Framework for Improving Critical Infrastructure Cybersecurity that serves as a roadmap for boards of directors to address cyber-risks-related issues. This framework was developed to provide organizations with the best cybersecurity practices and industry standards required to address cyber-risks-related issues (National Institute of Standards and Technology, 2014, 2020; Vigliarolo, 2021). The framework is designed to help corporations to become proactive and develop strategies to tackle complex cybersecurity issues. Although the cybersecurity framework is optional for any organization, some stakeholders have suggested that the framework should be a baseline for the establishment of best cybersecurity practices in various organizations (Vigliarolo, 2021). In this regard, the boards of directors may either choose to use this exact framework or work with the senior management to develop a similar framework that aligns with the policies of their corporation.

1.4 Required Structural Changes for Appropriate Cyber-Risk Oversight and Management

Even though the National Institute of Standards and Technology has developed a suitable framework to ensure cyber-risk management, the boards of directors and senior management must have the expertise required to translate the concepts of the framework into effective action plans (Cheng & Groysberg, 2017; Metivier, 2018). Although the boards of directors either assume full oversight responsibility or delegate the role to the audit committee to address cyber-risks, many boards do not have the technical skills required to evaluate the measures put in place by the management to tackle cybersecurity issues (Deloitte, 2016; Cheng & Groysberg, 2017; Metivier, 2018). Furthermore, the audit committee of the board of directors man not possess the skills and support required to assume full oversight of the organization's cyber-risk management (Deloitte, 2016; Alina et al., 2017). Boards of directors that lack a good understanding of cybersecurity-related issues are unlikely to have the ability required to oversee cyber-risk management effectively (Deloitte, 2016; Alina et al., 2017; Cheng & Groysberg, 2017; Metivier, 2018). In view of this, some companies have mandated their boards of directors to undergo cyber-risk training programs (Deloitte, 2016; Alina et al., 2017; Metivier, 2018).

Other organizations have recommended that the board of directors must comprise members with good technical knowledge and understanding of IT-related issues that pose significant risks to the corporation.

Another strategy proposed to bridge the expertise gap and channel the attention of the boards on known cybersecurity issues is the creation of a separate committee on the board, headed by a former chief security information officer, to address the cyber-risks-related issues (Arbuckle, 2017; Chan, 2018). The establishment of such committees will foster a company-wide approach to cyber-risk management that will enhance risk monitoring and reporting for the board of directors and the senior management. This strategy will also increase the focus of the board on the allocation of adequate resources and the provision of the support required by company executives to carry out effective risk management practices (Arbuckle, 2017; Chan, 2018). Although the Dodd-Frank Act mandates large financial companies to establish independent committees on their boards to manage cyber-risks, some organizations have chosen to create such cyber-risk committees on their boards to proactively address cybersecurity issues (Deloitte, 2016; Arbuckle, 2017; Chan, 2018). Although the aforementioned strategies can be employed by the boards of directors to bridge the knowledge gap and address cybersecurity issues, it is not a panacea to the thorough oversight of cybersecurity-related issues.

1.5 Internal Roles and Responsibilities of Boards of Directors

The corporation must have the personnel required to execute effective management of cyber-risks and prepare regular reports on cyber-risks management to the board of directors (Aguilar, 2014; Deloitte, 2016). According to Deloitte (2016), some organizations have established board-level committees that are responsible for managing cyber-risks. According to Aguilar (2014), more than a third of the organizations with the appropriate personnel for cyber-risk management have full-time employees that address privacy and security risks. These employees use guidelines that are consistent with the industry standards and best cybersecurity practices recommended by the National Institute of Standards and Technology (Arbuckle, 2017; Chan, 2018; Vigliarolo, 2021). Moreover, previous studies have indicated that organizations that employed a full-time chief security information officer who reported to the senior management directly were able to detect more cybersecurity incidents and reduce financial losses in each cybersecurity incident (Arbuckle, 2017; Chan, 2018; Bailey et al., 2020). In view of this, the boards of directors should explore assigning specific full-time personnel to oversee cybersecurity issues to mitigate the negative aftermaths of cyber-attacks. The boards of directors must also have a clear understanding of the personnel at the company, which has primary oversight responsibility to manage cyber-risks (Cheng & Groysberg, 2017; Metivier, 2018). This strategy will help the company to successfully carry out cyber-risk management practices.

1.6 Preparedness of the Boards of Directors

Irrespective of the framework or measures developed by boards of directors to carry out cyber-risk management in their respective companies, the boards must ensure that their organization is prepared for inevitable cyber-attacks and the aftermaths of such incidents (Aguilar, 2014; Metivier, 2018; Bailey et al., 2020). According to Rogers and Ashford (2015), the speed at which the organization mitigates the aftermaths of a cyber-attack depends on its level of preparedness. Therefore, corporations must be prepared to respond within minutes to hours to mitigate the aftermaths of inevitable cyber-attacks. Roland and Humes (2014) also emphasized that the board of directors must devote the required personnel to detect the cyber event, analyze the incident, prevent further damage as a result of the cyber-attack, and prepare an effective response plan to stop the attack.

Even though there is no general approach to prevent and mitigate various forms of cyber-attacks, the boards of directors must endeavor to implement effective response plans to various cyber-attacks (Roland & Humes, 2014; Rogers & Ashford, 2015; Bailey et al., 2020). According to Aguilar (2014), a poorly developed response plan can inflict more damage compared to the main cyber-attack. Therefore, the boards of directors must devote more time and allocate adequate resources to ensuring that the management has developed and implemented a well-constructed response plan (Rogers & Ashford, 2015; Bailey et al., 2020). Most importantly, the boards of directors must make sure that the response plan aligns with the best cybersecurity practices for firms in the same sector (Rogers & Ashford, 2015; Deloitte, 2016). In this regard, the company must disclose how it intends to prevent and mitigate cyber-attacks to its clients/customers and investors. The nature and level of disclosure may be based on the discretion of the board of directors (Vittorio & Holland, 2021). However, the board of directors must ensure that the content of the disclosure gives their client/customers and investors a heads-up about the likelihood of cyber-attacks so that they can protect themselves.

1.7 What the Board Needs to Know about Cybersecurity

Cybersecurity can be defined as the techniques employed to ensure the protection of digital data that is stored, used, or transmitted on an information system (Seema et al., 2018). It encompasses the development of diverse processes, practices, and technologies to protect systems, networks, and programs from damage, unauthorized access, or cyber-attacks (Seema et al., 2018). According to Seema et al. (2018), specialized and unspecialized cybersecurity measures must be developed to protect the confidential information stored, used, or transmitted on an information system from all forms of cyber threats. In the past decade, cybersecurity has been the utmost concern of various stakeholders due to the high risks of cybercrime (Seema et al., 2018; Kalakuntla et al., 2019). The development of different technologies has increased the exposure of sensitive information to cyber-attacks and the incidence of cybercrimes. Many individuals, governments, and enterprises have been victims of cyber-attacks orchestrated by cybercriminals. Some of these cyber-attacks include the hacking of confidential information, wholesale fraud, malware attacks, and phishing (Singh, 2019; Tunggal, 2021b). Some of the aftermaths of the aforementioned cyber-attacks include huge debts, loss of sensitive information, and poor relationships between the customers/clients and the affected organization or enterprise (Vittorio & Holland, 2021). In view of this, concerned stakeholders have sought the expertise of professionals to ensure the protection of sensitive data. The development of technologies to facilitate online transactions has also contributed to an increase in cybercrimes. The high risks of cybercrime associated with online transactions are because the digital tools and technologies used to facilitate online transactions store crucial and confidential information of users. Therefore, high cybersecurity standards must be implemented to reduce the exposure to cyber threats associated with the use of cloud services, smart devices, internet banking, and e-commerce platforms (Vigliarolo, 2021).

According to Vigliarolo (2021), the establishment of such cybersecurity standards is quintessential to safeguarding the confidential information of users and ensuring the cybersecurity of digital infrastructures in different parts of the world.

The processes, practices, and techniques carried out to ensure cybersecurity protects systems, networks, and programs from different forms of cyber threats (Seema et al., 2018). The existence of diverse forms of cyber threats poses significant challenges to the cybersecurity of enterprise and government networks. Most often, cyber threats aim to gain unauthorized access to the sensitive information held by a country, organization, or individual. This information may include military assets, political secrets, corporate data, and personal assets.

Common examples of threats are cyberterrorism, cyber warfare, and cyber espionage. Cyber terrorism involves the innovative use of digital tools and technologies by terrorists to carry out various political agendas. Cybercriminals who engage in cyber-terrorism launch cyber-attacks on systems, networks, and telecommunication infrastructures (Seema et al., 2018). In contrast, cyber warfare pertains to the use of digital tools and technologies by a country to inflict damage on another country's network. Cyberwarfare attacks are mainly carried out by skilled hackers who have proficient knowledge about computer networks. These hackers carry out their operations under the support of their respective countries. Most of the time, the goals of these hackers are to compromise the valuable data stored in the other country's network systems, obstruct medical and transportation services, impair e-commerce activities, or disrupt the communication systems of another nation (Seema et al., 2018). Cyber espionage involves the use of digital tools and technologies to gain unauthorized access to sensitive information without the permission of the holders or owners of the data. According to Seema et al. (2018), cyber espionage is often carried out through the insertion of malware or the application of cracking techniques to gain economic, strategic, or political advantage.

The negative consequences of cybersecurity cannot be overemphasized (Kalakuntla et al., 2019). Firstly, the financial damage caused by cyber-attacks has detrimental impacts on the affected government, enterprise, or individual. Secondly, the occurrence of a data breach affects the reputation of the affected organization. This reputational damage may also lead to loss of sales, customers/clients, or low revenue. Thirdly, legal consequences of a data breach, such as regulatory sanctions and fines, make it difficult for most organizations to recover from the aftermath of cyber-attacks.

Furthermore, the use of sophisticated tools to launch cyber-attacks enables cybercriminals to gain unauthorized access to corporate information and the financial information of users (Kalakuntla et al., 2019; Downs, 2020; Waldman, 2021). Most importantly, general data protection regulations have been developed in various countries to ensure that organizations implement measures to protect users' data. In view of this, cybersecurity has become an integral aspect of multiple operations in diverse countries. As a result, there has been an increase in the establishment of appropriate and effective response plans to mitigate the aftermath of cyber-attacks (Downs, 2020). However, the successful development and implementation of such plans depend on the understanding of concerned stakeholders about the fundamentals of cybersecurity.

Chapter 2

Role of Board of Directors in Cyber-Risk Oversight

2.1 Fundamental Concepts of Cybersecurity

The fundamentals of cybersecurity include confidentiality, integrity, and availability (Malla Reddy College of Engineering & Technology, 2020). Confidentiality refers to the protection of sensitive information from unauthorized users. Confidentiality also maintains the anonymity of authorized users who share and hold sensitive data on various platforms.

However, the secrecy of authorized users may be compromised by the occurrence of man-in-the-middle (MITM) attacks or the poor encryption of sensitive data (Pande, 2017; Malla Reddy College of Engineering & Technology, 2020). Some of the measures carried out to ascertain confidentiality include data encryption, biometric verification, two-factor authentication, and the use of security tokens (Pande, 2017). On the other hand, integrity prevents the modification of confidential information by unauthorized users. Some of the measures implemented to ensure the integrity of sensitive data are the use of file permissions, regular data backups, cryptographic checksums, and uninterrupted power supplies (Pande, 2017). Availability ensures that authorized users have access to their information whenever it is required. Some of the measures implemented to ensure the integrity of confidential data are data redundancy, the backup of sensitive data to external drives, and the implementation of firewalls (Malla Reddy College of Engineering & Technology, 2020).

DOI: 10.4324/9781003608059-2

2.2 Cyber-Attacks

A cyber-attack can be defined as the deliberate exploitation of networks and computer systems by cybercriminals (Malla Reddy College of Engineering & Technology, 2020). This type of attack often involves the use of malicious codes, data, or logic to execute cybercrimes such as identity theft, financial information theft, and others. The main categories of cyber-attacks are web-based attacks and system-based attacks (Malla Reddy College of Engineering & Technology, 2020). The various types of web-based and system-based attacks are discussed in the following subsections.

2.2.1 Web-Based Attacks

Web-based attacks are cyber-attacks that are launched on web applications or websites.

The main types of web-based attacks include the following (Malla Reddy College of Engineering & Technology, 2020):

1. Injection attacks. This type of cyber-attack involves the insertion of data into a web application to either seize control of the application or retrieve specific information. Typical examples are code injection, SQL injection, and XML injection.
2. Phishing. This type of cyber-attack involves the theft of users' information such as login credentials, debit or credit card numbers, passwords, and others. Phishing occurs when a cybercriminal acts as a trustworthy entity to carry out fraudulent activities.
3. DNS spoofing. This type of cyber-attack involves the hacking of computer systems.

   DNS spoofing is carried out by introducing data to the cache of the DNS resolver, which allows the hacker to return the name server to the wrong IP address. DNS spoofing diverts traffic to the computer(s) of the hacker. This type of cyber-attack can go on for extended periods without detection.
4. Session hijacking. This type of attack involves the hijacking of a user's session over a protected network. Web applications are designed to create cookies that save user sessions. Cybercriminals can steal the cookies using this cyber-attack to gain access to a user's data.

5. Brute force. Brute force involves the application of the trial and error method. This type of cyber-attack enables the cybercriminal to generate and validate many guesses that can be used to retrieve data such as personal identification numbers, passwords, and other information. Brute force is a technique that can be employed by cybercriminals to crack encrypted data or security analysts to evaluate the network security of an organization.
6. Denial of Service. This type of cyber-attack is carried out to make a network or server resource unavailable to users. Denial of Service attacks can be achieved by flooding the targeted network or server with information or traffic that leads to a crash of the network or server. Cybercriminals use a single internet connection and a single system to launch Denial of Service attacks on a server. Denial of Service attacks can be classified as either protocol attacks, volume-based attacks, or application-layer attacks. Protocol attacks are launched to consume the server's resources. This type of attack is often measured in a packet. In contrast, volume-based attacks aim to saturate the bandwidth of the server, while application-layer attacks crash the webserver. The volume-based attack is measured in bit per second, while the application-layer attack is measured in request per second.
7. Dictionary attacks. This type of cyber-attack involves storing and validating a list of commonly used passwords to retrieve an original password.
8. URL interpretation. This type of cyber-attack involves the alteration of specific parts of a URL. URL interpretation allows the cybercriminal to create a webserver to deliver unauthorized web pages.
9. File inclusion attacks. This type of cyber-attack enables a cybercriminal to gain unrestricted access to confidential files that are held on the webserver. File inclusion attacks may also be launched to insert malicious files on the webserver by adding functionality.
10. Man-in-the-middle (MITM) attacks. This type of cyber-attack allows a cybercriminal to intercept and act as a bridge between a server and a client/customer. As a result, the cybercriminal can insert, read or change the sensitive information in the breached connection.

2.2.2 System-Based Attacks

Systems-based attacks are cyber-attacks that are launched to compromise a computer network or computer system. Common examples of system-based attacks include the following (Malla Reddy College of Engineering & Technology, 2020):

1. Virus. A virus can be described as a malware program that spreads from one computer file to the other without the knowledge of the user. Viruses are considered as self-replicating malware programs because they can multiply by inserting copies of themselves into other computer files and software programs. This malware is also designed to execute other instructions that may damage the computer system.
2. Trojan horse. Trojan horse is a malicious program that causes unexpected alterations to the activities and settings of a computer system. This malware misleads the user, which makes it difficult to detect. The trojan horse often appears as a normal software application on the computer system. However, when this application is opened or executed, the running of specific malicious codes occurs in the background of the computer system.
3. Worm. This type of system-based attack interferes with the normal functions of the computer system. The primary aim of this malware is to make copies of itself and spread it to different parts of the computer system. Most of the time, this malware originates from attachments sent via email from trustworthy owners to their clients.
4. Backdoors. Backdoors enable cybercriminals to bypass authentication processes. Most often, software developers create backdoors so that operating systems and applications can be accessed for different purposes, such as troubleshooting.
5. Bots. Bots are automated software programs that are designed to interact with different network services. Some bots execute functions automatically, while others carry out instructions when they receive a particular input. Common examples of this automated software program include chatroom bots, crawlers, and malicious bots.

2.3 The Main Layers of Cybersecurity

There are seven main layers of cybersecurity. These layers include the following: mission-critical assets, data security, application security, endpoint security, network security, perimeter security, and human layer security (Malla Reddy College of Engineering & Technology, 2020). Mission-critical assets are the data that must be protected from cybercriminals, while data security pertains to the protection of the data that is stored or transferred on different networks and systems. Similarly, application security prevents unauthorized access to applications that contain mission-critical assets. Application security also ensures the internal security of different applications. On the other hand, endpoint security prevents unauthorized access to various networks, while network security protects the connection between different networks and devices (Malla Reddy College of Engineering & Technology, 2020). Network security also guarantees the safety of the networks of different organizations. The sixth layer of cybersecurity, perimeter security, encompasses the digital and physical security procedures that protect various enterprises. The human layer of cybersecurity is considered the weakest layer of cybersecurity because it is vulnerable to attacks by cybercriminals. In view of this, cybersecurity measures such as phishing simulations and access management regulations have been established to protect the mission-critical assets of organizations from insider threats, cybercriminals, and negligent users (Malla Reddy College of Engineering & Technology, 2020). In order to ensure the efficacy of cybersecurity measures, protocols must be tailored to protect each layer of cybersecurity from cyber threats and cyber-attacks.

2.4 Cybersecurity Vulnerabilities, Cyber Threats, and Assets

In recent times, there has been an increase in the occurrence of data breaches (Seema et al., 2018; Downs, 2020; Waldman, 2021). The rapid development of various sophisticated tools has made it difficult for individuals, organizations, and governments to be fully immune to cyber-attacks. Therefore, organizations that specialize in the transmission, management, and storage of sensitive data must implement measures that will foster the regular monitoring of their cyber environment. Such cybersecurity measures must also be tailored to detect vulnerabilities in the security of networks and systems and address loopholes that may be exploited by cybercriminals (Malla Reddy College of Engineering & Technology, 2020; Vittorio & Holland, 2021). Prior to the identification of cyber threats to modern networks and data systems, concerned stakeholders must be able to distinguish between cybersecurity vulnerabilities and cyber threats.

Cybersecurity vulnerabilities can be described as the weaknesses or loopholes in the security of a network or system. The presence of these weaknesses or loopholes may be exploited by cybercriminals to launch cyber-attacks on a network or system (Pande, 2017; Malla Reddy College of Engineering & Technology, 2020; Vittorio & Holland, 2021). Common examples of vulnerabilities in networks and systems are SQL injections, cross-site scripting, server misconfigurations, and the transmission of confidential data as non-encrypted plain text. In contrast, cyber threats can be described as instances or circumstances that may have negative impacts on the security of networks or systems. Cyber threats may also affect the effective management of data on different systems and networks. Common examples of cyber threats are phishing attacks that lead to the installation of malicious applications that impairs the standard functions and activities of a system and the failure of employees to adhere strictly to cybersecurity protocols, which may lead to the occurrence of data breaches. Natural disasters such as a tornado are also considered cyber threats because they often disrupt access to networks or systems (Malla Reddy College of Engineering & Technology, 2020). The probability of cyber threats and the potential loss that may be incurred as a result of cyber threats are referred to as cybersecurity risks.

Cybersecurity risks increase the likelihood of the occurrence of cyber-attacks launched by cybercriminals (Seema et al., 2018). Cybercriminals have access to various software, hardware, and data that can be used to launch cyber-attacks against the government, enterprises, and individuals. In this regard, the purpose of cybersecurity is to prevent cybercriminals from inflicting damage on concerned stakeholders through cybercrime (Malla Reddy College of Engineering & Technology, 2020). Cybercrime can be described as a crime committed using a computer or internet-connected devices. Therefore, concerned stakeholders must develop ways to protect their enterprises and clients/customers from cybercriminals.

In an attempt to protect the corporate, financial, and personal information of concerned stakeholders, a security model referred to as the confidentiality, integrity, and availability (CIA) triad was developed (Fruhlinger, 2021). Confidentiality enables individuals to protect sensitive data from unauthorized users. The protection of confidentiality depends on the ability of the security expert to define and enforce specific access levels to private data. The process of enforcing confidentiality often involves the separation of private data into different categories that are organized by the sensitivity of the information and the individuals who require access to the private data (Fruhlinger, 2021). The sensitivity of the information depends on the level of damage that will be suffered by the user if a security breach occurs. Common ways to ensure confidentiality includes the encryption of files and volumes, access control lists, and file permissions. Similarly, integrity is a crucial component of the security model that ensures the protection of private data. This component of the CIA triad is designed to prevent the alteration or deletion of data by unauthorized users. Integrity also facilitates the reversal of any damage to the sensitive information inflicted by unauthorized users. In contrast, availability is the third component of the CIA triad that makes data available to users (Seema et al., 2018; Bailey et al., 2020; Fruhlinger, 2021). Different authentication methods, systems, and access channels are used to make data available to authorized users.

Although the CIA triad is considered a core factor in most cybersecurity practices, this view of the security model limits makes concerned stakeholders ignore other important factors that are required to develop an impregnable cybersecurity system (Malla Reddy College of Engineering & Technology, 2020). The fact that the availability component of the CIA triad ensures that authorized users have access to their sensitive information does not guarantee the protection of that data. Moreover, there is no certainty that an unauthorized user has not used an individual's hardware resources without permission (Malla Reddy College of Engineering & Technology, 2020). Concerned stakeholders must understand that the CIA triad helps to plan and implement effective security protocols. This security model cannot be used as a substitute for cybersecurity measures. However, a good understanding of the CIA triad will help stakeholders to avoid the drawbacks of this security model (Fruhlinger, 2021).

The device, data, or other components of a company's system that is valuable is referred to as assets. The device and other components of the system are considered assets because they hold sensitive information that is valuable to a particular organization (Malla Reddy College of Engineering & Technology, 2020). For instance, the smartphone, laptop, or desktop of an employee can be considered an asset because it contains confidential information. Similarly, the applications on the aforementioned devices are regarded as assets (Malla Reddy College of Engineering & Technology, 2020). Other examples of assets include critical infrastructures such as support systems and servers.

2.5 Importance of Effective Cyber-Risk Oversight

The increase in the exposure of systems and networks that hold confidential data to cyber threats has necessitated the development of cybersecurity protocols (Kalakuntla et al., 2019; Internet Security Alliance, 2020).

Irrespective of the cybersecurity measures implemented in an organization to ensure the protection of networks, other parties connected to the network such as suppliers, vendors, and clients may serve as a potential vulnerability point in the network (Internet Security Alliance, 2020). For instance, a cybercriminal who could not access the network of a renowned oil company introduced malware into the online menu of a restaurant patronized by the company's employees. When the workers placed orders using the online menu, the cybercriminal gained unauthorized access and successfully breached the firm's system (Internet Security Alliance, 2020). The financial cost of the damage caused by the launch of cyber-attacks is estimated to be more than $400–$500 billion each year (Morgan, 2016).

According to the Internet Security Alliance (2020), nations can only maximize the benefits of globalization by creating an effective and robust digital infrastructure that is secure and safe for all stakeholders (Olavsrud, 2016). In view of this, the protection of stakeholders should be a major element that should be considered and tailored into the development of cybersecurity protocols.

Most often, the boards of directors prioritize the development of strategies to promote various technological innovations and increase the profitability of their company. The undermining of the importance of cybersecurity by the boards of directors has resulted in high economic, reputational, and regulatory costs for affected organizations (Vittorio & Holland, 2021). For instance, even though investments in the development of technological solutions such as smart devices and cloud computing may help the company to save costs and enhance organizational efficiency, the improper implementation of these solutions may pose significant threats to the security of the company. In contrast, the proper implementation of the aforementioned technological innovations may enhance the cybersecurity of the firm (Internet Security Alliance, 2020). Therefore, the board of directors and senior management must be able to strike a suitable balance between cybersecurity and mitigation of losses to ensure the growth and economic development of their company in competitive markets.

Furthermore, the board of directors must make sure that the cybersecurity practices are integrated into their organization's systems, networks, and each step of the company's business operations. According to Internet Security Alliance (2020), the basic cybersecurity controls that effectively prevent more than 85% of cyber-related intrusions include the following: the restriction of administrative and user privileges, and making sure that the operating system contains regular updates for software applications. Notable examples of restricting user installation and administrative privileges are whitelisting and preventing the installation or modification of software applications (Internet Security Alliance, 2020). These cybersecurity practices enhance business efficiency and guarantee a positive return on investment. In addition, the board of directors and senior management in leading organizations must employ both reactive and proactive strategies to prevent and mitigate the negative impacts of cyber-attacks. In this regard, the board of directors and senior management must implement cybersecurity protocols that will enable them to generate intelligence and anticipate where potential cybercriminals might attack (Internet Security Alliance, 2020). In order to achieve the aforementioned objectives, the board of directors and senior management must subject their systems, processes, and networks to frequent and rigorous testing to identify vulnerabilities.

2.6 Setting the Tone for Cybersecurity in an Organization

The oversight responsibility of the boards of directors is to ensure that the organizational culture and framework required to enhance the cybersecurity of the organization have been put in place. According to Lipton et al. (2018), the board of directors must uphold their oversight role to ensure that the cyber-risk management policies and procedures developed and implemented by the senior management and cyber-risk managers align with the strategy and risk appetite of their respective companies. The author further explained that the members of the board must ensure that the cyber-risk policies and procedures are effective. In addition, the board of directors must make sure the required steps are taken to promote an enterprise-wide organizational culture that fosters cyber-risk awareness behaviors. Employees across all departments should also be trained to recognize, escalate, and address cyber-risks beyond the organization's risk appetite (Lipton et al., 2018). This approach will ensure that there are no weak cybersecurity links in any department within the company. Most importantly, the board of directors must be aware of the magnitude and type of cyber-risks their company is exposed to. The members of the board must fully mandate the senior management to develop strategies to minimize potential cyber-risks.

According to Hess and Morton (2020), a company's approach to ensuring cybersecurity must be embedded within its strategy to manage all forms of risks. Even though firms and their boards of directors are confronted with the issue of a high dynamic cyber-risk landscape that increases exposure to cyber-attacks, various strategic recommendations and guidelines have been provided by the European Director's Association and the Internet Security Alliance to help organizations establish an effective cyber-risk management framework (Hess & Morton, 2020). According to the Internet Security Alliance (2020), there are five major principles that must be followed to carry out effective cyber-risk management in companies. The principles documented in this section of the paper will be presented using a generalized format to foster reflections and discussions among the boards of directors of various companies. These principles can be tailored to suit the particular characteristics of the company, such as product life-cycle stages, company size, business plans, organizational culture, stakeholder concerns, geographic footprint, and many more.

First Principle: The Boards of Directors must understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue

In previous years, organizations have considered information security as an operational or technical problem that should be resolved by the personnel in the IT department (Internet Security Alliance, 2020). In most companies, cybersecurity efforts are handled by the IT department because of the corporate structures that have been put in place by the company. This corporate structure makes the boards of directors ignore the responsibility of overseeing the cybersecurity of the company. Although the crucial responsibility of securing the confidential information of the company is left to the personnel in the IT department, this department does not have the support and resources required to assume this responsibility. Moreover, deferring oversight responsibilities to the personnel in the IT department hinders effective communication and the critical evaluation of cybersecurity issues (Internet Security Alliance, 2020). As a result, the organization will encounter various challenges when trying to implement strategies to address cyber-risks.

Most organizations invest hugely in innovative digital technology to create and add value to their products and services. In view of this, the technical infrastructure is often the major focus of companies for the development of business strategies and improvement of operations. Depending on the services provided by the firm, some organizations may rely more on technical infrastructure compared to others (Hess & Morton, 2020; Internet Security Alliance, 2020). However, boards of directors must understand that cyber-risks must be prioritized the same way as the development of IT infrastructure. They must develop strategies to evaluate the cybersecurity of assets and the risks associated with a potential data breach. Therefore, the board of directors must understand that cybersecurity is an enterprise-wide risk management problem that must be addressed from a cross-divisional, strategic, cross-departmental, and economic perspective (Hess & Morton, 2020; Internet Security Alliance, 2020). Cybersecurity must not be considered as only an IT problem but an issue that may inflict damage to stakeholders, disrupt business operations, and compromise the security of confidential information and company assets. In view of this, the oversight of cyber-risk management should be the responsibility of all members of the board of directors.

The board of directors cannot rely on a single approach to address all cybersecurity-related risks (Hess & Morton, 2020; Internet Security Alliance, 2020). The members of the board must develop plans that are tailored to effectively manage all possible forms of cyber-risks. Companies must also create an organizational culture that ensures all employees take cybersecurity issues seriously. In this regard, best cybersecurity practices should be integrated into the human resource training programs and workshops in the company. Employees must also be enlightened and stay up-to-date on emerging cyber threats in different parts of the world (Hess & Morton, 2020; Internet Security Alliance, 2020). Most importantly, the board of directors must adopt a whole-of-organization strategy to address cybersecurity issues and mitigate the aftermaths of cyber-attacks.

In addition, effective corporate governance on cyber-risks-related issues is necessary to mitigate the negative consequences of cyber-attacks. Therefore, the members of the board must be fully involved in the development, implementation, and modification of the strategies established to deal with cyber threats and cyber-risks. The board of directors must also allocate adequate funds and resources needed across the organization to deal with known and unknown cyber threats (Internet Security Alliance, 2020). The members of the board must also make sure that the senior management incorporates risk assessment and cyber resilience into their business strategy and enterprise-wide risk management plan.

There are many difficulties in addressing all possible cyber-risks in a business ecosystem (Internet Security Alliance, 2020). These difficulties have been attributed to the sophisticated approaches employed by cybercriminals to launch cyber-attacks. For instance, the advent of spear phishing has enabled cybercriminals to successfully carry out high-profile data breaches.

This form of cyber-attack often compromises the confidentiality and integrity of sensitive data held in various systems. Moreover, the adoption of product distribution strategies that involve several suppliers and vendors in different regions and countries can increase the exposure of an organization to cyber-risks (Hess & Morton, 2020; Internet Security Alliance, 2020). Similarly, the acquisition and merging of companies increase cyber-risks due to the poor integration of complex systems within a short period.

Organizations also find it difficult to create a secure system that manages the level of connectivity between suppliers, clients/customers, partners, affiliates, and the corporate network. The most notable occurrences of data breaches resulted from vulnerabilities in the suppliers or vendors that are connected to the corporate network (Vittorio & Holland, 2021). Multiple corporations have established trust-based relationships with their suppliers and vendors (Internet Security Alliance, 2020). As a result, they share the personal information of a large number of their customers/clients with these suppliers and vendors. Cybercriminals are aware of this loophole and exploit it to gain unauthorized access to the confidential information embedded in the corporation's system.

Another potential vulnerability to the cybersecurity of a company is the storage of large amounts of sensitive data on external networks or public clouds. The fact that these companies neither operate nor have full control over these networks is a major risk. Many companies assume that cloud providers will develop adequate security measures to protect their data (Internet Security Alliance, 2020). However, this is a common mistake that may inflict damage to the reputation of the company if a data breach occurs. In this regard, the board of directors needs to make sure that the senior management assesses the cybersecurity of the company's network and the large business ecosystem in which it carries out its business operations. The members of the board must frequently engage the senior management in discussions to determine the different levels of cyber-risks that exist in the organization's business ecosystem. The board of directors must also collaborate with the management to develop suitable cyber-risk tolerance and posture for their organization (Internet Security Alliance, 2020).

The board of directors must also pay keen attention to the valuable assets of the company (Internet Security Alliance, 2020). It is the responsibility of the board to instruct the senior management on low and high probability cyber-attacks that may have catastrophic impacts on the organization. The senior management must then develop a strategy to ensure the protection of the organization's assets (Hess & Morton, 2020). The management must also assure the members of the board about the efficacy of the protection strategy created to protect the corporation's confidential information.

Despite the knowledge that it is the responsibility of the board of directors to carry out cyber-risk oversight in their respective organizations, most members of the board do not know how to effectively manage cyber-risks (Cheng & Groysberg, 2017). Even though cyber-risks can be addressed by developing an enterprise-wide risk management approach, these risks cannot be eliminated. Therefore, the board of directors must have a good understanding of the nature of the cyber threats in their company's environment (Cheng & Groysberg, 2017). The members of the board must be willing to explore a wide array of approaches to enhance the security of their company. Some of these approaches include the delegation of specific cyber-risk-related issues to audit, technology, risk, or international committees and the frequent discussion of cybersecurity-related oversight responsibilities with the management and the board (Internet Security Alliance, 2020). Prior to the nomination of members of the committee appointed to carry out cybersecurity oversight responsibilities, the members of the board must develop well-defined criteria that will guarantee the selection of appropriate candidates (Internet Security Alliance, 2020). After the establishment of the committee, the members of the committee must make sure that the strategies chosen by the board to address cybersecurity issues are suitable and applicable. The committee and the board of directors should have regular meetings to discuss the possible implications of digital transformation issues and opportunities on the cybersecurity of the organization (Internet Security Alliance, 2020). The board must always be briefed on cybersecurity issues and incidents such as mergers, acquisitions, and strategic partnerships that may expose the company to cyber-risks.

Similarly, committees with specific oversight responsibilities for cyber-related risks must receive cybersecurity briefings quarterly (Internet Security Alliance, 2020). Cybersecurity briefings must also be issued to the committee when cyber-risks-related issues arise. The boards of directors can foster the sharing of knowledge about cybersecurity-related issues by inviting members to attend committee-level discussions on cyber-risks (Internet Security Alliance, 2020). The provision of cross-committee membership is another effective way to promote dialogue about cyber-risk-related incidents among board members.

Second Principle: Board Members should understand the legal implications of cyber-risks as they relate to specific circumstances of their corporations

Over time, there has been an increase in the complexity and evolution of the regulatory and legal landscape that pertains to cybersecurity (Hess & Morton, 2020; Internet Security Alliance, 2020). As a result, the laws and regulations that guide disclosures, data protection, privacy, information sharing, and the protection of infrastructure have been subject to continuous modifications. Therefore, the members of the board must be up-to-date on the current liability issues encountered by their companies, directors, and shareholders. For instance, high-profile cyber-attacks may lead to lawsuits such as customer and shareholder class-actions. Such lawsuits may result in regulatory enforcement actions. The plaintiff may allege that the company's board of directors ignored their fiduciary duty by failing to implement effective measures to ensure the adequacy of the organization's protection against cyber breaches and their aftermaths (Hess & Morton, 2020; Internet Security Alliance, 2020). Depending on the sector of the company, exposures to cyber-risks vary significantly. Irrespective of the outcome of lawsuits or legal merits, the reputational harm caused by the occurrence of a data breach may be severe. Therefore, it is quintessential for the members of the board to document their due diligence in ensuring the protection of the organization against cyber breaches and their consequences (Hess & Morton, 2020; Internet Security Alliance, 2020). In view of this, the board of directors must consider the following:

1. Effective ways to stay aware of the region, sector, and industry-specific requirements that apply to the company. Therefore, board members must be conversant with the laws and regulations established at the local, regional, state, and national levels.
2. Efficient methods to document discussions about cybersecurity-related issues and cyber-risk management.
3. The critical analysis of emerging cyber-risks as it relates to the resilience and response plans of the company.
4. Determine the information to disclose if the company is attacked by cybercriminals.

The board of directors plays a crucial role in influencing the organizational culture in their company (Hess & Morton, 2020). Therefore, the members of the board must adopt a vigorous approach to ensuring the cybersecurity of their organization. Board members must also hold the management accountable to show employees that it is important to uphold best cybersecurity practices. Corporate governance structures must also be implemented to underpin an organizational culture that is centered on effective cyber-risk management. The board of directors should also participate in data breach simulations to increase their understanding of the response procedure of the company to cyber-attacks (Hess & Morton, 2020; Internet Security Alliance, 2020). This simulation will also help the board to mitigate the consequence of cyber-attacks and prepare board members for a potential scenario that requires them to make quick and important decisions.

The board minutes of cybersecurity-related discussions should document occasions when cyber-risk-related issues were present on the agenda at board meetings or audit committee meetings (Hess & Morton, 2020; Internet Security Alliance, 2020). The board minutes must also reflect when cybersecurity-related issues were tailored to specific business problems prior to the organization of employee training or the completion of strategic partnerships. Furthermore, the board minutes may include updates about particular cyber-risks, cyber-attack mitigation strategies, the incorporation of the company's cybersecurity strategies with its technological innovations, business operations, and policies, and reports about the cybersecurity program implemented in the company to ensure the protection of sensitive data (Hess & Morton, 2020; Internet Security Alliance, 2020).

In many countries, the government has considered the development of new regulations and policies to enhance cybersecurity and ensure privacy (Hess & Morton, 2020; Internet Security Alliance, 2020). Even though the board of directors needs to make sure that all employees adhere to the regulations provided by the government, board members must understand that compliance with these regulations does not ascertain cybersecurity (Internet Security Alliance, 2020). According to the Internet Security Alliance (2020), the regulations implemented by the government provide minimum cybersecurity measures that may not be enough to prevent cybercriminals from gaining unauthorized access to the confidential information of an organization. Moreover, the regulations developed by the government cannot prevent the launch of sophisticated cyber-attacks by cybercriminals (Internet Security Alliance, 2020). Therefore, the board of directors must contact their external and legal counsel regularly to gain a better understanding of the legal landscape in their respective countries. The role of the external and internal legal counsel is to help the organization manage the conflicting and overlapping regulations implemented by policy-makers and legislators. The implementation of such conflicting regulations is often due to the lack of coordination among policy-makers and legislators and the change in the priorities of the government. The internal and external legal counsel must brief the board of directors regularly about the requirements of the legal regulations that apply to the organization (Internet Security Alliance, 2020). The feedback provided in the form of documented reports from the senior management in the company will also help the members of the board to determine if the corporation has developed adequate measures to address its cyber-risks and potential legal risks.

Even though the reporting and disclosure requirements of an organization depend on the business activities carried out in a particular sector, the board of directors must understand that their overriding role is to exercise diligence, skill, and care for their stakeholders (Internet Security Alliance, 2020). In view of this, it is the responsibility of board members to define and enforce regulatory frameworks that will ensure the privacy and protection of sensitive data. The board of directors must also create sustainable multi-stakeholder platforms and strengthen its national and international cooperation with stakeholders (Internet Security Alliance, 2020). The cybersecurity laws and regulations developed by policy-makers are centered on the following:

1. The establishment of regulations that are under the European Union's requirements for ensuring privacy and the protection of sensitive data.
2. The incorporation of cybersecurity regulations into existing laws on financial technology.
3. The inclusion of requirements to ensure the notification of regulatory authorities of cyber breaches.

The members of the board must also be aware of cybercriminal activities that are associated with the underground economy, such as cryptocurrency trading and the laundering of assets. According to the Internet Security Alliance (2020), such activities may pose significant threats to the cybersecurity of a company.

Although policy-makers in various countries are constantly exploring ways to improve existing rules and develop new effective privacy and data protection regulations, the priority of most government authorities is the implementation of cybersecurity regulations that ensures privacy. As a result, countries in Latin America have begun to incorporate the European Union's general data protection regulation and other security directives into their existing data protection regulations. Countries in Latin America have also employed the cybercrime model developed by the Budapest Convention to enhance the cybersecurity of various organizations. In view of this, the board of directors must make sure their organization develops requirements that will facilitate the implementation of appropriate organizational and technical measures to ensure high-level cybersecurity, that guarantees privacy and data protection (Hess & Morton, 2020; Internet Security Alliance, 2020).

Currently, there have been new cybersecurity policies and requirements for storing and processing data due to the rapid development of new financial technology solutions and the increase in exposure of these solutions to cyber-attacks (Internet Security Alliance, 2020). These cybersecurity policies and requirements were developed to enlighten companies in various sectors about the cybersecurity measures that must be implemented to address cyber-risks. The increased focus of countries on the cybersecurity of financial technology services and devices has increased the cybersecurity obligations of financial institutions. The boards of directors of such institutions must be aware of their company's heavy cybersecurity obligations and collaborate with the management to develop effective strategies to address all forms of cybersecurity-related issues (Hess & Morton, 2020; Internet Security Alliance, 2020). The board of directors must also have a good understanding of existing and new policies and requirements developed at the national or international level to exercise their cybersecurity obligations appropriately.

The internal and external legal counsel of an organization plays an essential role in the mitigation against cyber-risks. The growth and increase in the number of active regulators in the field of corporate governance and cybersecurity have increased the importance of legal counsel in the fight against cyber-attacks (Internet Security Alliance, 2020). Therefore, the board of directors must ask the management to solicit the expertise of internal and external legal counsels' views on the implementation of a cybersecurity framework to mitigate against regulatory and legal risks, potential disclosure considerations that pertain to various cyber-risks, and the cyber-attack response plan developed by the organization. The legal counsel should also advise the management and the board on ways to interact with regulators in the field of corporate governance and cybersecurity, and manage important documents like board minutes (Internet Security Alliance, 2020). Most importantly, the management and the board of directors must receive regular updates from the legal counsel about the changes made to existing regulatory guidance and disclosure standards provided by the legislators and policy-makers.

The members of the board must understand that they may face litigation if their external or internal stakeholders are affected by a cyber breach

(Internet Security Alliance, 2020). The board of directors may also face litigation if shareholders claim that they failed to implement appropriate measures to ensure the protection of the corporation's assets or poorly managed the response to a data breach. Corporations may also be mandated to bring litigation as injunctions that freeze financial transactions or claims against third-party vendors or suppliers who are alleged to be responsible for a data breach (Internet Security Alliance, 2020). Under the aforementioned circumstances, the board of directors must make strategic decisions that are based on costs, the reputation of the company, prospects of success, and duties to their shareholders.

Third Principle: Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board-meeting agenda

A survey carried out by the National Association of Corporate Directors (NACD) (2016) indicated that 14% of the board of directors believe that all members have a good knowledge of cyber-risks. However, the Organization of American States (OAS) revealed that most corporate boards of directors have little or no understanding of cybersecurity and their respective fiduciary roles (Internet Security Alliance, 2020). Although some members of the board have a certain level of awareness of cybersecurity-related issues, they do not understand how cyber-risks may affect their respective corporations. The board's lack of understanding about the implications of cyber-risks explains why the management of cybersecurity-related issues has been reactive and centered on perimeter defense rather than proactive. The resilience of an organization to cyber-attacks depends on the understanding of the board of directors and the senior management about the importance of preventing and proactively mitigating cyber-risks (Hess & Morton, 2020; Internet Security Alliance, 2020). Most often, board members are unaware of where to address cyber-risks within their organizations until after the occurrence of a data breach. The board of directors must employ cybersecurity best practices within their corporate governance structure to prevent and proactively mitigate cyber-risks (Internet Security Alliance, 2020). The members of the board must have a good knowledge of the cyber-risks their company is exposed to, primary cyber-attack strategies, and protocols developed by the organization to deal with cyber threats. In view of this, the board of directors must receive regular briefings from the senior management about cybersecurity-related issues (Internet Security Alliance, 2020). According to NACD (2016), the threats and vulnerabilities to ensuring cybersecurity changes daily.

Consequently, the standards required to oversee and manage cyber-risks must be reviewed regularly to prevent and proactively mitigate cyber-risks (National Association of Corporate Directors, 2016, 2017). In order to achieve the aforementioned strategy, the boards of directors must have a certain level of cyber literacy (Hess & Morton, 2020; Internet Security Alliance, 2020).

The increase in the exposure of corporations to cyber threats has led to an increase in the responsibilities of board members. In this regard, the role of the board of directors exceeds having a good knowledge of cyber threats and receiving regular reports from the senior management (Hess & Morton, 2020; Internet Security Alliance, 2020). The members of the board must apply standard board management principles such as constructive challenge and inquiry to enhance the cybersecurity of their organization. In view of this, some organizations have considered adding experts in cybersecurity and/or information technology to the board of directors (Deloitte, 2016; Arbuckle, 2017; Chan, 2018). Although this is an effective approach to bridge the knowledge gap of the board of directors, this approach may not be applicable in all organizations. Generally, the members of the nominating and governance committee in a company must consider various factors while filling board vacancies. Some of these factors are financial knowledge, industry and global experience, the desire to control stakeholders, and other skill sets. However, business owners and shareholders have significant influence over the membership of the corporate board. Therefore, these individuals determine if a cyber expert will be added to the board of directors (Internet Security Alliance, 2020).

Irrespective of the decision of business owners or shareholders to add cybersecurity and/or information technology experts to the board of directors, the members of the board can employ other means to bring knowledgeable perspectives on cybersecurity-related issues into the boardroom. For instance, the board of directors may schedule examinations or deep-dive briefings from objective and independent cybersecurity experts. These experts can help the board to validate the efficacy of the cybersecurity programs implemented in the company. The members of the board can also solicit the expertise of independent advisors of the board, such as external auditors and external counsel on industry-wide and multi-client perspectives on cyber-risks (Hess & Morton, 2020; Internet Security Alliance, 2020). The board of directors should also participate in relevant cybersecurity education programs provided within or outside the organization to stay up-to-date on emerging cyber-risk trends. Moreover, opportunities should be provided for the members of the board to share the knowledge they obtained on cybersecurity from external programs with fellow members. The creation of cybersecurity education opportunities for business owners, shareholders, and board members is another effective way to positively influence board decisions on cybersecurity-related matters (Internet Security Alliance, 2020).

Most board members are experts in various fields. Even though directors have a high level of expertise in certain subject matters from their previous career backgrounds, they must employ a broad view of enterprise-wide risk management and response to successfully prevent and mitigate cyber-attacks (Hess & Morton, 2020). Although it is not compulsory for a corporation to include a cybersecurity expert on its board of directors, board members must have a clear understanding of where cyber responsibilities lie in the organization. In some companies, this oversight responsibility lies on the board committee, specific executives of the senior management, or the entire board of directors (Aguilar, 2014; Hess & Morton, 2020; Internet Security Alliance, 2020). However, this oversight responsibility does not cover the management of cybersecurity and cyber-risks-related issues, which is quintessential to preventing and mitigating cyber breaches.

The members of the board must understand that cyber-risks pose significant threats to stakeholders because corporations cannot protect themselves from all forms of cyber-attacks. The lack of full protection from cyber-attacks is due to the high digital interconnection of this rapidly evolving world (Aguilar, 2014; Internet Security Alliance, 2020). Moreover, cyber adversaries may have more sophisticated resources than the largest organizations. As a result, there are many difficulties associated with tracing or apprehending cybercriminals compared to conventional criminals (Aguilar, 2014; Seema et al., 2018; Internet Security Alliance, 2020). Nonetheless, the board of directors may address cyber-risks by increasing their access to security experts. Firstly, the board of directors may establish a check-and-balance system by soliciting the expertise of renowned cybersecurity experts. For instance, some companies have created reporting structures by using the following independent sources: the perspective of the individual responsible for cyber-risk management, the perspective of the individual responsible for the assessment of cyber-risks, and the perspective of the operational manager of a company (Internet Security Alliance, 2020). This structure enables the company to challenge the measures and approaches developed to ensure cybersecurity and explore various perspectives of cyber-risks.

According to the NACD (2016), the quality of information about cybersecurity provided to the board of directors was rated the lowest compared to other information. About 25% of public company directors in the United States indicated that they were not satisfied with the quality of the information provided by the senior management about cybersecurity (National Association of Corporate Directors, 2016). Some of the reasons for the dissatisfaction of the board of directors with the management's cybersecurity reports are the difficulty in interpreting the information, difficulty in using the information to evaluate the overall performance of the organization, and inadequate transparency about the overall performance of the organization (National Association of Corporate Directors, 2016, 2017). Although cyber-risks and cybersecurity are relatively new disciplines compared to financial analysis, the board of directors must establish clear expectations with the senior management about the format for the documentation of cybersecurity reports. The members of the board must also indicate the frequency and amount of details about the cybersecurity information and performance indicators that the management must include in the report (Internet Security Alliance, 2020). Furthermore, the board of directors must mandate the management to write the report using business terms.

Most importantly, the members of the board must understand that there may be a certain level of inherent bias in the report compiled by the management to trivialize the true state of the cyber-risk environment. According to Internet Security Alliance (2020), about 60% of IT staff do not report cyber-risks until such risks are difficult to mitigate or likely to result in negative aftermaths. Therefore, the boards of directors must develop an organizational culture that fosters transparent and open communication on cyber-risk reporting and management.

Fourth Principle: Board directors should set the expectation that management will establish an enterprise-wide cyber-risk management framework with adequate staffing and budget

The advent of digital technology has facilitated the integration of modern organizations, irrespective of the geographic location of employees. However, the decision-making procedures and reporting structures in these modern organizations are based on previous legacies in which each department and unit in the company make independent decisions. Therefore, the board of directors must ensure that the management is adopting an appropriate enterprise-wide approach to address cybersecurity-related matters (Hess & Morton, 2020; Internet Security Alliance, 2020).

In order to create an enterprise-wide approach to address cybersecurity-related matters, the company must first conduct an assessment of its specific cyber-risk profile and cyber threat environment. According to the Internet Security Alliance (2020), one of the greatest risks to the success of an organization that relies on digital interdependency is to conduct business operations under a poorly developed risk assessment mechanism. The success of the organization can be ensured if the board of directors has a clear understanding of the specific risk environment (Hess & Morton, 2020). The members of the board must also have a good knowledge of the availability of resources required to mitigate potential cyber-risks. The effective mitigation of cyber-risks starts with the development and implementation of an appropriate enterprise risk management system to facilitate the collection, assessment, prioritization, mitigation, and report of the organization's principal and potential cyber-risks (Hess & Morton, 2020; Internet Security Alliance, 2020).

The management must make sure that the board of directors is aware of the development and implementation of the framework developed to manage cyber-risks and protect the sensitive data of the organization. Most companies in the United States use the cybersecurity framework provided by the National Institute of Standards and Technology to establish information security standards, procedures, techniques, and practices that align business, policy, technological and cybersecurity issues (National Institute of Standards and Technology, 2020). This cybersecurity framework enables the senior management to develop an enterprise-wide approach to effectively manage cyber-risks in the organization. In other parts of America, countries have also begun to develop cybersecurity frameworks to ensure the protection of the corporation's assets. For instance, the government authorities in Peru have requested the technical expertise of the Organization of American States to establish an effective cybersecurity framework to address cyber-risks (Internet Security Alliance, 2020). The government in Peru also implemented the ISO 27001:2013 standard to prevent and mitigate cyber-attacks.

The board of directors must understand that specific cybersecurity frameworks exist for companies in different sectors. For instance, particular requirements for data protection and privacy may be mandated for companies that specialize in the production of financial technologies. Therefore, companies must select and adapt the appropriate framework to their unique industry, organizational culture, and business operations (Hess & Morton, 2020; Internet Security Alliance, 2020). In addition to having a good knowledge of the technical requirements for the establishment of the cybersecurity framework, the management must also develop a plan to ascertain technical cybersecurity and articulate the importance of the plan to the board of directors. Although the creation of a coherent framework that is driven by corporate goals facilitates compliance with requirements, the existence of this framework does not guarantee the protection and security of the company's confidential information. This is because the requirements of technical cybersecurity frameworks do not always provide an accurate picture of the measures put in place to ensure the protection of an organization's assets. However, the recent evolution in the discipline of cyber-risk management methodologies has facilitated the establishment of an empirical, contextualized, and economics-based approach to evaluate the cybersecurity of an organization (Internet Security Alliance, 2020).

The board of directors should clearly articulate their expectations of management. Some of these expectations include the adoption of a modern corporate structure to prevent the isolation of various departments in the organizations, and the implementation of a cybersecurity management framework that facilitates the creation of an enterprise-wide approach to enhance cybersecurity. This approach may involve the establishment of an enterprise-wide cyber-risk management team that is supervised by a management executive. The management executive must be an individual with enterprise-wide expertise, such as a chief financial officer, chief risk officer, chief information security officer, or chief operating officer. The board of directors must ensure that the enterprise-wide cyber-risk management team is not dominated by the IT department. In addition, the board of directors must provide the resources required by the team to assess and manage cyber-risks effectively. According to the Internet Security Alliance (2020), the board of directors must follow specific approaches to ensure proper cyber-risk governance in their respective organizations. These approaches include the following:

1. The board of directors must appoint personnel with cross-departmental authority to be responsible for the oversight responsibility of cyber-risk governance in the organization. In view of this, senior management executives such as the chief information security officer, chief risk officer, chief financial officer, or chief operating officer should be appointed to supervise the team.
2. The board of directors must appoint a cross-organization cyber-risk management team to carry out cyber-risk governance in the

organization. This team must comprise employees from all substantial stakeholder departments in the company, such as business leaders, representatives from the legal department, human resources department, internal audit department, finance department, IT department, and risk management department. The main objective of establishing a cross-organizational team is to ensure that all the departments in the company are involved in cyber-risk governance.

3. The members of the cross-organizational team must carry out a potential enterprise-wide risk assessment to determine the cyber threats the company is exposed to. The team must use a systematic framework that takes account of the complexity of cyber-risks and cyber threats. The adoption of this type of framework will help the members of the cross-organizational team to assess the current cyber threat environment of the company. Furthermore, this strategy will provide a detailed picture of the cyber-risks that pose a potential threat to the protection and security of confidential data. Most importantly, this assessment will facilitate the establishment of the company's risk appetite and the determination of its risk threshold. The outcome of the assessment will be employed in the selection of an appropriate cybersecurity framework that aligns with the goals and objectives of the company.
4. The board of directors must note that the laws and regulations on cybersecurity vary in different jurisdictions and industries. Therefore, the board of directors must mandate the management to identify the requirements and standards that apply to their specific company.
5. The management must adopt a collaborative approach to develop reports about the cybersecurity of the company. It is the role of the management to track cyber-risks and establish metrics to quantify the impacts of cyber threats and cyber-risk management strategies on the performance of the organization. For this, the management must carry out a thorough evaluation of the efficacy of cyber-risk management strategies and the cyber-resilience of the organization. This evaluation may be conducted quarterly with internal audits and other performance evaluations.
   In addition, the management must ensure that the report contains information that the members of the board need to know.
6. The senior management must develop an enterprise-wide cyber-risk management plan and internal communications strategy across all the business units and departments in the company. Although cybersecurity pertains to information technology, all stakeholders must be involved in the development, implementation, and evaluation of the

cyber-risk management plan developed to ensure the protection of the organization's assets. Regular tests should be carried out to determine the efficacy of the cyber-risk management plan.

7. The senior management must develop a cyber-risk budget that clearly articulates the resources required to meet the needs and risk appetite of the organization. Some of the resource requirements that should be documented in the budget are the need for experienced cybersecurity experts to determine the cybersecurity issues that can be addressed within the organizations or outsourced to third-party security experts. Considering the importance of cybersecurity, the allocation of resources should not be limited to the IT department. Therefore, allocations should be made to fund employee training, product development, public relations, management of vendors, and the tracking of legal regulations. The budget may also include a talent review or succession plan, assessment of the preparedness of successors, and determination of the need for additional employee training or recruitment of personnel with the required skill set. The aforementioned strategies will increase the level of preparedness of the company to prevent and mitigate cyber-attacks.

Fifth Principle: Board-management discussion about cyber-risk should include identification of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach

The board of directors must understand that it is impossible to ensure 100% cybersecurity in their respective organizations. The members of the board must also understand that the measures implemented to ensure the protection of confidential data are a continuum. Moreover, the implementation of cybersecurity measures does not ascertain the compliance of stakeholders. Therefore, the board of directors must make sure senior management teams identify the position on a spectrum of cyber-risk in which the company's controls and operations can be conducted optimally. In order to achieve the aforementioned objective, the management must determine the risk appetite of the organization (Internet Security Alliance, 2020).

Risk appetite can be defined as the level of risk a company is willing or unwilling to endure to achieve specific strategic objectives (Internet Security Alliance, 2020). The risk appetite of an organization must be one of the main priorities of the board of directors. Risk appetite is crucial because it is quintessential to the development of an effective enterprise-wide risk management approach. In this regard, the management must determine the degree of risk at which specific actions will be carried out to minimize the risk to a tolerable level. The proper determination and communication of a company's risk appetite among stakeholders drive the exhibition of positive behaviors, which is needed to set the boundaries required for running business operations successfully. The management must consider the corporate values of the company, stakeholders, the capacity of the organization, and available risk management strategies when determining the risk appetite of its firm (Internet Security Alliance, 2020). In view of this, they must consider the risks the corporation is willing or unwilling to accept, the risks that need to be addressed, the level of risks stakeholders are willing to bear, and the resources available in the company to manage various risks.

The risk appetite of a company depends on corporate objectives and particular circumstances in the corporation. Therefore, there is no general approach to determining the risk appetite of a company. However, the risk appetite of a company must be consistent with its corporate objectives and business strategy. The analysis of the cyber-risks the company is exposed to should be carried out during the process of the overall risk assessment. The outcome of this assessment will then determine the allocation of the resources required to prevent and mitigate cyber-risks. Furthermore, the senior management must provide the board of directors with a clear picture of the cyber-risk landscape, as well as the plan developed to address the risks (Internet Security Alliance, 2020). Therefore, the senior management and the board of directors must discuss and decide what systems, information, and business activities they are willing to lose. The aforementioned discussion will facilitate the determination of the level of cyber-risk, the company is willing to tolerate. Moreover, the decisions of the senior management and the board of directors will help prioritize the cybersecurity of data, systems, and business operations that are quintessential to the performance of their organization. The aforementioned decision is important because the failure of the board of directors and the management to ensure the protection of sensitive information can lead to data compromise (Internet Security Alliance, 2020). The compromise of confidential data may result in legal consequences such as regulatory sanctions for data breaches, which may damage the reputation of the organization.

Most often, the management and the board of directors in most companies apply the same cybersecurity measures to all data and systems in the company. However, the effective mitigation and prevention of cyber-risks depend on the level of sophistication of the defenses that have been put in place in the organization (Hess & Morton, 2020; Internet Security Alliance, 2020). Therefore, the senior management should focus on developing sophisticated defenses to handle cyber threats that pose significant risks to the organization. The management must allocate the resources required to implement advanced defense mechanisms that will ensure the protection of critical data and systems of the company. Most importantly, the board of directors should encourage the senior management to define the cybersecurity investments of their organization in terms of its return on investment. The efficacy of the cybersecurity investments can also be evaluated by conducting a regular reassessment of the company's return on investment (Hess & Morton, 2020; Internet Security Alliance, 2020). In addition, the management can also develop other cyber-metrics to define and assess the cyber-risks of an organization.

The board of directors and the management must concert efforts to develop and implement end-to-end solutions that can minimize cyber-risks (Hess & Morton, 2020; Internet Security Alliance, 2020). Such solutions may include preventive measures such as the regular review of cybersecurity frameworks, corporate governance practices, IT security, the management of cybersecurity services, and the completion of employee training programs. These preventive measures can help to reduce the negative consequences of a data breach. Other solutions are the application of sophisticated, proactive tools, provision of regular employee training, and cybersecurity expert response services to mitigate cyber-risk. The aforementioned strategies are crucial to adopt an enterprise-wide approach to the mitigation and prevention of cyber-risks at the managerial and board levels (Hess & Morton, 2020; Internet Security Alliance, 2020). Furthermore, the management must always inform the members of the board about the rapid evolution of the cyber-risk landscape and be flexible enough to make quick adjustments to existing cybersecurity measures and defense mechanisms of the company. The members of the board should also be willing to allocate the resources needed to purchase new technologies to prevent and mitigate cyber-risks such as data theft and corruption.

The rise in the emergence of cyber-attacks and the legal implications of such occurrences has increased the awareness of the management and the board of directors about the importance of cyber insurance (Internet Security Alliance, 2020). Cyber-insurance enables an organization to obtain financial reimbursement for the unanticipated loss associated with the occurrence of cybersecurity incidents. Examples of such cybersecurity incidents are data theft, disclosure of confidential data, phishing schemes, denial-of-service attacks, and malware insertions. Therefore, the members of the board must make sure that the company's confidential information has been insured. Before selecting a cyber-insurance firm, the board of directors must ensure that the policy offered by the cyber-insurance company suits the specific needs of their company. The frequent conduct of thorough interviews by insurers about the cybersecurity frameworks of the company will help the members of the board and the management understand the strengths and weaknesses of their cybersecurity measures and defense systems (Internet Security Alliance, 2020). Some insurers who collaborate with legal firms, public relations firms, and technology companies offer preventive measures to enhance the cybersecurity of a company.

Even though the impact of a cybersecurity incident may be assessed by carrying out a detailed assessment, the conduction of a thorough assessment may pose difficulties because various factors contribute to the occurrence of cybersecurity incidents. The increase in the publicity of the affair of a data breach may also complicate the cyber-risk evaluation procedure (Hess & Morton, 2020; Internet Security Alliance, 2020). The publicity of the occurrence may also result in reputational damage or influence stakeholders' views of the severity of the cybersecurity incident. The impact of reputational damage from a cyber incident is often severe and disproportionate. Therefore, the incumbent members of the board and C-suite must be prepared for the consequences of a cybersecurity incident. The board of directors must obtain assurances that the management has thought through the negative implications of cybersecurity incidents and devised effective strategies to ensure the proper management of cyber-risks in the company (Hess & Morton, 2020; Internet Security Alliance, 2020). These strategies may include the development of a communication and public relations plan to handle reputational risk, operational IT management, and the establishment of legal agreements with third-party vendors, suppliers, and other business partners to ensure cybersecurity.

2.7 Strong Focus of Institutional Investors on Cyber-Risk Management

The rise in the occurrence of cybersecurity incidents has increased the attention of institutional investors to the importance of cyber-risk management. As a result, risk management has become the utmost priority of institutional investors (Lipton et al., 2018). In recent times, institutional investors have taken certain steps to ensure the transparency of the activities of board members. These stakeholders have also pushed to obtain meaningful disclosures on the performance of the board of directors concerning their fiduciary roles and oversight responsibilities. For instance, a survey conducted by the NACD (2017) indicated that more than one in ten of the boards of directors who met with institutional investors took time to discuss the oversight of cyber-risks. According to Vanguard (2017), risk oversight is one of the main pillars underlying the evaluation of corporate governance practices in a particular organization. The publication by Vanguard (2017) further indicated that the members of the board are the eyes and ears of shareholders on risks. Therefore, shareholders rely on their board of directors to oversee the strategies developed by the management to prevent and mitigate cyber-risks.

In some situations, the scrutiny of institutional investors about proper risk management may translate into shareholder campaigns and recommendations from proxy advisory firms (Lipton et al., 2018). The proxy advisory firm may issue voting recommendations against a board of directors or withhold the occurrence of the board of director elections. The aforementioned decisions may be made by proxy advisory firms in the uncontested board of director elections or when an organization has experienced specific occurrences due to the failure of cyber-risk oversight responsibilities. Common examples of the failure of cyber-risk oversight responsibilities are bribery, the issuance of sanctions by regulatory bodies, serial or large fines, hedging of corporate stock, and legal settlements or judgments. For instance, in 2017, the Institutional Shareholder Services (ISS) issued voting recommendations against the board of directors at Wells Fargo due to the failure of their oversight responsibilities. The ISS recommended that all shareholders should vote against 12 out of the 15 board of directors at Wells Fargo, including the independent chairman of the organization. This decision was due to the failure of the members of Wells Fargo's board committees to carry out their oversight responsibilities. The ISS emphasized that the directors failed to provide a timely and efficient risk oversight procedure to mitigate the negative implications of the improper sale of retail banking services at Wells Fargo (Lipton et al., 2018). According to Lipton et al. (2018), the ISS has also issued voting recommendations against the board of directors who failed to carry out their oversight responsibilities in other organizations.

2.8 Corporate Culture and Risk Oversight

The members of the board and board committees on cybersecurity should collaborate with the top management to foster and promote an organizational culture that adopts enterprise-wide risk management (Lipton et al., 2018). The board of directors and the management must also make sure that the employees in the work environment understand and implement an enterprise-wide risk management approach to prevent and mitigate cyber-risks. The protocols involved in ensuring comprehensive risk management should not be considered a specialized function that is limited to the personnel in the IT department of the corporation. Cyber-risk management should be handled as a core, enterprise-wide component that is quintessential to the success and overall performance of an organization (Lipton et al., 2018). In view of this, risk assessment procedures and the evaluation of risk management processes should be integrated into all the decision-making processes of the company.

Transparency, communication, and consistency are quintessential factors to set an appropriate tone for cybersecurity at the top management level (Lipton et al., 2018). Therefore, the board of directors must communicate their vision to manage cyber-risks to all the personnel in the organization. The members of the board must share their commitment to their vision to carry out risk oversight responsibilities, intolerance to compliance failures, and ethics that must be followed to ensure cybersecurity throughout the corporation (Lipton et al., 2018). The oversight of corporate governance cultures should be one of the top priorities of board members, irrespective of the size or industry of their organization. The board members must also make sure that the cyber-risk management procedures and policies developed by the management should be integrated into the corporate strategy and business operations of the company. The directors must also seek assurances from the management that all employees follow the code of conduct and ethics of the organization. Furthermore, the top management must reinforce positive behaviors among employees by providing rewards and promotions to exemplary workers (Lipton et al., 2018). The management should also organize supplementary training programs for workers and carry out frequent compliance assessments (Internet Security Alliance, 2020). The management must brief the board of directors on the employee training programs and the protocols developed to ensure the protection of confidential data.

The recent developments about various forms of misconduct in the workplace have also contributed to the need to set an appropriate tone at the top management level (Internet Security Alliance, 2020). The misconduct of employees, such as the violation of cybersecurity compliance standards, may have deleterious impacts on the organizational culture, the morale of employees, and the preferences and perceptions of the public about the company. The delayed response of the board of directors to misconduct may damage the reputation of the company. Despite the cyber-risks associated with the violation of compliance and other misconducts, most boards of directors are yet to implement measures to address these issues appropriately. Moreover, some members of the board are yet to collaborate with the management to establish policies and procedures to prevent and mitigate cyber-risks (Internet Security Alliance, 2020). Therefore, the board of directors must consider its oversight responsibilities in respect to cybersecurity and concert efforts with the top management to address all forms of cyber-risks and cybersecurity-related incidents. The board of directors must also review the policies and procedures incorporated into the business operations of the organization regularly. In addition, the members of the board must work with the top management to develop an appropriate and effective response plan to cybersecurity-related incidents (Lipton et al., 2018). This response plan must involve the active participation of the legal counsel, human resources, and public relations personnel in the organization.

2.9 Cyber-Risk Oversight Function and Fiduciary Duties of the Board of Directors

The cyber-risk oversight function of the board of directors is derived from the state law on fiduciary duties, the state, and federal regulations and laws, the requirements and the national/international requirements and best practices for stock exchange listing (Lipton et al., 2018). The legal standards for the fiduciary duties of the board of directors in ensuring cyber-risk management were formulated by the Delaware courts. The Delaware courts have held that the board of directors at an organization is liable for a failure in board oversight responsibilities when board members fail to exercise their oversight roles (Lipton et al., 2018). A notable example of the sustained or systemic failure of board members to carry out their oversight responsibility is the lack of assurance from the top management about the development and implementation of a detailed information and reporting system on cybersecurity. The Delaware Court of Chancery's decisions have also expanded upon the aforementioned holding and reaffirmed its fundamental standard for members of the board in a corporation (Lipton et al., 2018). In view of this, lawsuits have been issued against board members due to claims of negligence of their oversight responsibilities. For instance, in 2009, some plaintiffs claimed that the directors of Citigroup failed to carry out their fiduciary duties of managing and monitoring various risks (In the Court Chancery of the State of Delaware, 2009). The plaintiffs further alleged that the defendants ignored certain red flags from press reports, which indicated the deteriorating conditions in the credit and subprime markets. However, the court dismissed the case and reaffirmed the high burdens plaintiffs in issuing a claim for the liability of a board of directors due to the failure to monitor business risk. The court emphasized that the proof of a systemic or sustained failure to exercise oversight roles is required to establish the necessary condition to liability claims (In the Court Chancery of the State of Delaware, 2009). Based on similar grounds, the court dismissed the claims of the plaintiff against the board of directors of Goldman Sachs about the failure of board members to oversee the risks in the subprime mortgage securities market (In the Court Chancery of the State of Delaware, 2011). Although the plaintiffs alleged that the compensation structure overseen by the board of directors in Goldman Sachs incentivized the top management to carry out risky investments that were beneficial to the management and detrimental to shareholders, the court reaffirmed that how an organization evaluates the risks involved in specific decisions cannot be "second-guessed by judges" (Lipton et al., 2018, p. 15).

The court also reiterated that the board of directors could only be held liable for the failure to carry out actions despite the presence of red flags. Under such circumstances, the board of directors will be held responsible for carrying out actions for reasons other than the interest of the stakeholders of their organization (In the Court Chancery of the State of Delaware, 2011). Similarly, the allegations of some plaintiffs against the board of directors of Duke Energy were dismissed by the Delaware Supreme Court because there was no evidence that the members of the board failed to carry out their oversight responsibilities despite the presence of red flags (Lipton et al., 2018). The Delaware Supreme Court stated that the board of directors of Duke Energy does not face a substantial likelihood in which they will be personally liable for deliberately causing the company to violate or disregard the law. The Delaware Supreme Court further explained that the plaintiffs did not meet the pleading requirement, which is to provide facts that support that the board of directors at Duke Energy deliberately violated or disregarded the law or carried out actions that were not in line with compliance standards. Even though the aforementioned cases were dismissed, the lawsuits caused significant damage to the reputations of Citigroup Inc., Goldman Sachs, and Duke Energy (Lipton et al., 2018).

However, the claims of the plaintiffs about the failure of the board of directors at Wells Fargo to carry out proper oversight responsibilities resulted in a different outcome (Lipton et al., 2018). Based on the Delaware law, the California court denied the motion of the defendants to dismiss the claims of the plaintiffs. This decision was made because the plaintiffs identified red flags that the board members of Wells Fargo should have identified and taken steps to address. However, the board of directors failed to carry out measures to address the red flags. The plaintiffs also alleged that the directors at Wells Fargo were aware that the employees in the company created millions of credit and debit card accounts for customers without their consent or knowledge. As a result, the Delaware court rejected the efforts of the defense to explain the reasons why the red flags were not addressed. The court concluded that even though the red flags may not appear to be significant to a large organization like Wells Fargo when viewed from a narrow perspective, the collective view shows that most of the directors deliberately disregarded their fiduciary roles despite their awareness of the increase in the creation of illegal accounts (Lipton et al., 2018). Therefore, the court stated that there is substantial proof of the likelihood of board members' oversight liability.

The outcome of the lawsuit brought against Wells Fargo is an important reminder to the board of directors that board procedures and decision-making can be questioned if the claims of the plaintiffs meet the pleading requirements of the court (Lipton et al., 2018). The pleading requirement is the provision of facts that the board of directors did not carry out actions to address the red flags that point to issues that can be experienced to reflect major problems. Therefore, the board of directors is admonished to follow logical and prudent risk management practices (Lipton et al., 2018). The members of the board must also ensure that their risk management policies are structured to meet all the requirements needed to satisfy the business judgment rule.

Chapter 3

Cybersecurity Framework

3.1 Laws and Regulations of Risk Management

In today's rapidly evolving financial landscape, understanding the intricate web of laws and regulations governing risk management is paramount for C-suite executives and board members. This chapter, "Laws and Regulations of Risk Management," delves into the critical legislation that shapes risk management practices within the financial sector. Key regulations such as the Dodd-Frank Act, the Foreign Corrupt Practices Act (FCPA), and guidelines set forth by the securities and exchange commission (SEC) play a vital role in establishing accountability and fostering robust risk management frameworks. By examining these laws, leaders can better navigate compliance challenges, enhance organizational resilience, and safeguard their institutions against financial and reputational risks. As regulatory scrutiny intensifies, a robust understanding of these frameworks is not just a legal obligation but a cornerstone of effective governance and strategic decision-making.

3.1.1 Dodd-Frank Act

The Dodd-Frank Act created new risk management protocols that are mandated by the federal government for financial institutions. The Dodd-Frank Act mandates bank holding organizations and non-bank financial institutions with an asset of at least $10 billion to set up an independent risk committee. The risk management committee must include one or more risk management experts with years of experience in the management of risks for large organizations (Lipton et al., 2018).

DOI: 10.4324/9781003608059-3

3.1.2 Securities and Exchange Commission (SEC)

The securities and exchange commission (SEC) mandates organizations to disclose the factors that make investments in the securities of a registrant risky in their annual reports. The SEC also requires a concise disclosure of the risk factors in the annual report (Securities and Exchange Commission, 2017; Lipton et al., 2018). However, there has been an increasing concern over the disclosure requirements stipulated by the SEC. Some organizations feel that they are compelled by the SEC to over-disclose and indicate boilerplate risk factors, which limits the utility of the disclosures (Securities and Exchange Commission, 2017).

The SEC has continued to review and expand its disclosure requirements to ensure that companies disclose the risk factors that pose significant threats to their business operations. In 2016, the SEC sought the public's view on the modernization and simplification of financial and business disclosure requirements in Regulation S-K (Securities and Exchange Commission, 2017; Lipton et al., 2018). The SEC then proposed the elimination of examples of risk factors included in Item 503(c) of Regulation S-K. The SEC explained that the provision of these risk factor examples might infer that the registrant must handle each of its risk factor disclosures, irrespective of the importance to its business operations. The SEC further stated that the elimination of such risk factor examples would encourage organizations to offer boilerplate risk factor disclosure (Securities and Exchange Commission, 2017; Lipton et al., 2018).

The SEC also mandates companies to disclose their board oversight responsibilities in ensuring effective risk management, the importance of the board of directors leadership structure to risk management, and the extent to which the risks emerging from an organization's compensation policies may exhibit a negative material effect on the company (Securities and Exchange Commission, 2017; Lipton et al., 2018). Furthermore, an organization must disclose how its non-executive officers, as well as compensation practices and policies, relate to risk-taking incentives and the effective management of risks (Securities and Exchange Commission, 2017).

3.1.3 Foreign Corrupt Practices Act (FCPA)

The enforcement policy for the Foreign Corrupt Practices Act (FCPA) was announced by the Department of Justice in 2017 (Lipton et al., 2018). This policy improved and codified a pilot program that was launched in 2016.

Organizations that participated in the pilot program were eligible for various mitigation credits if they voluntarily self-disclosed any form of FCPA misconduct in their workplace environment. Companies that implemented adequate and timely remedial measures and offered full cooperation towards the Department of Justice's investigation by disclosing important facts and identifying culpable personnel were also eligible for mitigation credits (FCPA Corporate Enforcement Policy, n.d.). The pilot program led to a rise in the number of organizations that willingly disclosed FCPA-related misconduct to the Department of Justice (FCPA Corporate Enforcement Policy, n.d.; Lipton et al., 2018). In view of this, about seven organizations received the Department of Justice's verdict to decline prosecution due to their involvement in the pilot program.

Based on the success of the pilot program, the Department of Justice adopted a formal and improved version of the pilot program to encourage organizations to willingly disclose FCPA-related misconduct (FCPA Corporate Enforcement Policy, n.d.; Lipton et al., 2018). The revised policy provides a presumption that the Department of Justice will not prosecute a company if it voluntarily self-reports FCPA misconduct, offers full cooperation to the Department of Justice, as well as adequately and timely remediates and consents to disgorge all forms of ill-received profits. However, this presumption will not hold if certain aggravating circumstances are associated with the nature and gravity of the offense (FCPA Corporate Enforcement Policy, n.d.; Lipton et al., 2018). Common examples of such circumstances include the following: the organization is a repeat offender, the occurrence of pervasive FCPA misconduct, the involvement of the executive management in the FCPA misconduct, and an increase in corporate return on investment due to FCPA misconduct.

In recent times, officials from the Department of Justice have employed the principles of the FCPA enforcement policy as a form of non-binding guidance in corporate investigations that are not within the FCPA jurisdiction (FCPA Corporate Enforcement Policy, n.d.; Lipton et al., 2018). The application of FCPA principles has led to an increase in anti-corruption enforcement in different parts of the world. The officials of the Trump administration at the Department of Justice and the SEC also fostered the enforcement of the FCPA. The officials issued significant enforcement actions against corporations and individuals that were guilty of FCPA misconduct. Similar anti-corruption laws and enforcement practices have been taking effect in continents such as Europe, Asia, and South America. Moreover, investigations into corrupt practices have become more predominant and international (FCPA Corporate Enforcement Policy, n.d.; Lipton et al., 2018). For instance, in 2017, coordinated international FCPA resolutions which involved the imposition of penalties were proposed by several countries.

3.2 Laws and Regulations on Cybersecurity

In 2018, the European Union's General Data Protection Regulation (GDPR) raised the regulatory bar on cybersecurity European Union (Lipton et al., 2018). The revised regulation includes an expansion of the requirements to ensure cybersecurity in European Union-based and non-European Union-based organizations. The GDPR imposes strict requirements on the collection and processing of data in companies. These requirements include increased data protection mandates, enhanced obligations to obtain the consent of the data owner, and stringent breach notification requirements. The GDPR may impose a severe penalty of 4% of a company's global revenue for non-compliance European Union (Lipton et al., 2018). The extraterritorial reach of the GDPR has contributed to its efficacy in ensuring cybersecurity in various organizations. Similarly, the New York State Department of Financial Services (DFS) in the United States has developed and implemented a detailed set of regulations to ensure cybersecurity in US-based companies (Lipton et al., 2018). The DFS mandates covered institutions authorized under the New York State insurance, banking, or financial services laws to adhere strictly to the minimum cybersecurity standards provided by the department. The revised DFS regulation also mandates covered institutions to develop and implement a cybersecurity program that is designed to protect the private data of the customers. The cybersecurity program must be approved by the boards of directors or senior corporate executive officers at the institution (Lipton et al., 2018). Furthermore, annual compliance certifications should be obtained to ascertain the efficacy of the cybersecurity program.

Similarly, the SEC has channeled its focus to data breach notification and market disclosure (Lipton et al., 2018). Ever since the Division of Corporation Finance of the SEC issued interpretative guidance for cybersecurity disclosure in 2011, public companies have been mandated to self-disclose the risks of cybersecurity incidents if they belong to one of the most important factors that contribute to the risk of an investment (U.S. Securities and Exchange Commission, 2011). In 2018, the Division of Corporation Finance of the SEC issued new guidance to provide clarification on its expectations on the aforementioned disclosures. The revised guidance is an expansion of the guidance provided in 2011, which advises public companies to provide an evaluation of the adverse effects of cyber-risks and cybersecurity incidents (Lipton et al., 2018). The revised guidance also mandates the timely disclosure of such risks.

The revised guidance also delves into new aspects of cybersecurity such as board oversight responsibilities, disclosure procedures and control, selective disclosures and insider trading (Lipton et al., 2018). In view of the SEC's regard for risk oversight, the revised guidance requires public companies to disclose the role of their board of directors in the management of cyber-risks. Public companies are mandated by the SEC to issue a disclosure if the cyber-risks are material to the conduction of business operations (Lipton et al., 2018). Even though some members of the board are actively involved in various forms of cyber-risk oversight, the requirements issued by the SEC for more disclosure may prompt directors to deepen or sharpen their level of involvement in cyber-risk oversight.

The SEC has indicated that it may adopt an aggressive approach to ensure that companies adhere to its disclosure requirements (Lipton et al., 2018). The revised guidance of the SEC also warns that the directors, officers, and other insiders in a corporation must not trade the securities of a company while they have the material non-public information. Such information may include the knowledge of a particular cybersecurity incident that occurred in the organization. In recent times, companies such as Yahoo! and Equifax have been investigated by the SEC, Department of Justice, and Federal Trade Commission. These regulatory bodies investigated the sale of shares by the executive officers in Equifax after the occurrence of a cybersecurity breach (Lipton et al., 2018). Therefore, the board of directors is always advised to examine their insider trading policies to make sure they carry out effective operations.

The members of the board are also advised to give special consideration to the restriction of insider trading prior to the public disclosure of factors that make investment risky or speculative.

3.3 Cybersecurity Governance, Risks, and Compliance

Cybersecurity governance encompasses the maintenance and management of cybersecurity measures developed to prevent and mitigate cyber-attacks (Governance and Standards Division, 2017; Lipton et al., 2018;

Internet Security Alliance, 2020). However, most directors, business managers, security managers, auditors, and other concerned stakeholders find it challenging to carry out effective cybersecurity governance in their respective organizations. The Governance and Standards Division (2017) developed a set of principles that serves as a guide to ensure effective cybersecurity governance in an organization. The application of these principles will help the board of directors to address the various risks associated with data breaches or cyber-attacks (Governance and Standards Division, 2017).

These principles include the following:

1. The board of directors and the senior management must be aware of the impacts of cybercrime or cyber warfare on the organization. These stakeholders should view the concept of cybersecurity as measures that must be implemented to prevent and mitigate the negative impacts of cybercrime or cyberwarfare. In order to ensure the proper governance of cybersecurity, the board of directors and senior management must identify the risk tolerance threshold of their organization and estimate the impact of cyber-risk on business operations. In addition, the members of the board and management must have an in-depth knowledge of various ways in which end users may be targeted by cybercriminals and affected by cyber-attacks or cybersecurity incidents.
2. The members of the board and senior management must have a good understanding of both organizational and individual behavior and culture patterns. According to the Governance and Standards Division (2017), business values and risks that are associated with cybersecurity arrangements are heavily influenced by individual and organizational culture. These cultures include employee and end-users' habits, behavior patterns, and social interactions. In order to ensure the proper governance and management of cybersecurity, the aforementioned factors must be accounted for and incorporated into the tactical, strategic, and operational cybersecurity measures developed to prevent and mitigate cyber-risks.
3. The senior management and senior risk officers should identify and clearly state the business case for cybersecurity, such as cost-benefit considerations and organizational culture, risk tolerance threshold, and risk appetite of the organization to the board of directors. The aforementioned factors will determine the cybersecurity measures that will be adopted by the company. In order to provide appropriate and

adequate cybersecurity, the business case must be well-defined and understood by the senior management and senior risk officers.

4. The board of directors must establish cybersecurity governance in the organization by setting clear rules, policies, and procedures that give the management and employees a sense of direction and logical boundaries. In order to achieve this goal, the board of directors must collaborate with the management to develop, implement, and improve a cybersecurity governance framework. The aforementioned stakeholders should ensure that the principles for the establishment of the framework align with the corporate strategies and business objectives of their organization.
5. All concerned stakeholders such as the board of directors, senior management, and senior risk officers must have a good knowledge of the cybersecurity assurance objectives that the organization aims to achieve. Cybersecurity encompasses multiple aspects and specific areas of information security. The board of directors must ensure that the senior management and senior risk officers set clear, plausible, and manageable cybersecurity assurance objectives.
6. The board of directors, senior management, and senior risk officers must work together to establish and enhance systemic cybersecurity. Most often, cybercriminals target the weakest link in an organization's system to launch a cyber-attack. Therefore, the members of the board and the management must understand that cybersecurity is a system of interdependent elements and the connections between these elements, and use this knowledge to develop, implement and optimize the company's cybersecurity measures.

3.4 Effective Approach to Establishing Cybersecurity Governance

An effective approach to ensuring effective cybersecurity governance involves the establishment of boundaries and frameworks to ensure the proper management of cyber-risks and cybersecurity-related issues, and the development of formal policies and procedures to guide stakeholders on ways to prevent cyber-risks (Governance and Standards Division, 2017). In addition to the prevention of cyber-risks, cybersecurity involves the development of procedures to handle unexpected cybersecurity incidents. In this regard, the members of the board and senior management must ensure that the state of cybersecurity governance in the company is corrective and preventive (Governance and Standards Division, 2017). The stakeholders must develop and implement corrective and preventive measures to prevent and mitigate all forms of cyber-attacks.

Effective cybersecurity governance determines the precautions, preparations, and protocols that are required to address conventional and unconventional cybersecurity incidents caused by a data breach or cyber-attack (Governance and Standards Division, 2017).

Unconventional cyber-attacks or cybersecurity incidents are launched by cybercriminals who have developed ways to circumvent the cybersecurity measures that are likely to be implemented in an organization. Therefore, cybersecurity governance must be flexible enough to allow the organization to handle both conventional and unconventional cyber-attacks and cybersecurity incidents. In order to establish flexible and effective cybersecurity governance, a six-step approach must be adopted by the board of directors and the senior management (Governance and Standards Division, 2017). These steps are discussed in the next subsections.

3.4.1 Step 1: The Identification of Stakeholder Needs

1. The board of directors, members of the independent board committee, and the senior management must identify the interests of internal and external stakeholders in organizational cybersecurity.
2. The board of directors, members of the independent board committee, and the management must incorporate confidentiality needs and mandated secrecy during the identification process.
3. The members of the board and the senior management must ensure that the principles of cybersecurity governance support the organization's objectives and protect the interest of stakeholders.
4. The members of the board and the senior management should identify reporting requirements to communicate and report detailed information about cybersecurity.
5. The members of the board and the senior management must articulate and define instances of the reliance of stakeholders on the briefings of external consultants.
6. The board of directors and the senior management must take note of the secrecy and confidentiality requirements for external consultants.

3.4.2 Step 2: The Management of Cybersecurity Transformation Strategy

Cybersecurity transformation may occur after the review and revalidation of an existing cybersecurity strategy. The purpose of carrying out cybersecurity transformation is to improve the overall system of cybersecurity governance and management from one stable state to another to ensure the effective prevention and mitigation of cyber-risks (Governance and Standards Division, 2017). The approach required to ensure successful cybersecurity transformation includes the following:

1. The board of directors, members of the independent board committee, and the senior management must review the regulatory and legal provisions for cybercrime and cyberwarfare.
2. The board of directors and members of the independent board committee must ensure that the senior management determines the risk tolerance threshold of their company concerning the occurrence of cyber-attacks and data breaches.
3. The board of directors and members of the independent board committee must ensure that the management must validate organizational needs concerning the occurrence of cyber-attacks and data breaches.
4. The members of the board must ensure that the management identifies and articulates paradigm shifts in cybersecurity or possible game-changers that may affect the efficacy of cybersecurity governance.
5. The senior management must document systemic vulnerabilities in cybersecurity as it pertains to the corporate strategy and business objectives of the organization.
6. The board of directors and members of the independent board committee must collaborate with the management to identify and validate effective and appropriate cybersecurity strategies.
7. The board of directors and members of the independent board committee must concert efforts with the management to determine the responsiveness, adaptability, and resilience of the cybersecurity strategies implemented in the company.
8. The board of directors and members of the independent board committee must collaborate with the management to identify rigid or brittle elements of cybersecurity governance that may increase the likelihood of unconventional cyber-attacks or data breaches.

9. The board of directors and members of the independent board committee must define their cybersecurity expectations and ensure that they align to the strategies implemented to prevent and mitigate cyber-risks. The expectations of these stakeholders must also align with the organizational culture and ethics of the company.
10. The board of directors and members of the independent board committee must collaborate with the senior management to identify the emergence or existence of ethical or cultural discontinuities in the organization.
11. The senior management must define the target culture for cybersecurity and develop a cybersecurity awareness program to promote this culture in the company. The senior management must brief the board of directors about the target culture identified in the organization and the need to organize a cybersecurity awareness program.
12. The board of directors, members of the independent board committee, and the senior management must be committed to ensuring the effective management of the cybersecurity transformation strategy.

3.4.3 Step 3: Definition of the Cybersecurity Structure

1. The board of directors, members of the independent board committee, and the management must define the cybersecurity organizational structure in the company.
2. The board of directors and members of the independent board committee must ensure that the senior management identifies the barriers to the adoption of cybersecurity measures.
3. The management should highlight the organizational segregation of duties and information.
4. The board of directors and members of the independent board committee should make sure the management implements an appropriate cybersecurity function for the prevention of cyber-risks and response to cyber-attacks.
5. The management must determine an optimum decision-making model to ensure cybersecurity. The management must inform the board of directors about this model prior to its application in the company.
6. The board of directors and members of the independent board committee must make sure the management defines a high-level responsible, accountable, consulted, informed (RACI) model for the cybersecurity function.

7. The board of directors and members of the independent board committee should consider all forms of extended decision rights that may be applied when a risk crisis or cybersecurity incident occurs in the company.
8. The senior management must determine the specific obligations, roles, and tasks of committee members, chief executive officers, chief financial officers, and chief risk officers. The management must inform the board of directors and independent board committee about the responsibilities of the aforementioned stakeholders.
9. The board of directors and members of the independent board committee must ensure that all the committees in the organization carry out cybersecurity practices and transformation activities.
10. Cybersecurity transformation activities should be incorporated into the committee agenda.
11. The board of directors and members of the independent board committee must ensure the management establishes escalation points for cyber-attacks, data breaches, and other cybersecurity incidents.
12. The management must define cyber threats and vulnerability escalation paths for cybersecurity transformational activities and measures.
13. The senior management and senior risk officers should establish crisis-mode and fast-track decision processes that will escalate the notification of cybersecurity incidents to these stakeholders and the board of directors.
14. The board of directors and members of the independent board committee must make sure that the senior management establishes and identifies the appropriate channels and means to communicate cybersecurity incidents and information in the organization.
15. The senior management and senior risk officers must prioritize reporting cybersecurity incidents to the board of directors and members of the independent board committee by employing the principles of a need-to-know basis and least privilege rights.
16. The board of directors and members of the independent board committee must make sure the management establishes appropriate guidance to ensure compliance with cybersecurity laws and regulations in the organization.
17. The management must incorporate cybersecurity measures into the information security protocols of the organization. These stakeholders must also highlight cybersecurity areas that are intentionally kept separate and distinct from other areas in the company.

18. The senior management and senior risk officers must create interfaces between cybersecurity functions and other security roles in the company.
19. The senior management and senior risk officers must integrate cybersecurity reporting into the general reporting methods for information security in the organization.

3.4.4 Step 4: Management of Cyber-risks

1. The board of directors and members of the independent board committee must concert efforts with the senior management and senior risk officers to identify the risk appetite and risk tolerance thresholds of the company in terms of cyber warfare/cybercrime breaches and attacks.
2. The senior management and senior risk officers must ensure that the risk tolerance thresholds align with the overall strategy, such as zero-tolerance developed to address cybersecurity incidents.
3. The senior management and senior risk officers must compare cybersecurity information with the risk tolerance thresholds required to ensure general information security to identify inconsistencies.
4. The board of directors and members of the independent board committee must ensure that the management incorporates cyber-risk assessment and management into the overall information security framework for the company.

3.4.5 Step 5: Optimization of Cybersecurity Resources

1. The board of directors and members of the independent board committee must ensure that the senior management and senior risk officers evaluate the efficacy of cybersecurity resources in comparison with the information risk and security demands of the company.
2. The board of directors and members of the independent board committee must ensure that the senior management and senior risk officers validate the reliability of the cybersecurity resources in terms of the specific objectives and goals established to prevent and mitigate cyber-attacks.
3. The management must ensure external resource management to optimize cybersecurity resources in the organization.
4. The senior management and senior risk officers must make sure that the cybersecurity resources management procedures align with the overall information security demands of the organization.

3.4.6 Step 6: Monitor the Efficacy of Cybersecurity

1. The board of directors and members of the independent board committee must ensure that the senior management and senior risk officers track the effects and outcomes of cybersecurity incidents, such as the variations in data breach incidents and methods employed by cybercriminals to launch cyber-attacks.
2. The management should compare the current state and target state expectations of cybersecurity transformation activities in the company.
3. The board of directors and members of the independent board committee must ensure that the senior management and senior risk officers incorporate cybersecurity metrics and measurements into the routine compliance monitoring mechanisms of the organization.
4. The board of directors and members of the independent board committee must ensure that the management evaluates the various threats and vulnerabilities that are quintessential to ensuring cybersecurity in the company. These stakeholders must also make sure the management integrates the dynamics of the cyber threat landscape into the cybersecurity strategies of the organization.
5. The board of directors and members of the independent board committee must ensure that the top management monitors the cyber-risk profile for data breaches and cyber-attacks, as well as the corresponding risk appetite of the company. This strategy will enable the senior management and senior risk officers to maintain an optimum balance between business opportunities and cyber-risks.
6. The board of directors and members of the independent board committee must ensure that the senior management and senior risk officers measure the efficacy of both internal and external cybersecurity resources in comparison with the defined information security goals, objectives, and demands of the organization.

Chapter 4

Required Structural Changes for Appropriate Cyber-Risk Oversight and Management

4.1 Third-Party and Fourth-Party Guidance on Best Practices For Board Oversight Risk Management

Many organizations outsource activities such as the manufacturing of product components and the provision of services to vendors referred to as third-party providers. Such organizations that outsource activities to third-party providers within or outside their jurisdiction must understand that they are responsible for the activities of these vendors and their strategic partners (fourth-party vendors) (Berman, 2018). Fourth-party providers are individuals to whom third-party vendors outsource their activities. Some of these activities include mobile banking, bill payments, core processing, and other services. According to Berman (2018), it is quintessential for organizations to identify high-risk vendors before outsourcing their services to these third-party providers. High-risk vendors or critical vendors are providers who are involved in activities that could have a detrimental impact on the business operations of an organization. Such business operations include information technology or payments services (Berman, 2018).

Third-party providers who work with critical fourth-party providers impose significant risks to the cybersecurity of organizations. Moreover, the costs and risks of managing third-party providers and vendors are quite high. In view of this, organizations must develop strategies to

DOI: 10.4324/9781003608059-4

reduce the risks associated with the outsourcing of activities to fourth-party providers. Firstly, the company must ensure that its third-party providers disclose their vendors. The third-party providers must be willing to disclose the cybersecurity, financial, and business continuity plans of their vendors to the organization. This approach will enable the company to evaluate the potential cost and risks of managing its relationship with the third-party providers and their vendors (Berman, 2018). Secondly, the organization must ensure that the contract issued to the third-party provider includes an assignment clause that prohibits the transfer of its rights to another vendor. The assignment clause must also emphasize that the third-party provider must issue a notice or seek the consent of the organization before outsourcing its activities to fourth-party providers.

The management of the relationships between companies and their vendors is an essential element of any enterprise risk management. In view of this, regulators developed detailed guidance to help companies monitor their relationships with third-party and fourth-party providers. The guidance provides information about vendor due diligence, the negotiation of contracts, effective ways to monitor third-party and fourth-party providers relationships, and the termination of contracts (Berman, 2018). The guidance provided by regulators helps organizations to understand how the management of third-party and fourth-party relationships fits into their overall strategic plan. Similarly, the Statement on Standards for Attestation Engagements 18 (SSAE 18) was published by the American Institute of Certified Public Accountants to help companies to minimize the risks of fourth-party providers (American Institute of Certified Public Accountants, 2016). The SSAE 18 includes an element of vendor management that requires a vendor to provide detailed information about the responsibilities and scope of its fourth-party providers. The SSAE 18 also mandates third-party providers to address the audits, performance reviews, and monitoring of their vendors (American Institute of Certified Public Accountants, 2016; Berman, 2018).

In recent years, various private organizations and industry-specific regulators have also recommended and published best practices for the board of directors' oversight of risk management. For instance, the National Association of Corporate Directors' Blue Ribbon Commission on risk governance and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) have provided best practices that will guide the board of directors in carrying out their oversight responsibilities

(National Association of Corporate Directors, 2017; Lipton et al., 2018). In 2017, COSO published a final version of its revised and internationally recognized enterprise-wide risk management framework. The framework comprises the following inter-related components: risk governance and culture in the organization, setting objectives for risk management, the execution of risks, the communication and reporting of risk information, and the monitoring of the performance of enterprise-wide risk management strategies. The risk culture component encompasses the tone of the company in carrying out risk governance, while the execution of risks pertains to the conduction of risk assessments that are quintessential to the development of effective corporate objectives and business strategies (Lipton et al., 2018).

One of the main changes made to the previous framework includes the provision of a simple definition of enterprise risk management to enable all the personnel in an organization to have a better understanding of the concept (Lipton et al., 2018). Another change is the clear evaluation of the role of risk culture in effective risk management. Other changes made to the framework are the provision of a detailed discussion of strategies for effective risk management, renewal of the emphasis between value and risk, increased alignment between enterprise risk management and performance, the explicit documentation of the link between risk management and decision-making in the organization, increased focus on the incorporation of the enterprise risk management approach, clear delineation between internal controls and enterprise risk management, and the improved explanation of the concept of risk tolerance and risk appetite.

The provision of a revised framework will help the members of the board to understand the importance of the relationship between risk management and the assumptions underlying various business strategies (Lipton et al., 2018). Moreover, the framework will help the board of directors to strengthen their role in the oversight of risk management.

Similarly, the Conference Board Governance Center published a document titled "The Next Frontier for Boards: Oversight of Risk Culture" (Gupta & Leech, 2015). This document provides recommendations that will help the board of directors to carry out risk governance. The report emphasizes that the board of directors must obtain periodic briefings on the board of directors' oversight of risk culture expectations from consulting firms, chief internal auditors, or external risk management experts (Gupta & Leech, 2015). Other useful recommendations provided in the document are discussed in the following sections.

4.2 The Provision of Education on the Board's Oversight of Risk Culture Expectations

The Institute of Internal Auditors and other consultants have emphasized the importance of providing education on the board's oversight of risk culture expectations (Gupta & Leech, 2015). Therefore, the board of directors should proactively issue a request to consulting firms, chief risk officers, chief internal auditors, and other experts in risk governance to provide briefings on the board's oversight of risk culture expectations. Board members can also solicit the expertise of the aforementioned specialists on the urgency with which concerned stakeholders such as the courts, local regulators, institutional investors, activist investors, and credit rating agencies will hold the management and board of directors accountable in risk governance (Gupta & Leech, 2015).

The board of directors of companies, particularly board members of organizations in the financial services industry should increase expectations of board oversight of risk culture from regulators. For instance, in the United Kingdom, the board of directors is mandated to make certain public disclosures concerning their responsibility in the oversight of risks. The members of the board are also required to confirm that none of the issues that have come to their attention suggests that the mandated representations on risk governance from board chairs concerning risk oversight practices are misleading or wrong (Gupta & Leech, 2015). According to Gupta and Leech (2015), there may be newly codified regulatory expectations of board oversight of risk culture from regulators in subsequent years.

4.3 Execution of a Complete Risk Culture Gap Assessment in the Organization

The selection criteria for carrying out a risk culture gap assessment depends on the business sector and the jurisdiction of the company. The Financial Stability Board guidance on sound risk culture is recommended for large international organizations in the financial sector (Gupta & Leech, 2015). However, the lower expectations mandated by local regulators for the oversight of risk governance may be adopted by other companies outside the financial sector. This recommendation is because few regulations have been codified by the SEC concerning the oversight responsibilities of board members in public companies outside the financial sector. Therefore, such companies are mandated to follow the generalized and broad proxy disclosure requirements documented in the SEC's Proxy Disclosure Enhancements rule (Gupta & Leech, 2015). However, the public statements issued by the SEC have emphasized the need for effective board risk oversight. According to Gupta and Leech (2015), this public remark may signal the inclusion of additional SEC codification of board risk oversight expectations for public companies outside the financial sector and may be published in subsequent years.

4.4 Implementation of a Board and C-Suite Driven or Objective-Centric Approach to Internal Audit and Enterprise Risk Management

The traditional risk-centric approaches and internal audit methods to enterprise risk management have not led to the establishment of the risk appetite framework and the oversight of risk culture recommended by local and international regulators (Gupta & Leech, 2015). Therefore, there is a need to incorporate certain changes to the traditional risk-centric approaches and internal audit methods in organizations. The publication by the Conference Board Governance Center recommends the implementation of a board and C-suite driven or objective-centric approach to internal audit and enterprise risk management should be adopted by companies to ensure the efficacy of their risk management frameworks (Gupta & Leech, 2015). According to Gupta and Leech (2015), the board of directors must seek assurances from the management about the specific results of the approaches developed to carry out the cyber-risk assessment. The management must also assure the board of directors that the risk assessment methods are yielding reliable results (Gupta & Leech, 2015). Therefore, the board must ensure that the management incorporates an enterprise risk management approach to create robust risk assessment procedures. Such risk assessment processes often yield reliable and consolidated reports on various forms of residual risks.

In past times, internal audit groups focused on carrying out spot-time audits that provided subjective views on the control efficacy of risks to the senior management and the board of directors (Gupta & Leech, 2015). However, the role of internal audit groups has been modified due to the expanded requirements envisioned by the Financial Stability Board (Financial Stability Board, 2013). A report titled "Principles for an Effective

Risk Appetite Framework" was published by the Financial Stability Board (2013) to guide the members of internal audit groups and personnel in internal audit departments on the compilation of reports to the board of directors on the efficacy of the enterprise risk management approach and risk appetite framework implemented in the organization.

4.5 Regulators Should Consider Safe Harbor Provisions for Board Risk Oversight

The low punitive nature of the legal system in the United Kingdom has led to the increased focus on board risk oversight in the region. In contrast, the punitive legal system in the United States enhances litigation risks, which may sometimes be effective in risk assessment disclosures and procedures (Gupta & Leech, 2015). In this regard, the nature of the US legal system is considered a double-edged sword. However, regulators should develop reforms that will provide a safe harbor for organizations and boards of directors who followed the regulatory requirements in good faith. These requirements should include the implementation of risk appetite frameworks and the documentation of briefings and reports on residual risks that are linked to vital business objectives and corporate strategies (Gupta & Leech, 2015). These safe harbor provisions may also apply to the board of directors of companies that involved their legal counsel about the residual risk status of the organization. Some of the residual risk statuses that should be shared with the legal counsel are contractual non-compliance, poof of illegality, deliberate acceptance of specific risks, and the lack of viable control measures to prevent and mitigate specific risks.

Chapter 5

Internal Roles and Responsibilities of Boards of Directors

5.1 CEO Accountability for Risk Appetite Frameworks and Board Reports on Residual Risk Status

The main reason for the slow implementation of robust enterprise risk management systems is due to the absence of C-suite accountability that provides the board of directors with consolidated enterprise briefings on the residual risk status of the company (Gupta & Leech, 2015). The guidance provided by the Financial Stability Board to ensure the development of effective risk appetite frameworks emphasizes the importance of increased accountability of chief executive officers. The Financial Stability Board (2013) clearly stated that chief executive officers must collaborate with a chief risk officer and chief financial officer to establish a proper risk appetite framework for their financial institution. The Financial Stability Board (2013) also emphasized that the risk appetite framework must be consistent with the short- and long-term corporate strategies, business objectives, capital plans, risk capacity, and compensation programs of the organization. In addition, the risk appetite framework must align with the supervisory expectations of the board of directors.

The chief executive officer, the chief risk officer, and the chief financial officer must also be accountable and provide reports on the escalation

DOI: 10.4324/9781003608059-5

and timely identification of breaches in risk tolerance and exposure of the company to material risks (Gupta & Leech, 2015). The role of the chief executive officer is to obtain the aforementioned results and communicate this information to the board of directors. Therefore, the chief executive officer must develop effective ways to delegate specific roles to ensure the provision of reliable information to the members of the board about the residual risk status of the company concerning its objectives and strategies. The delegation of roles may involve the appointment of a chief risk officer in the company (Gupta & Leech, 2015). Delegation may also entail assigning specific roles to a chief operating officer, senior vice president, or chief internal auditor to ensure the implementation of an effective enterprise risk management approach and risk oversight protocols. Most importantly, chief executive officers must understand their role in ensuring the reliability of risk assessment procedures and risk appetite frameworks that provide the risk status information for the board of directors (Gupta & Leech, 2015). This information will help the board of directors to identify the specific areas of the organization with the highest risks.

The requirements stipulated by regulators are often influenced by the political agenda of government officials. For instance, the enactment of the Dodd-Frank Wall Street Reform, Sarbanes-Oxley Act of 2002 and 2010, and Consumer Protection Act were all influenced by political agenda. These acts facilitated the financial sector governance reforms in various organizations (Gupta & Leech, 2015). Therefore, the board of directors of financial institutions must ensure that they follow the requirements provided by the regulators to improve board risk oversight.

Effective board oversight is quintessential to accomplishing good risk governance in an organization. However, the recent increase in the occurrence of financial crises and scandals in various companies has raised questions about the efficacy of board risk oversight in various organizations (Gupta & Leech, 2015). Some examples of the crises and scandals that have occurred in different companies are foreign exchange rate regulation scandals, multi-billion-dollar anti-money laundering settlements, and the provision of evasive tax services to clients in some banks. In view of this, US-based organizations are admonished to closely monitor SEC actions to ensure proper risk oversight. Companies in other regions such as the United Kingdom should also be prepared to follow a similar trend (Gupta & Leech, 2015).

5.2 Other Recommendations on Ways to Improve Risk Oversight

The board of directors must seek effective ways to promote continuous risk dialogue with the senior management of the organization (Lipton et al., 2018). The members of the board must also establish relationships between them and their independent committees and work together to ensure risk oversight in the company. The board of directors must also ensure the allocation of appropriate resources to support the development and implementation of risk management systems. Most importantly, the members of the board must ensure that risk management approaches are tailored to address specific risks in the company. Therefore, the board must make sure the risk management systems put in place in the organization addresses the following (Lipton et al., 2018):

1. Facilitates the timely identification of the material risks that the organization faces.
2. Ensures the implementation of appropriate risk management strategies that aligns with the organization's business strategies, risk tolerance thresholds, specific exposures to material risks, and the corporate objectives of the company.
3. Incorporates consideration of material risks and risk management into the development of strategies and decision-making processes throughout the organization.
4. Facilitates the adequate transmission of the required information about material risks to the senior management, board of directors, and independent board committee members.

According to Lipton et al. (2018), the board of directors and independent board committee members in an organization must carry out specific actions to ensure effective oversight of risk management. These actions include the following:

1. The board of directors and the senior management must carry out a regular review of the risk appetite and risk tolerance thresholds of the company. These stakeholders must also ensure that the corporate strategy and business objectives of the organization are consistent with the risk appetite and risk tolerance thresholds identified in the company.

2. The board of directors, senior management, and independent board committee members must work together to create a clear framework for holding the chief executive officer accountable for developing and maintaining an effective risk appetite framework. The chief executive officer must also be held accountable for providing the board with regular periodic reports on the residual risk status of the company.
3. The board of directors, senior management, and independent board committee members must concert efforts to review the various categories of risk their organization may face. These stakeholders must also review the likelihood of occurrence of risks, risk concentrations, and interrelationships in various areas of the company and the possible impact of such risks. Moreover, the members of the board must collaborate with the management to establish mitigation measures and action plans to address the materialization of specific risks in the company.
4. The board of directors, senior management, and independent board committee members must review effective ways in which the risks in various areas of the company can be measured. The objective of this review should be to determine the setting of individual and aggregate risk thresholds, as well as the procedures and policies needed to mitigate or prevent various risks. The stakeholders must also proffer timely responses and action plans to mitigate the consequences of materialized risks.
5. The board of directors, senior management, and independent board committee members must concert efforts to review the analysis and assumptions that underpin the identification of the principal risks in different areas of the workplace environment. The members of the board must also seek assurances from the management about the efficacy of the procedures put in place to facilitate the timely determination of materially modified or new risks. In addition, the protocols implemented in the company must enable the management to understand and account for the impacts of the materially modified or new risks on the performance of the company.
6. The board of directors must review its expectations with the senior management and independent board committee members. The expectations of the board should include each stakeholder's responsibility and role in risk oversight and risk management in the organization. This review will help stakeholders have a better understanding of their respective roles and accountabilities.

7. The members of the board should review the organization's management compensation structure and ensure that it suits the risk appetite and risk culture of the company. The board of directors must also make sure they provide appropriate incentives for adequate risk management in their organization.
8. The risk procedures and policies adopted by the senior management in the organization must be reviewed by the board of directors and independent board committee members. The board of directors must also review the protocols developed by the management to report risk-related issues and provide updates to the board and independent committee members. The board of directors must also ensure that the procedures and policies developed by the management are comprehensive and appropriate.
9. The board of directors and independent board committee members must review the management's implementation of risk procedures and policies for the company. The members of the board must also ensure that the policies and procedures are strictly adhered to throughout the organization.
10. The members of the board and independent board committee members must review the type, quality, and format of the risk-related information provided to the board with the senior management.
11. The board of directors and independent board committee members should review the steps taken by the senior management to ensure the independence of risk management functions and the processes developed to resolve the issues that arise if specific risks materialize in the company. The members of the board must also review the procedures put in place to address the escalation of variations in business operations and risk management functions.
12. The board of directors and independent board committee members must review the senior management's design of the organization's risk management functions. The stakeholders must also review the backgrounds and qualifications of senior risk officers and other personnel involved in the development and implementation of risk policies in the company. The board of directors and independent board committee members should also ensure that the required number of personnel are assigned to carry out risk management functions in the company. The number of personnel should be based on the size of the organization and the scope of its business operations.

13. The members of the board and committee should review the main elements that comprise the risk culture of the organization with the senior management. These stakeholders must also concert efforts to set up a tone that reflects the core values of the company. The members of the board must also share their expectations on the conduct of employees with the management. For instance, the board expects the employees in the company to always act with integrity and escalate non-compliance issues within and outside the company. Other expectations include the implementation of effective accountability mechanisms to make sure all employees comprehend the organization's approach to risks and risk-related objectives, as well as the creation of a workplace environment that encourages open communication, fosters a critical attitude during decision-making processes, offers a reward, and reinforces the desired risk management behaviors among employees in the company.
14. The board of directors, senior management, and independent board committee members must review how the risk management strategy of the company will be communicated to the appropriate departments in the organization. This review will facilitate the successful integration of the enterprise-wide approach in the organization.
15. The members of the board, senior management, and independent board committee members must review the internal systems of informal and formal communication across various departments in the company. This review will foster the coherent and prompt flow of risk-related data across and within all business units in the company, and timely escalation of risk-related information to the senior management, board of directors, and board committee members.
16. The board of directors and independent board committee members must review the reports provided by the senior management, internal auditors, independent auditors, regulators, legal counsel, external experts, and stock analysts concerning the risks faced by the organization and the risk management functions of the organization. The members of the board must also employ their experience, expertise, and knowledge to determine if the risk oversight functions are well-equipped to oversee each facet of the company's risk profile, including the aspect of cybersecurity. The board of directors must also determine if the provision of education on subject-specific risks is necessary for the organization.

Furthermore, the board of directors must formally conduct an annual review of the organization's risk management system (Internet Security Alliance, 2020; Lipton et al., 2018). The board must also review both committee-level and board-level risk oversight procedures and policies implemented by the senior management in the company. The review should also include a detailed presentation of relevant and best risk management practices that have been tailored to prevent and mitigate risk-related issues in the company. The board of directors and independent board committee members should also solicit the expertise of external consultants in reviewing the effectiveness of the risk management systems of the company (Internet Security Alliance, 2020; Lipton et al., 2018). These external consultants can also help the board of directors, independent board committee members, and senior management to understand and analyze specific risks that pose significant issues to the performance of the company.

The board of directors should understand that risks are subject to sudden and constant change and ensure that regular risk assessments are carried out in the company (Internet Security Alliance, 2020; Lipton et al., 2018). The review of risk assessment processes should not replace the need to carry out frequent re-assessments of the procedures and operations that take place in the company. The members of the board must learn from past mistakes and external events, such as the Wells Fargo case (Lipton et al., 2018). Most importantly, the members of the board and independent board committee members must ensure that the practices in their organization allow them to address critical issues whenever they arise (Internet Security Alliance, 2020; Lipton et al., 2018). If a new or main risk occurs in the company, the senior management must carry out a thorough investigation and provide a detailed report of the outcome to the members of the board and independent board committee members.

The board of directors should also pay more attention to the identification of external pressures that may push an organization to take excessive risks (Lipton et al., 2018). In recent times, some organizations have come under external pressure from activist investors and hedge funds to focus on producing short-term results, which is sometimes at the expense of accomplishing long-term goals. Such demands may push a firm to carry out steps that will increase its risk profile. Examples of the impacts of such requests include the rise in leverage to pay out dividends or repurchase shares, spinoffs that result in underinvestment in areas that are critical to helping an organization to maintain a competitive edge in the sector, and poor investment decisions that lead to smaller capitalizations (Lipton et al., 2018). Therefore, board members must also consider the best ways to address such pressures. Although some of the demands advocated by activist shareholders are logical for some organizations under certain circumstances, the members of the board must focus on the impact of these demands on the risk profile of the company (Lipton et al., 2018). The board of directors must also be prepared to resist external pressures to carry out actions that are not in the best interest of the company or its shareholders. In addition, the board of directors must explain the reasons for such decisions to the shareholders of the organization.

5.2.1 Situating Risk Oversight Functions in an Organization

Despite the importance of discussing the impacts of fundamental risks on the corporate strategy of a company with all members of the board, most board of directors delegate the role of overseeing risk management to the audit committee. Even though this practice is consistent with the New York Stock Exchange (NYSE) regulation that mandates the members of the audit committee to discuss policies related to risk management and risk assessment, the responsibility delegated to the audit committee should be more of a coordination role. Therefore, the board of directors must make sure that they oversee the coordination role of various committees established to address the specific risks that arise from certain structures in the organization. The financial institutions covered by the Dodd-Frank Act must have a committee that is devoted to ensuring effective risk management. The criteria required for the selection of dedicated members of the risk management committee depends on the industry, corporate strategy, business objectives, and company size, among others.

The members of the board should understand that the effective management of different types of risks depends on the expertise of the members of various risk management committees. Therefore, the creation of different risk management committees provides an added advantage that outweighs the benefits of establishing a single risk management committee. In view of this, many companies have created separate risk management committees (Ernst and Young Center for Board Matters, 2017). According to a survey of S&P 500 companies carried out by the Ernst and Young Center for Board Matters (2017), the number of companies that have at least one separate risk committee increased from 61% in 2011 to 75% in 2017. The board of directors of these companies has at least one individual risk committee apart from mandatory risk committees such as compensation risk committees, audit committees, and risk governance committees (Ernst and Young Center for Board Matters, 2017). However, the establishment of a separate risk management committee is less predominant in companies that are not in the financial industry (Ernst and Young Center for Board Matters, 2017).

Despite the benefits of having separate risk committees, issues may arise in delegating the specific responsibilities of the separate risk committees (Lipton et al., 2018). The primary oversight role and decision-making process of these separate committees must align with the overall risk management system of the organization. The board of directors must seek assurances from the members of each separate risk committee that their responsibilities do not conflict with the overall risk management system put in place in the organization (Lipton et al., 2018). Furthermore, the board of directors must make sure they coordinate and communicate their overall risk oversight roles appropriately (Ernst and Young Center for Board Matters, 2017; Lipton et al., 2018).

The importance of having separate risk committees is that they can be tasked with the primary oversight of risk in specific areas of the organization (Lipton et al., 2018). For instance, banking industries have finance or credit committees, while energy-producing organizations often maintain policy committees that are dedicated to handling safety and environmental issues that may arise while carrying out their business operations. Irrespective of the risk oversight roles delegated to specific committees, the board of directors must ensure that the activities of the different committees are well-coordinated to support the risk management processes and systems that have been put in place in the organization. The board of directors that limits the primary oversight role or risks in the organization to the audit committee must ensure that the members of the committee schedule a time for the periodic review of risk management processes with the board (Lipton et al., 2018). The board of directors must also seek assurances from the audit committee that each member understands their role, which includes the review of accounting compliance, financial statements, and the primary oversight of risks in the company.

5.2.2 Maintaining the Lines of Communication and Information Flow in the Organization

The relationship between the board of directors, senior management, and senior risk officers influences the ability of the board to carry out its oversight role in an organization. Similarly, the flow of information among the members of the board, senior management, and senior risk officers determines the efficacy of the board in the oversight of risk management. Therefore, the board of directors should be proactive in demanding sufficient data related to various risks in the organization (Lipton et al., 2018). The members of the board must make sure they receive credible and timely information from the senior management and senior risk officers. The information obtained from the senior management and senior risk officers will serve as a basis for the development of effective responses and action plans by the board of directors.

The specific committees charged with primary risk oversight must hold periodic sessions to meet with the top executives who are responsible for ensuring risk management in the organization. The members of the committees charged with primary risk oversight duties must also meet with independent members of the board of directors to discuss the risk culture in the organization, the risk oversight functions of the board, and the main risks faced by the organization. Moreover, the senior management and the senior risk managers in the company should understand that they are empowered to inform the board of directors or risk committee of escalated risks that require the urgent attention of the board outside regular reporting protocols and schedules (Lipton et al., 2018). The board of directors should also foster the report of red flags or yellow flags by the senior management and the senior risk managers to ensure the proper and prompt investigation of risks in the company.

5.2.3 Periodic Review of Legal Compliance Programs

The senior management and the senior risk managers must provide the board with an adequate review of the organization's legal compliance programs (Lipton et al., 2018). The aforementioned stakeholders must also explain how the legal compliance programs of the company are designed to address its risk profile, as well as identify and prevent the escalation of risks in the organization. The board of directors must also seek assurances from the senior management and the senior risk managers that the legal compliance programs are tailored to address the specific needs of the organization (Lipton et al., 2018). Certain principles must be followed to ensure the proper review of the legal compliance programs in the organization (Internet Security Alliance, 2020). These principles are centered on setting a strong tone at the top to ensure effective risk management. In this regard, the board of directors, senior management, and the senior risk managers must emphasize the organization's commitment to providing the full compliance of all employees with internal policies, legal requirements, and regulatory requirements (Lipton et al., 2018; Hess & Morton, 2020; Internet Security Alliance, 2020). The aforementioned cultural element should be the basis of periodic reviews of legal compliance programs.

The establishment of well-tailored legal compliance programs and organizational culture that prioritizes good ethical conduct are critical factors that the Department of Justice assesses under the Federal Sentencing Guidelines (Lipton et al., 2018). This assessment is often carried out if corporate personnel engages in any form of ethical misconduct in an organization.

However, the Deputy Attorney General has called for a review of the Federal Sentencing Guidelines of the Department of Justice to enhance enforcement guidance. Nonetheless, it is expected that individual accountability will still be the main feature of the enforcement guidance (Lipton et al., 2018). Therefore, the board of directors and the senior management must continue to carry out quick investigations and remediations of ethical misconduct in their company. The board of directors and the senior management of the organization should also make sure the legal compliance program is designed by individuals with the required expertise. The legal compliance programs should provide interactive training sessions and written materials to all employees to enhance their knowledge of the importance of ethical conduct in the organization.

There should be a periodic review of legal compliance policies to assess their efficacy and implement the required changes. The legal policies and procedures of the company should be practicable and align with existing business objectives and strategies. The board of directors and the senior management of a company must also implement measures to ensure consistency in the enforcement of legal policies through the implementation of appropriate disciplinary measures. Appropriate reporting systems should also be put in place at the board-, management-, and employee-level so that employees and the management know who to report suspected compliance violations to in the company. The establishment of such report systems will help the management to comprehend the informational needs of the board of directors and independent board committee members required to carry out the oversight of risks (Lipton et al., 2018). The organization may also decide to appoint a chief compliance officer and/or set up a compliance committee to administer the legal compliance program to internal stakeholders. The specific roles of the chief compliance officer and compliance committee will include the facilitation of employee education on legal compliance and the issuance of periodic reminders for legal compliance training and briefings (Lipton et al., 2018). The board of directors may choose to develop a separate compliance program to address specific areas of compliance that are quintessential to the performance of the organization.

5.2.4 Provision of Special Considerations to Cybersecurity Risks

The continuous reliance of companies on technological advancements that characterize every aspect of modern life and business has led to the rapid growth of cyber threats and cyber-attacks (Herjavec Group, 2017). The rise in the use of computing devices and their connection to the "Internet of Things" has also increased the exposure of various business functions across diverse sectors to cybersecurity risks. According to a report issued by Herjavec Group (2017), the cost of cybercrime may exceed $6 trillion by the end of 2021. This assumption is accurate as many large companies such as Colonial Pipeline and Software AG have experienced financial damage due to the occurrence of a security breach (Turton & Mehrotra, 2021; Waldman, 2021). Moreover, the successful hacking of computer networks owned by companies such as Colonial Pipeline, Software AG, Equifax, Twitter, Microsoft, and SEC highlights the negative implications associated with the rise in cyber-attacks (Lipton et al., 2018; Aria Cybersecurity Solutions, 2021; Waldman, 2021).

Some of the aftermaths of cyber-attacks suffered by renowned companies include network security breaches, data theft, online exposure of confidential information, significant damage to information technology infrastructure, and reputational damage to various companies (Lipton et al., 2018; Aria Cybersecurity Solutions, 2021; Waldman, 2021). In view of this, regulators and lawmakers in the United States and other parts of the world have channeled their focus to the prevention and mitigation of cybersecurity risks. For instance, in the United States, the enforcement and regulatory activities that pertain to cybersecurity has increased at the national and state level. Similarly, the European Union developed the General Data Protection Regulation, which guides the handling of data for various organizations (Lipton et al., 2018). The companies in the United States are mandated to comply with the requirements of the country and the European Union. Therefore, the board of directors in these companies must implement a comprehensive cybersecurity prevention and mitigation program. The members of the board must also allocate the resources required to purchase and deploy state-of-the-art defense technologies in the company (Aguilar, 2014; Lipton et al., 2018; Aria Cybersecurity Solutions, 2021). Furthermore, the board of directors and the senior management should develop core cybersecurity protocols such as the organization of training sessions for employees, patch installation, the installation of effective data and system testing systems, and the implementation of regular and effective cybersecurity incident response plans (Lipton et al., 2018). Most importantly, the members of the board must be actively involved in cyber-risk oversight.

The increase in the prominence of cyber-risks has also contributed to the decision of organizations to incorporate cyber-risks and cybersecurity within the internal audit functions of the company. A survey on the internal audit capabilities and needs carried out by Protiviti (2016) indicated that about 73% of the organizations surveyed had incorporated cybersecurity and cyber-risk within their internal audit functions. Protiviti (2016) also documented that there was a 53% increase in the number of companies that incorporated cybersecurity and cyber-risk within their internal audit functions. In this regard, the board of directors should seek assurances from the senior management that internal audit roles are carried out by personnel who have the required technical expertise, background, resources, and experience needed to address cyber-risks in the company. In addition, the members of the internal audit department should understand the importance of conducting periodic tests to evaluate the efficacy of the organization's risk mitigation and prevention strategies (Lipton et al., 2018; Internet Security Alliance, 2020). These stakeholders must also forward the report of the evaluation to the members of the internal audit committee of the board.

The members of the board should also evaluate their level of preparedness to prevent or mitigate the consequences of cybersecurity incidents. These stakeholders must also evaluate the effectiveness of the action plans developed to address the occurrence of a cyber breach. In view of this, the board of directors should consider the following actions documented in a publication written by Bonime-Blanc (2016):

1. Identification of the crown jewels of the organization. This action plan involves the identification of the mission-critical data and systems of the company, which are referred to as crown jewels. Subsequently, the board of directors must work with the senior management to employ appropriate cybersecurity measures that are outlined in the National Institute of Standards and Technology's framework (National Institute of Standards and Technology, 2020; Vigliarolo, 2021).

2. The board of directors must ensure that a practical cybersecurity incident response plan has been put in place by the senior management. The members of the board must also identify key personnel and designate roles such as the procedures for the containment and mitigation of cyber-attacks, protocols for the continuity of business operations, and the determination of required notifications that must be issued during the execution of a cyber-attack notification plan.
3. The members of the board should make sure the senior management has developed effective response services and technologies to prevent or mitigate the consequences of cybersecurity incidents. Some of these services and technologies may include intrusion detection technology, off-site data backup mechanisms, data theft prevention technology.
4. The members of the board should make sure the authorizations required to allow the monitoring of the organization's networks and systems have been put in place.
5. The board of directors should ensure that the legal counsel of the organization is conversant with the use of technology systems and has a good knowledge of ways to effectively manage cybersecurity incidents. This approach will decrease the response time needed to mitigate the negative impacts of cybersecurity incidents.
6. The board of directors must establish relationships with agencies and organizations that share information on cybersecurity incidents. In addition, the members of the board must actively engage with law enforcement officials prior to the occurrence of a cybersecurity incident.

5.2.5 Provision of Special Considerations to Address Environmental, Social, and Governance Risks

Environmental, social, and governance risks are a general subset of risks that an organization must manage (Lipton et al., 2018). Companies manage environmental, social, and governance risks through the identification and mitigation of risks that pose significant threats to specific areas of the company. Some of these risks are labor standards, environmental liabilities, the safety of consumers, succession of leadership, product safety, and contingency plans for macro-level risks. The contingency plans are often centered on the determination of energy and supply chain alternatives and the development of backup recovery plans for natural disaster scenarios like climate change. Even though the board of directors has taken certain measures to oversee the management of material risks, the increase in the scrutiny of the public and large institutional investors about environmental, social, and governance risks has increased the attention of shareholders to ensure that their board of directors has implemented reliable measures to evaluate, disclose, and manage these risks (Lipton et al., 2018). The ability of an organization to manage environmental, social, and governance risks depends on the leadership and good governance of the board of directors (Lipton et al., 2018). In view of this, shareholders are demanding that the members of the board must exercise the leadership needed to address widespread issues that are related to environmental, social, and governance risks.

Many stakeholders have advocated the effective oversight of environmental, social, and governance risks by the members of the board. In view of this, a series of reports and frameworks have been issued to the board of directors regarding the management of environmental, social, and governance risks (Ernst and Young Center for Board Matters, 2018; Lipton et al., 2018). These reports and frameworks serve as a guide that will enable the members of the board to incorporate matters related to environmental, social, and governance risks into the corporate strategy and business objectives of the corporation (Ernst and Young Center for Board Matters, 2018; Lipton et al., 2018). A proxy season review conducted by the Ernst and Young Center for Board Matters (2018) showed that the most prevalent topic proposed by shareholders was related to environmental, social, and governance risks. In some instances, the shareholders' proposals were supported by key institutional investors (Ernst and Young Center for Board Matters, 2018). The Ernst and Young Center for Board Matters (2018) reported that about 79% of investors in the surveyed companies believe that climate change is an essential risk factor, while 61% of the investors emphasized that the utmost priority of companies should be centered on the provision of reliable reports on various risks. Similarly, the Institutional Shareholder Services (ISS) stressed that the proper management of environmental, social, and governance risks is a major requirement under which it will issue recommendations to vote in favor of the proposal of shareholders (Ernst and Young Center for Board Matters, 2018).Therefore, the board of directors and senior management must conduct regular assessments of the risk appetite and risk tolerance threshold of the company towards environmental, social, and governance risks (Lipton et al., 2018).

Public's view on the role of companies in the prevention and mitigation of environmental, social, and governance risks has continued to evolve in recent years (Lipton et al., 2018). In this regard, the board of directors is admonished to consider how their risk oversight responsibilities apply to environmental, social, and governance risks. The role of the members of the board in overseeing the management of environmental, social, and governance risks such as energy sources, disruption of supply chain networks, environmental impacts of business operations, and labor practices involves the application of general risk oversight practices in the company. However, the rise in the scrutiny of the public and investors on how companies address environmental, social, and governance risks has necessitated the development of risk oversight practices that are tailored to address environmental, social, and governance risk-related issues (Lipton et al., 2018). The board of directors should also collaborate with the senior management to identify environmental, social, and governance issues that are crucial to the success of their company and the well-being of their consumers. These stakeholders must also decide on relevant and appropriate procedures and policies that must be implemented to ensure the regular and effective assessment, monitoring, and management of environmental, social, and governance risks.

The board of directors should foster the external reporting of the organization's approach, response plan, and progress made in addressing environmental, social, and governance risks (Lipton et al., 2018). The members of the board and the senior management should also engage with institutional investors and other shareholders to share knowledge and increase their awareness of key environmental, social, and governance issues in the organization. In specific circumstances, the board of directors may consider obtaining frequent briefings on relevant environmental, social, and governance issues and the approach implemented by the management to address these matters.

On the whole, the creation of more focused independent committees such as the corporate responsibility committee and sustainability committee is the most reliable way to effectively address environmental, social, and governance issues in the company (Lipton et al., 2018). Such committees will be given specific tasks that pertain to the oversight of certain environmental, social, and governance issues in the company. The members of such committees will also be tasked with the specific roles of reviewing and updating existing committee charters and board-level guidelines on corporate governance to address environmental, social, and governance issues (Lipton et al., 2018). Most importantly, the board of directors must make sure the committees tasked with the aforementioned duties collaborate with other committees such as the audit committee to ensure the effective management of environmental, social, and governance risks in the company.

5.2.6 Anticipation of Potential Risks

The risk management structure in an organization should encompass the efforts taken by the board of directors, senior management, senior risk officer, and other stakeholders to analyze and assess the areas in the company that are more likely to be exposed to future risks (Lipton et al., 2018). The risk management structure must also assess how the interrelationships of existing risks in the company may be altered and how the procedures for the anticipation of future risks are established. Future risks may be inherent in the strategic plans of the company or may arise from the competitive landscape of the organization. The high likelihood of technological advancements and other developments may also pose risks to long-term value creation, as well as the profitability and sustainability of an organization. The aforementioned phenomenon explains why the anticipation of potential risks is a critical element of preventing or mitigating such risks before they escalate into major crises in the organization. Therefore, the board of directors must ask the senior management and senior risk officers to discuss and compile a detailed report of possible sources of future risks that may materialize in different areas of the organization (Lipton et al., 2018). These stakeholders must also proffer effective solutions to address potential vulnerabilities that are significant to the successful performance of the company.

Appendix: Questions the Board Should be Asking the C-Suite/CISO on Cyber Resiliency

Despite huge investments in the implementation of defense systems to prevent and mitigate cyber-attacks, cybercriminals have continued to develop and use sophisticated methods and tools to breach these cybersecurity barriers and systems (Seema et al., 2018; Kalakuntla et al., 2019; Downs, 2020; BBC News, 2021). Although some companies have enhanced their capabilities to prevent and mitigate cyber-attacks, few of these have the strong cybersecurity foundation required to address cybersecurity incidents. Moreover, most of these organizations are not prepared to deal with the increase in the emergence of cyber threats from sophisticated attackers arising from the rising dependence of institutions on digital capabilities. According to Accenture (n.d.), organizations must develop and implement a robust cybersecurity approach to harness the diverse benefits of digital capabilities and ensure cyber resiliency. Therefore, the utmost priority of the board and top management of the company should be the creation of an organizational culture that is centered on ensuring the cybersecurity of the company. In this regard, companies must hasten the development of the new capabilities required to thrive in this new era of digital dependency. The board of directors of companies must also implement the leadership and governance needed to maximize the advantage of digital capabilities while ensuring cyber resiliency (Accenture, n.d.). Furthermore, the top management in the company needs to select a set of metrics to evaluate the efficacy of cybersecurity measures in comparison with the strategy and objectives of the business. The funds required to carry out cybersecurity activities should also be allocated by the organization to ensure the appropriate delivery of prompt cybersecurity measures.

Most importantly, the board should ask the C-Suite/CISO specific questions on cyber resiliency. According to Accenture (n.d.), the responses of the C-Suite/CISO to these questions are quintessential to engendering positive and sustainable improvement in leadership and governance, organizational culture, allocation of resources, as well as the measurement and monitoring of the efficacy of cybersecurity in the organization (Accenture, n.d.). For instance, in most companies, the chief information security officer is not allowed to report directly to the board of directors. The chief information security officer reports to the chief information officer, while the chief information officer conveys the information to the board of directors. However, the aforementioned strategy is a significant drawback to enhancing the cyber resilience of an organization. The specific roles of each stakeholder should be made clear by the management.

The chief information security officer is expected to report directly to the board of directors and ensure that the board is informed about the cybersecurity status of the company. In contrast, the role of the chief information officer is to head and lead the infrastructure teams. In addition, the chief information security officer should establish a matrix reporting structure that enhances direct communication with the chief risk officer (CRO), chief operating officer (COO), chief executive officer (CEO), and the board of directors. If possible, the chief information security officer should be invited regularly to attend risk or cybersecurity committee meetings.

Moreover, the chief information security officer should be actively involved in the planning process within the C-Suite, and the review of the plans with the board of directors. In view of this, it is quintessential for the board of directors to ask their chief information officer, chief information security officer, and chief executive officer the right questions about their strategies to improve leadership and governance, enhance the cyber-risk culture of the organization, ensure the proper allocation of internal and external cyber resources, as well as to measure and monitor the effectiveness of cybersecurity measures. Some of the questions that may be asked by the board of directors to evaluate the understanding of their chief information officer, chief information security officer, and chief executive officer about the internal and external cyber threat landscape are listed in the next subsection (Harvard Business Review, 2021). The expected response of the senior management to each question is also discussed in the following subsections.

What Trends in Digital Technology Do You Anticipate Impacting the Future of Data Protection and Information Security for the Company? Do You Think the Organization is Prepared for Them?

The chief information officer, chief information security officer, and the chief executive officer must understand that recent trends in digital technology may impact the future of data protection and information security for the company. For instance, the top management must be aware that the recent trends in the advancement of digital technology contribute to the emergence of sophisticated techniques like ransomware attacks employed by cybercriminals to successfully launch cyber-attacks. Ransomware attacks plague companies with data theft and huge financial damage due to the costs of mitigating cyber-attacks (Panda Security, 2021).

Moreover, the management must be aware that the recent trends in digital technology have contributed to an increase in the occurrence of extortion attacks, where cybercriminals steal an organization's data and encrypt it so that they can gain unauthorized access to its confidential information. Later, the cybercriminals use this confidential information to blackmail the company by threatening to release its confidential information unless a ransom is paid within a particular deadline (Downs, 2020; BBC News, 2021; Panda Security, 2021). The senior management must understand the burden of this cyber threat to the company.

Even though most of the information technology departments in companies rely on Virtual Private Networks (VPNs) to access their network, this cybersecurity measure is inadequate in ensuring the protection of sensitive data (Panda Security, 2021). The management must realize that the most common entry vector to launch ransomware attacks is phishing and must develop strategies to prevent such cyber-attacks. Most importantly, the chief information officer, the chief information security officer, and the chief executive officer must establish and implement prompt response plans to mitigate the occurrence of ransomware attacks. These stakeholders must also be prepared to transition the business activities of the company from VPNs to Zero-Trust Network Access (ZTNA) (Panda Security, 2021). ZTNA is considered a more secure alternative for regulating and strengthening remote access to confidential information and minimizing the occurrence of ransomware attacks.

The chief information officer, the chief information security officer, and the chief executive officer must ensure that the company is prepared to bolster its cybersecurity to meet the demands of the continuous advancements in digital technology. In view of this, the top management must find and employ well-trained cybersecurity professionals and information security experts to help enhance the security of their systems and networks (Panda Security, 2021). The senior management must also focus on increasing the awareness of their employees on how to detect cyber-attacks. The management can also organize company-wide training programs to help the board and other concerned stakeholders address cybersecurity issues. The board of directors must ensure that the top management holds such training programs regularly (Panda Security, 2021). The members of the board must also seek assurances from the top management that the efficacy of each training session is evaluated by subjecting employees to various assessments. In addition, the top management must also make sure that their organization approaches the development and implementation of security strategies with a sense of urgency (Panda Security, 2021). This approach will help the company to minimize cyber-risks and vulnerabilities that may compromise the security of the company's assets. As the trends in digital technology continue to evolve, the top management must collaborate with the board of directors and members of the independent board committee to seek out effective and appropriate ways to secure their confidential data and defend corporate networks from increasingly complex ransomware attacks and other cyber-risks.

Which Corporate Cyber-Risks Could Most Significantly Impact the Growth of the Organization? How Will You Address Them?

Different corporate cyber-risks may pose significant threats to the growth and business continuity of an organization. The first corporate cyber-risk is the failure of the top management to cover the basics of cybersecurity (Bianculli, 2021). Most often, organizations rely on the implementation of a single layer of security or antivirus to prevent hackers from gaining unauthorized access to the organization's network or systems. However, such measures contribute to the vulnerabilities in an organization's infrastructure. The failure of an organization to implement basic cybersecurity measures enables cybercriminals to exploit the vulnerabilities in its infrastructure. According to Bianculli (2021), cybercriminals can exploit less than a dozen vulnerabilities to gain unauthorized access to a company's corporate network or systems. In view of this, the chief information officer, the chief information security officer, and the chief executive officer must develop and implement fundamental security measures such as timely patching and data encryption to strengthen the defenses of the company against cyber-attacks launched by cybercriminals.

The lack of understanding about the sources of corporate cyber-risks also poses a significant threat to the growth of a company. Most organizations fail to comprehend that they are vulnerable to cyber-attacks. Moreover, some companies are not aware of the value of their critical assets and the sophistication or profile of potential cyber-attackers (Bianculli, 2021). The chief information officer, the chief information security officer, and the chief executive officer must know that corporate cyber-risks are not easily detected in an organization. Therefore, the top management should develop and implement an appropriate plan to identify and mitigate these corporate cyber-risks in the long term (Bianculli, 2021).

Most often, technology is considered the main source of corporate cyber-risks. However, sociological and psychological factors in the organization may also be sources of corporate cyber-risks in the company (Bianculli, 2021). In view of this, the top management must be aware that the organizational culture in a company plays an integral role in how the organization perceives or addresses cybersecurity. The senior management must also know that organizational culture in a company also influences the role of stakeholders in the prevention and mitigation of cyber-attacks (Bianculli, 2021). Therefore, the prevention and action plans developed by the chief information officer, the chief information security officer, and the chief executive officer should foster the development of an organizational culture that promotes the detection of cyber-risks or threats and enhances the company's defenses against cyber-attacks.

The lack of cybersecurity policies in organizations is another corporate cyber-risk that impacts the business continuity and growth of an organization (Bianculli, 2021). According to Bianculli (2021), companies in the technology and finance sectors are not the only firms that are at risk of suffering from a cyber-attack. Cybercriminals are targeting every single organization across the globe (Downs, 2020; BBC News, 2021;

Bianculli, 2021; Panda Security, 2021). Even though the rise in the frequency of high-profile data breaches has increased the awareness of the C-suite in some organizations, the knowledge of this trend is not enough to prevent or mitigate the aftermath of an internal or external cyber-attack. Therefore, the chief information officer, the chief information security officer, and the chief executive officer must establish cybersecurity standards that will reduce their exposure to cybercriminals. The C-suite must prioritize the development of a cybersecurity policy and ensure that employees adhere to the stipulations in the policy. Furthermore, organizations should solicit the expertise of both internal and external cybersecurity professionals to strengthen their defenses against cyber-attackers and ensure data privacy (Bianculli, 2021). The cybersecurity policy of a company should foster the identification of corporate cyber-risks related to the cybersecurity of the organization, establishment of cybersecurity governance, protection of the information, system, and network of the company, development of procedures and oversight protocols to prevent and mitigate cyber-risks, and the detection of unauthorized activity (Bianculli, 2021). In addition, the cybersecurity policy should help the board of directors, committee members, and the C-suite to identify and handle the cyber-risks associated with funds transfer requests, the provision of remote access to users' information, and the outsourcing of business operations to third-party providers and their vendors (Bianculli, 2021).

The inability of stakeholders to distinguish between a compliance policy and a cybersecurity policy may impact the growth of an organization (Bianculli, 2021). Some stakeholders assume that ensuring compliance with the rules and regulations of an organization that does not incorporate a clear focus on cybersecurity is equivalent to protecting the organization from cyber-attacks. According to Bianculli (2021), the efficacy of enterprise risk management depends on the access of an organization to various parts of the security system. In view of this, cybersecurity is considered a company-wide responsibility rather than the obligation of the personnel in the IT department. Therefore, the board of directors, committee members, senior management, and other employees in the organization are responsible for overseeing how information flows through the corporate network and systems. The management and other employees in the organization must also have the knowledge required to detect cyber-risks and protect against the leakage of sensitive data to cybercriminals. Most importantly, the C-suite must be adequately prepared to prevent or mitigate the aftermath of a cyber-attack.

Recommended approaches to enhance the preparedness of the C-suite includes the development and implementation of a cyber-incident prevention and response plan, the dedication of the required personnel to detect the cyber event, analyze the incident, prevent further damage as a result of the cyber-attack, and the allocation of adequate resources towards the development and implementation of a well-constructed response plan (Rogers & Ashford, 2015; Bailey et al., 2020).

The human factor plays an essential role in the strengthening of an organization's information security defenses (Bianculli, 2021). The individuals who occupy high positions in a company (e.g., C-suite), are less likely to become malicious insiders. However, low-level employees in a company may weaken the security defenses of an organization. According to Bianculli (2021), privilege abuse is a leading cause of cyber breaches and data exposure by malicious insiders. Hence, the C-suite must be mindful of how they set and monitor the access levels of low-level employees in the company. Moreover, the development and implementation of a cybersecurity policy will ensure the protection of sensitive data from these malicious insiders and mitigate potential cyber-risks to the growth of the organization.

The implementation of the bring your own device policy is another corporate cyber-risk that threatens the protection of the confidential information of a company. Although this policy was implemented to provide employees with a flexible work environment and improved working conditions, this policy brings corporate cybersecurity risks to the company. According to Bianculli (2021), one in five companies that adopted the bring your own device policy has suffered from a mobile security breach driven by malicious Wi-Fi and malware. Bianculli (2021) also documented that the cybersecurity threats to the bring your own device policy imposes significant burdens on the company's IT resources and help desk workloads. Despite rising threats to mobile security and cybersecurity breaches, it is estimated that only 30% of companies have increased their cybersecurity budgets to address the risks associated with the adoption of the bring your own device policy. Furthermore, 37% of organizations that adopted the bring your own device policy do not have plans to increase their cybersecurity budget. In view of this, the C-suite must increase the awareness of the board of directors, committee members, and other employees in the organization about the risks associated with the adoption of the bring your own device policy (Bianculli, 2021). Moreover, the chief information officer, the chief information security officer, and the chief executive officer should ensure password protection, restrict the access levels of low-level employees, and monitor the activities of low-level employees on the corporate network.

The lack of funds, talents, and resources required to incorporate specific cybersecurity measures is another risk that could also expose an organization to different cyber-risks (Bianculli, 2021). Organizations with a tight budget and scarce resources are more likely to incur corporate cyber-risks. This is because such organizations are less likely to allocate the funds required to enhance the layers of security in their company and mitigate the negative aftermaths of cyber-attacks. The C-suite should set logical expectations towards the achievement of cybersecurity objectives and ensure the allocation of affordable resources to achieve such objectives. However, it may be difficult for the members of the board and the management to achieve cybersecurity goals without the required number of cybersecurity experts or funds needed to employ full-time personnel who are dedicated to preventing, detecting, and mitigating cyber-risks (Bianculli, 2021).

The lack of training on information security is another corporate risk that can impact the growth of an organization. According to Bianculli (2021), increasing the awareness of employees about cybersecurity through employee training is critical to ensuring the safety of an organization and protecting it from unexpected cyber-attacks. The priority of the C-suite should be to organize regular training sessions on information security for employees. The chief information officer, the chief information security officer, and the chief executive officer must also investigate and compile a list of the most common file types that cybercriminals used to gain unauthorized access to a company's system (Bianculli, 2021). The outcome of this investigation will help the management and the board to determine the cybersecurity measures that will be incorporated into training on cybersecurity.

The chief information officer, the chief information security officer, and the chief executive officer must understand the importance of developing an effective response plan (Bianculli, 2021). The lack of an effective cybersecurity incident response plan is a major risk to any company. Therefore, these stakeholders must be prepared to mitigate the negative aftermaths of potential cyber-attacks. The cybersecurity incident response plan should include measures to prevent cyber-attacks and strategies to reduce the occurrence of a cyber-attack.

Unfortunately, most organizations are not well-prepared to mitigate the negative aftermaths of potential cyber-attacks (Bianculli, 2021). According to the NTT Group (2016), there has been a rise in the number of companies that are not prepared to deal with the aftermath of a potential cyber-attack.

The report further indicated that about 77% of companies do not have a formal cybersecurity incident response plan, while 23% of organizations have established a formal cybersecurity incident response plan (NTT Group, 2016). The C-suite of organizations that do not have a cybersecurity incident response plan may consider allocating resources towards the prevention of cyber-attacks. This strategy will enable organizations to detect the occurrence of a cyber-attack in its early stages. Moreover, the strategy will help the C-suite manage cyber threats effectively. However, the C-suite must understand that the aforementioned strategies do not eliminate the need to develop and implement a cybersecurity incident response plan. The management must also emphasize to the board that it is preferable to implement a cybersecurity incident response plan to reduce the negative impacts of cyber-attacks and ensure the business continuity of the organization (Bianculli, 2021).

The presence of polymorphic and stealth malware is a major risk to the business continuity of an organization (Bianculli, 2021). Polymorphic malware is destructive or intrusive software that is designed to cause harm to a user's computer system. Common examples of polymorphic malware are worm, virus, and Trojan. It is often difficult to detect malware programs because the software changes constantly. Therefore, the C-suite should understand that the organization may require an additional layer of security in addition to the use of antivirus or anti-malware programs.

The chief information officer, the chief information security officer, and the chief executive officer must ensure that the company's first line of defense is a technological solution that can proactively identify the presence of polymorphic malware programs on a computer system (Bianculli, 2021). The anti-malware programs selected by the C-suite should be designed to prohibit access to malicious servers and prevent data loss. The chief information officer, the chief information security officer, and the chief executive officer should also devise effective strategies such as the timely patching of vulnerabilities to keep the computer systems of the organization protected from cyber-attacks (Bianculli, 2021). As the emergence of corporate cyber-risks and cyber-attacks continue to increase, the C-suite must also develop extreme measures to prevent and mitigate the aftermath of such cybersecurity incidents. Some of these measures include the disconnection of specific computer systems from the Internet and the shutdown of network segments that are at risk of being compromised by cyber-attackers (Bianculli, 2021).

In addition, the chief information officer, the chief information security officer, and the chief executive officer should consider the high level of sophisticated tools used by cybercriminals to launch cyber-attacks before implementing cybersecurity measures. For instance, the C-suite of the company may recommend the automation of certain steps in the business operations to prevent or mitigate cyber-attacks launched using automated systems. Moreover, the automation of business operations will enable the chief information officer, the chief information security officer, and the chief executive officer to address a high volume of cyber threats. The C-suite of the organization should select a cybersecurity solution that scans both outgoing and incoming Internet traffic to detect cyber threats. The cybersecurity solution should also be designed to prevent the infiltration of the company's computer system by cybercriminals (Bianculli, 2021).

On the whole, the board of directors expects the chief information officer, the chief information security officer, and the chief executive officer to identify the aforementioned vulnerabilities in the infrastructure of the organization that can endanger its future growth or current financial situation. The top management must then explore potential solutions to the cybersecurity issues of the organization (Bianculli, 2021). According to Bianculli (2021), the acknowledgment of the existence of cyber-risks that exposes the company to cyber-attacks and the integration of cybersecurity measures is quintessential to ensuring business continuity and the protection of the company's assets. Therefore, the main objective of the chief information officer, the chief information security officer, and the chief executive officer should be the integration of cybersecurity measures into each step of business operations of the organization. The top management must also develop an effective prevention and response plan that will enhance information security and protect the company from cyber-attacks. In addition, the top management should establish a business continuity plan that will enable the organization to handle the aftermath of a potential cybersecurity breach.

What Cyber Metrics and Key Performance Indicators (KPIs) Are You Using to Evaluate the Exposure of the Company to Insider Threats, Loss of Sensitive Information, and Data Theft?

The C-suite of an organization must select appropriate cyber metrics and key performance indicators (KPIs) to evaluate the exposure of the company to insider threats, loss of sensitive information, and data theft efficiently

(Bianculli, 2021). If the chief information officer, the chief information security officer, and the chief executive officer cannot measure the efficacy of cybersecurity measures, these stakeholders will not be able to monitor the impact of these measures in the prevention and mitigation of cyber-attacks. Considering the constant evolution of cyber threats and the rapid development of the technology required to prevent these threats, the C-suite of the company must implement evaluation procedures that will facilitate the effective evaluation of cybersecurity measures. However, the effective evaluation of cybersecurity measures can only be carried out when appropriate cyber metrics and KPIs have been selected by the senior management.

The importance of selecting appropriate cyber metrics and KPIs cannot be overemphasized. According to Bianculli (2021), the analysis of key risk indicators and KPIs gives the C-suite of the organization an overview of how the members of the security team are functioning over a specific period. Cyber metrics give the senior management quantitative information that can be used to show board members the impacts of the actions taken by the chief information officer, the chief information security officer, and the chief executive officer to ensure the integrity and protection of confidential information, as well as the assets of the company. Furthermore, the analysis of KPIs and cyber metrics will enable the chief information officer, the chief information security officer, and the chief executive officer to know which cybersecurity measures are effective or ineffective (Bianculli, 2021). The outcome of the analysis will then be put into consideration when making decisions about the selection of cybersecurity measures for future projects.

The provision of reports using cybersecurity metrics is an important part of the role of the chief information officers, the chief information security officers, and the chief executive officers that are driven by the rising interests of shareholders, regulators, and the board of directors (Tunggal, 2021a). Many members of the board in the financial sector have regulatory and fiduciary duties to manage cyber-risks and ensure the protection of personally identifiable information. The role of the C-suite is driven by new regulations such as the Gramm-Leach-Bliley Act, Personal Information Protection and Electronic Documents Act (PIPEDA), Prudential Standard CPS 234, and New York Department of Financial Services (NYDFS) Cybersecurity Regulation (Tunggal, 2021). Moreover, the implementation of extraterritorial data protection laws such as the European Union General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and Brazil's law of general data protection (LGPD), and security management has increased the focus of the C-suite in every organization to the importance of analyzing cybersecurity metrics and KPIs. In view of this, cybersecurity experts use cyber metrics to document reports about cybersecurity to non-technical colleagues in the organization. Some examples of cyber metrics that the C-suite of an organization tracks and presents to stakeholders include the following:

1. The monitoring of unidentified devices on internal networks. Employees may expose an organization to malware and other cyber-risks whenever they bring their devices to the work environment. Moreover, the poor configuration of Internet of Things (IoT) devices may compromise the cybersecurity of an organization. In view of this, the C-suite must incorporate network intrusion detection systems in the cybersecurity measures of the organization (Tunggal, 2021).
2. Degree of preparedness. The C-suite of the organization must make sure that the devices of employees on the corporate network are fully patched. The senior management must also ensure that vulnerability management and vulnerability scans are part of the chief information security controls implemented to minimize the risk of vulnerability exploits by cybercriminals (Tunggal, 2021).
3. The number of intrusion attempts. The C-suite must keep track of the number of times cyber-attackers have gained unauthorized access to systems or networks in the organization. The senior management may use firewall logs as a source of references to gather sufficient evidence (Tunggal, 2021).
4. The number of cybersecurity incidents. The C-suite should keep track of the number of times a cyber-attacker has breached the networks or compromised the information assets of the organization (Tunggal, 2021).
5. The mean time to detect cybersecurity incidents. This metric measures the time taken for the cybersecurity team to notice the indicators of compromised corporate assets and other cybersecurity threats. Therefore, the senior management should take note of how long cybersecurity threats go unnoticed by the cybersecurity team in the organization (Tunggal, 2021).
6. The mean time to resolve cybersecurity incidents. This metric measures the quality of the cybersecurity incidence response plan implemented in the organization. Therefore, the C-suite should keep track of the mean response time for the cybersecurity team in the organization to respond to a cyber-attack once they detect it. (Tunggal, 2021).

7. The mean time to contain cybersecurity incidents. This metric determines how long it takes the security team to identify attack vectors across different endpoints in the organization. The C-suite can use this metric to monitor the time it takes the security team of the company to contain cybersecurity incidents (Tunggal, 2021).
8. First-party cybersecurity ratings. The measurement of this metric enables the C-suite to convey information about cyber metrics to colleagues who do not specialize in information technology. The first-party cybersecurity ratings are scores that can be easily understood by all employees in the organization. In this regard, the C-suite should include first-party cybersecurity ratings in reports prepared for the board of directors and shareholders. These ratings should also be used to communicate with colleagues during briefings on cybersecurity-related issues. Furthermore, the C-suite should incorporate first-party cybersecurity ratings into the existing cybersecurity risk assessment procedure. A letter-grade may be used to assess the cybersecurity status of an organization in real-time using criteria such as phishing risk, email spoofing, network security, Domain Name System Security Extensions (DNSSEC), Domain-based Message Authentication, Reporting, and Conformance (DMARC), social engineering risks, data leaks, vulnerabilities, and risk of man-in-the-middle cyber-attacks. This strategy will help the C-suite to identify which cyber metrics require additional attention (Tunggal, 2021).
9. Average vendor cybersecurity rating. This cyber metric helps the chief information officer, chief information security officer, and chief executive officer to monitor the cyber threat landscape beyond the borders of the organization. The continuous monitoring of third-party and fourth-party risks can help the senior management to reduce vendor risks and enhance vendor management (Tunggal, 2021).
10. Patching cadence. This cyber metric measures how long it takes the cybersecurity team of an organization to implement application cybersecurity patches or address high-risk vulnerabilities and exposures. Most often, cyber-attackers employ sophisticated tools to exploit the lag between patch release and implementation. For instance, the successful spread of ransomware called WannaCry was due to the cybercriminal's ability to exploit a zero-day vulnerability referred to as EternalBlue. Even though the vulnerability exploited by the ransomware was patched quickly by cybersecurity experts, many companies were victims of the attack due to inadequate patching cadence (Tunggal, 2021).

11. Access management. The C-suite must keep track of the number of users who have administrative privileges. The chief information officer, the chief information security officer, and the chief executive officer must also explore cost-effective ways to reduce privilege escalation attacks in the organization (Tunggal, 2021). According to Tunggal (2021), the C-suite can ensure access management by restricting access to lower-level employees and developing effective access control principles for all users in the organization.
12. A comparison of peer performance with organizational performance. This cyber metric is currently used by the senior management in various companies to report information about cybersecurity to the board of directors. The comparison of peer performance with organizational performance is highly compelling and visually appealing to members of the board. In addition, this metric is considered the preferable choice for board presentations because it is easily understood by all stakeholders. The C-suite should consider drafting executive summary reports at regular intervals to easily benchmark the cybersecurity performance of the company against key industry peer performances within a specific duration (Tunggal, 2021).
13. Vendor patching cadence. This cyber metric enables the C-suite of an organization to determine the number of cyber-risks their third-party vendors are exposed to. Vendor patching cadence also helps the chief information officer, the chief information security officer, and the chief executive officer to determine the number of critical vulnerabilities in the organization that is yet to be remediated.
14. Mean time required for vendors' cybersecurity incident response. This cyber metric measures the mean time taken by the cybersecurity team of an organization's vendors to respond to a cybersecurity incident. This cybersecurity incident may be intrusion attempts by cybercriminals or a cyber-attack. Intrusion attempts are indicators that enable the C-suite to determine if the organization is a potential target. The longer the mean time required for vendors to respond to cybersecurity incidents, the higher the likelihood that the organization will suffer from a third-party cyber breach or data leak (Tunggal, 2021). According to Tunggal (2021), the primary cause of data breaches is poor vendor management. Therefore, the chief information officer, the chief information security officer, and the chief executive officer should develop regulations and policies that will enhance third-party and fourth-party risk management in the organization. Some of these regulations and policies have already been discussed in this handbook.

The C-suite of an organization must ensure that they choose the right cyber metrics, KPIs, and key risk indicators (Tunggal, 2021). The selection of appropriate cyber metrics, KPIs, and key risk indicators depends on the following: type of industry, needs of the organization, cybersecurity regulations, guidelines, and best practices, as well as the risk appetite of the company and its clients/customers. Most importantly, the chief information officer, the chief information security officer, and the chief executive officer must select cybersecurity metrics that are easily digestible by both technical and non-technical stakeholders. If all stakeholders do not understand the cybersecurity metrics selected by the C-suite, the senior management must consider choosing other cyber metrics or develop effective ways to explain the metrics to them. The senior management may consider the use of industry comparisons and benchmarks to help both technical and non-technical stakeholders to understand complex cyber metrics, KPIs, and key risk indicators (Tunggal, 2021).

The C-suite of the organization must also understand that the most critical cyber metric is cost (Tunggal, 2021). Therefore, the chief information officer, the chief information security officer, and the chief executive officer should focus on presenting the board of directors and members of the executive team with concise information about how cybersecurity measures have contributed to an increase in revenue or cost savings in the organization. The C-suite must provide compelling evidence to the board of directors and members of the executive team on the efficacy of the cybersecurity measures implemented in the company (Tunggal, 2021). In addition, the chief information officer, the chief information security officer, and the chief executive officer should develop cost-effective critical security controls to enhance the cybersecurity of the organization.

How Are You Re-assessing the Insider Risks in the Organization as it Pertains to Recent or Upcoming Changes to the Workforce?

The chief information officer, the chief information security officer, and the chief executive officer must be aware of the possibility of insider risks in the organization due to upcoming changes in the workforce (Panda Security, 2021). For instance, some organizations allow full-time or a hybrid model of remote work. Such organizations employ remote-only workers who reside in different geographical locations across the globe. Most of these employees are hired without carrying out face-to-face interviews. Companies that hire such employees are exposed to the risks of insider threats. Therefore, the chief information officer, the chief information security officer, and the chief executive officer must give additional consideration to the reality of insider threats, as well as the possibility of data loss and theft by employees.

The board of directors and the top management must also be conversant with the fact that most threat actors have sophisticated methods and tools to infiltrate corporate networks and compromise confidential data (Panda Security, 2021). According to Panda Security (2021), about 15–25% of cybersecurity breach incidents are caused by trusted business vendors.

Therefore, the aforementioned stakeholders must not ignore the possibility and increasing sophistication of threat actors within their organization. The top management must take insider threats seriously and consider such threats a real cyber-risk. In order to minimize the risks posed by insider threats, the top management must have the appropriate tools and systems to detect these threats.

What is the Process for When a Large-Scale Insider Risk Incident Takes Place?

Best Practice 1. The first step to take when a large-scale insider risk incident occurs is to carry out enterprise monitoring (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). This step involves the identification of corporate assets that are at risk of being compromised and the determination of all contents within the organization's network that represents a cyber-risk. The efficacy of insider cyber threat management depends on the C-suite's ability to locate, identify, and classify corporate assets. The implementation of continuous monitoring plans by the senior management to keep track of insider behavior and other related cyber-risks also contributes to the effectiveness of insider risk management in an organization. Therefore, the C-suite must reach out to important stakeholders in the company and organize meetings to discuss and prioritize the critical areas of concern in the organization (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). The C-suite may develop a simple scoring system using letters A–F, numbers 1–10, or high, medium, and low to prioritize the critical areas of concern in the company.

The focus of the C-suite should be centered on corporate assets that receive the highest priority of stakeholders or sensitive information that may be costly to the company if compromised (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). Such confidential data may include all files and data that comprise customer or personal information, intellectual property, or other sensitive information. The C-suite in various organizations may define corporate assets and cybersecurity incidents differently, depending on the sector or focal point of the company. Once the chief information officer, the chief information security officer, and the chief executive officer have identified and prioritized the company's critical assets, this confidential information must be fingerprinted and inventoried to ensure that it is neither copied to flash drives or any other form of mobile storage nor sent out through instant messaging or e-mail (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). Some examples of assets that are exposed to cyber-risks by the vertical market in various sectors include the following (Cybersecurity and Infrastructure Security Agency, 2020):

1. Banking industries and credit companies. Account skimming, personal and financial information theft, and the diversion of funds.
2. Financial institutions. Acquisition and merger plans, private investigation data, and non-public financial information.
3. Retail companies. Pricing information, credit card verification on cards, and the personal data on credit holders.
4. The government. Personal and classified information and national secrets.
5. Public organizations. Private information on earnings that have not been released to the market, intellectual property, and information on new products.

The chief information officer, the chief information security officer, and the chief executive officer must understand that cybersecurity risks cannot be evaded through the implementation of data-leak prevention strategies that are designed to detect a vector of communication such as email. In this regard, the C-suite must search for more recent and sophisticated solutions that can enhance the monitoring and detection of actions by malicious insiders.

Best Practice 2. The C-suite must anticipate and think through the investigation outcome of the large-scale insider risk cybersecurity incident (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). This step involves the senior management identifying the corporate assets that are at risk and overlaying the types of cybersecurity incidents they anticipate to address based on the nature of the critical assets. The process of thinking through and articulating possible cybersecurity incidents will help the C-suite to create effective policies, eliminate false positives, and retrieve relevant data about the incident. This data can be used by the chief information officer, the chief information security officer, and the chief executive officer to reconstruct the timeline of the incident, monitor correlated events, and determine the notifications and triggers that should be incorporated into investigation policies (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

The C-suite must also carry out typical customer data-loss investigations on the malicious leak of the data of customers by vengeful insiders, the intentional theft of customer lists for lucrative purposes by employees, and stolen or misplaced laptops with the data of customers (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). Although the loss of customer data is sometimes due to accidents like the loss of a CEO or junior salesperson's laptop that contains several customer records, some cases of data loss are caused by the deliberate acts of vengeful insiders. Therefore, the C-suite of the organization should closely monitor deliberate acts such as the theft of personal information for resale on platforms like the dark web by insiders. Cases of intentional identity theft often involve outsourced services, contractors, or users who do not carry out proper cyber-risk management oversight.

Most often, the aforementioned group of individuals does not have a strong allegiance with a specific organization. The chief information officer, the chief information security officer, and the chief executive officer should also monitor and document suspicious actions around the personal information of customers. These stakeholders must also log and notify the top executives and the board of directors about severe actions like the cut and paste of customers' data from the company's databases and the unauthorized download of the personal information of customers to USB drives (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). Similarly, the C-suite should carry out intellectual property investigations on the deliberate theft of intellectual property for financial benefits, the malicious exposure of intellectual property by revengeful insiders, and the follow-up of unintentional data leak or loss in the company (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

Although the accidental exposure of intellectual property may occur in a company, intellectual properties such as proprietary formulas, computer-aided design files, and product plans are often targeted by vengeful insiders for deliberate identity theft. Deliberate acts such as intentional data leaks and anonymous sending of proprietary formulas to competitors may cause significant damage to the organization (Cybersecurity and Infrastructure Security Agency, 2020). For instance, some insiders may sell the intellectual property of a company to its competitors to further personal objectives like securing a new job position with the rival organization. In this regard, the C-suite should carry out investigations to identify anomalous off-hours activity, unusual mobile storage uses like gigabyte transfers, or other suspicious activities with software applications. The chief information officer, the chief information security officer, and the chief executive officer should ensure that various leading indicator actions like unauthorized instant messaging sessions are logged to facilitate the reconstructions of the timeline of the cybersecurity incident (Cybersecurity and Infrastructure Security Agency, 2020).

Considering the fact that many national and internal banks wire-transfer a huge amount of cash daily, organizations have developed and implemented policies to detect suspicious behaviors among insiders (Cybersecurity and Infrastructure Security Agency, 2020). The C-suite of the organization may conduct fraud investigations on policies that address the manipulation of files, records, and other data, collusion and coercion, and fraudulent account access by insiders. In the banking industry and financial institutions, the tampering of financial data and records is considered fraudulent activity. Therefore, the C-suite, if each company in the banking industry or financial institution should notify the organization about signs of modification of financial statements, invoices, and other financial records. The Sarbanes-Oxley Act mandates the executives in an organization to certify the financial results and reports of their organization on the efficacy of internal control measures over financial reporting. In view of this, the top executives in various corporations have incorporated financial reporting to all user activities that may serve as potential indicators of fraudulent activities (Lipton et al., 2018).

Best Practice 3. The cybersecurity team in different organizations also places alerts on user activities that indicate unscrupulous behaviors (Cybersecurity and Infrastructure Security Agency, 2020). Some of these behaviors include off-hours access to confidential databases, the deliberate disconnection of a user's computer from the corporate network, and inappropriate use of encryption by employees. Perpetrators of fraudulent activities often employ extreme measures to cover their tracks or hide their illegitimate activities. Therefore, the chief information officer, the chief information security officer, and the chief executive officer must use sophisticated tools that will foster investigations on policies that address the manipulation of files, records, and other data, collusion and coercion, and fraudulent account access by insiders (Cybersecurity and Infrastructure Security Agency, 2020). The outcome of thorough investigations and detailed documentation of all activities and data provides compelling evidence and grounds for the prosecution of the perpetrator. This approach also offers insight into the deployment of policies that will proactively monitor similar unscrupulous behaviors across the organization (Raytheon, 2009; Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020).

The chief information officer, the chief information security officer, and the chief executive officer should also carry out investigations on abuse or improper conduct by privileged users (Cybersecurity and Infrastructure Security Agency, 2020). Common instances of abuse or improper conduct by privileged users are the creation of false accounts, insertion of backdoors or logic bomb viruses, and the deliberate abuse and sabotage of corporate infrastructure.

Employees such as database and network administrators who have advanced access rights may leverage their privilege to access the organization's systems and networks to launch a cyber-attack. The access of such malicious users to the company's systems and networks puts the intellectual property, personal data of customers, and infrastructure integrity of the organization at risk. This presumption is based on the fact that such users have the expertise and access to sophisticated tools required to discreetly launch a cyber-attack. Therefore, the C-suite must pay closer attention to these users because they may pose a significant threat to the cybersecurity of the organization (Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020).

The senior management must understand that conducting investigations on abuse or improper conduct by privileged users may be challenging due to the aforementioned facts (Raytheon, 2009). In order to ensure the efficacy of the investigation, the C-suite of the organization must develop specific policies for the administrators that keep track of the activity of users within applications, such as log file modifications, logons, and the creation of user accounts. Furthermore, the senior management should document and replay investigations to identify deliberate acts of malice by insiders, such as intentional data theft, the creation of backdoor access, or the insertion of harmful codes (Cybersecurity and Infrastructure Security Agency, 2020). The C-suite must also go back and mine event logs while investigating the abuse of privileged access by sophisticated users. This strategy will help the chief information officer, the chief information security officer, and the chief executive officer to correlate seemingly innocuous incidents that exhibit the malicious intent and harmful behavior of privileged users (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). The approach will also allow the senior management to gather additional proof of the unproductive and subversive activities of privileged users.

The chief information officer, the chief information security officer, and the chief executive officer must carry out compliance investigations on corporate governance adherence, general compliance audits, and violations of personally identifiable information or protected health information compliance in the organization (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). The C-suite may also search for pieces of evidence of non-violation, proof of the adherence of employees to policies, or the efficient logging and documenting of best practices to ensure compliance with the stipulated regulations of the organization. Retailers, financial companies, and hospitals must be highly regulated by the C-suite because of the large volumes of sensitive information that these organizations manage. In view of this, regulations such as the federal Health Insurance Portability and Accountability Act (HIPAA) mandates the healthcare provider in various regions must make sure the personal health information of patients are protected from cybercriminals. Similar regulations like the Sarbanes-Oxley Act mandates executives in financial institutions to ensure the protection of customers' data. Therefore, the C-suite in financial institutions and banking industries must ensure that the personally identifiable information of customers is protected (Lipton et al., 2018). The violation of corporate governance rules by employees may expose an organization to legal risks. Thus, the senior management must also monitor the adherence of employees to corporate governance guidelines stipulated in the employee handbook (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

The chief information officer, the chief information security officer, and the chief executive officer should investigate the profile of insiders who are more likely to expose the organization to cyber-risks (Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020). Such individuals include employees who have resigned or are about to resign, users who have years of expertise in the use of sophisticated technology, employees with high privilege access such as network or system administrators, former employees with access to the company's network or system, contractors, and outsourced service or call center employees. A quintessential factor in addressing insider threats is understanding the motivations and profiles like the job status of violators (Cybersecurity and Infrastructure Security Agency, 2020). Therefore, the C-suite of the organization must have a good knowledge of behavioral and user profiles to make the investigation process easier. Moreover, the chief information officer, the chief information security officer, and the chief executive officer should work with the board of directors and committee members to develop and implement general monitoring policies to ensure the protection of the organization's intellectual property (Cybersecurity and Infrastructure Security Agency, 2020). These stakeholders should also build stringent policies around employees or other individuals who have access to the core intellectual property of the organization. The C-suite of the enterprise can also collaborate with the personnel in the human resources department to identify employees who are likely to expose the organization to cyber-risks. These stakeholders must further consider deploying policies around such employees to specifically search for anomalous activities such as the copying of large files to USB devices, high-volume printer output at odd hours, or other leading indicators of intellectual property theft (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 4. The C-suite must lay a monitoring foundation for investigations in the company (Raytheon, 2009; Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020). Considering the high complexity and number of cases of how employees and other insiders work with information technology resources, the C-suite of every organization must work with the board of directors and committee members to develop insider risk management policies that will define, monitor, and enforce the stipulations in the policies for user actions, access, data handling, and data transfer. The implementation of such policies will enable the senior management to ensure that employees or other insiders are not exposing the corporation to cyber-risks. The solutions developed must also help the C-suite to investigate cases of actualized or attempted violation of policies and determine if the act was deliberate or malicious. The outcome of this investigation will help the senior executives to manage the underlying problems caused by the insider attack appropriately (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

In addition, the C-suite must analyze the activity of users on endpoint devices and the internal network of the organization (Cybersecurity and Infrastructure Security Agency, 2020). This approach requires the deployment of a network device to monitor network traffic and users on individual computers. This solution will help the senior management to ensure that mobile and disconnected users adhere to the policies of the organization. The C-suite's goal of monitoring insider activities should be centered on the identification of unpredictable and predictable violations of policies to facilitate the development of appropriate responses to mitigate the aftermath of such violations (Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 5. The senior management must also decide whom and where to monitor (Cybersecurity and Infrastructure Security Agency, 2020). The C-suite must understand that it is impossible to analyze and capture all the data sent through the company's egress points or processed using the organization's computer systems or networks. In view of this, the C-suite needs to prioritize the most valuable assets to the organization and create series of monitoring regulations around users who have the most access to such assets or who stand to benefit the most from obtaining such assets. For instance, a policy may be created to detect if information about the organization's secret product plan is copied to USB devices or sent via email using the desktops of users with the highest level of access to valuable assets. The senior management can also create policies that monitor the mobile or USB storage use of employees in specific departments such as engineering and production to manage the level of exposure of the company's data at this level to cyber-risks. A different set of policies should be established for contractors and outsourced call center representatives to monitor the activities of users that attempt to retrieve customer data from the company's database. Sophisticated monitoring should be implemented by the C-suite to keep track of the activities of system and network administrators such as file modifications, logins, or other leading indicators of compliance violations. The activities of employees who have resigned or whose employment was terminated by the organization should be monitored closely by the C-suite (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

The chief information officer, the chief information security officer, and the chief executive officer must decide on disclosing or withholding information about their monitoring capabilities to employees (Raytheon, 2009). Some senior executives believe that the disclosure of the monitoring capabilities of the organization to employees will deter them from carrying out malicious acts or engaging in criminal activities. In this regard, this decision is considered a valid approach to ensuring cybersecurity and addressing concerns about the monitoring of insiders by the organization. On the other hand, some senior executives think it is more advantageous for the organization to withhold information about its monitoring capabilities from employees (Cybersecurity and Infrastructure Security Agency, 2020). This decision is based on the presumption that the C-suite is more likely to identify employees with malicious intentions or dishonest tendencies, as such employees will not have an avenue to evade being detected by the implemented monitoring policies. Therefore, the C-suite must decide if the reinforcement of positive behavioral change obtained from the disclosure of the monitoring capabilities of the company outweighs the high risk of users circumventing the barriers put in place to keep track of their activities (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 6. The C-suite must analyze the vulnerabilities, leading indicators, and areas of concern in the organization (Raytheon, 2009; Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020). The major challenge of many companies is the lack of visibility into the activities of insiders. In view of this, the senior management should assess the vulnerabilities that expose the organization to the risk of an insider attack. The C-suite should also look for leading indicators of the unscrupulous behavior of users rather than focusing only on the specific incidents that led to the insider attack. Some of the policies that may be implemented by the C-suite in an organization to enhance visibility are the monitoring of user's unusual network traffic spikes at odd hours, the use of non-business applications, and traffic going to unauthorized geographic destinations such as file transfer protocol sites in China or Russia. The senior management must also monitor the user's viewing of harmful or unauthorized content such as job search sites, pornography, or hate sites that indicate job dissatisfaction, potential legal risks, or low productivity of the employee (Cybersecurity and Infrastructure Security Agency, 2020). Furthermore, the C-suite should monitor unusual offline activities, inappropriate use of encryption, high volumes of file transfer to USB devices or mobile storage, and high printing volumes at unusual hours. Once the senior management has investigated the activities of users at different levels of the organization and identified factors that contributed to the occurrence of the insider attack, these stakeholders must develop an efficient and effective action plan to remediate the problems caused by the aftermath of the insider attack (Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 7. The C-suite must establish procedures to investigate and remediate the non-critical violations (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). This practice will prevent the senior management from being overwhelmed with false-positive indicators and enable the investigation team to focus on critical violations. Such procedures may involve putting a system in place to automatically remediate non-critical violations or correct these violations with minimal intervention. There are various forms of automated remediation systems. The least intrusive automated remediation system sends prompts to educate and inform them about the risks of non-critical violations. The efficacy of automated remediation systems can be enhanced by incorporating policies that will lead to the escalation of critical violations (Cybersecurity and Infrastructure Security Agency, 2020). The procedures for the escalation of critical violations may involve the implementation of control that terminates the session or initiates a thorough workflow to quarantine the information and the notification of compliance officers. The compliance officers will then take the required actions to put an end to the unauthorized behavior of the user (Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 8. The C-suite must decide on the incidents that need to be investigated (Raytheon, 2009; Hartline, 2017). For instance, if the senior management discovers that a violation of a security policy has occurred, these stakeholders must decide on how to proceed with the investigation. The chief information officer, the chief information security officer, and the chief executive officer must either decide to proceed with the monitoring of the user's activities and allow the data to be retrieved from the company's network or stop the user from retrieving the data from the web by forcefully logging the individual off his/her work station. The C-suite must also determine the organization's thresholds for escalating incidents that need to be investigated (Cybersecurity and Infrastructure Security Agency, 2020). It is easier to identify such thresholds once the most valuable assets have been identified and the potential violators and risk scenarios have been outlined by the investigation team. For instance, the discovery of a USB copy of a simple computer-aided design file does not call for an investigation by the C-suite of the organization. However, the discovery of a copy of large numbers of computer-aided design files at odd hours by a network or system administrator or a recently sacked employee calls for an investigation by the C-suite of the organization (Cybersecurity and Infrastructure Security Agency, 2020).

However, the C-suite must understand that it is impractical to foresee all incidents despite thorough investigations (Raytheon, 2009). Occasionally, the need for an investigation may arise through non-digital avenues. For instance, the personnel in the human resources department may notify the senior management that an employee has openly expressed dissatisfaction with the company and cannot wait to occupy a new job position with a rival company or any other firm. In another instance, an outsider may notify the top executives that he/she has seen proprietary information about the company in a competitor's office or other inappropriate locations. Such instances warrant a thorough investigation by the chief information officer, the chief information security officer, and the chief executive officer. These stakeholders must employ sophisticated policies for known violations to identify incidents and leading indicators from the activities of the suspected violators (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

The C-suite must decide whether to conduct the investigation or enlist the expertise of a firm that specializes in the recovery of digital evidence. In some cases, the senior management may choose to seek the help of individuals who have made several attempts to conceal or remove their activities through the deletion of logs of their activities or the use of hacking tools (Cybersecurity and Infrastructure Security Agency, 2020). However, the C-suite must understand that the forensic recovery of files that have been deleted is an uphill task. Apart from the need to document several records of the effort of the management to recover digital evidence, the information generated during the investigation of complex data breaches may not be easily understood by juries. Therefore, the C-suite should enlist the services of firms that have years of experience in gathering, documenting, and presenting digital evidence about data breaches to ensure the successful prosecution of the identified violator. Soliciting the help of experts will also provide the senior management with detailed information generated from sophisticated disk-level forensic analysis and log analysis, which is required to carry out effective remediation in the organization (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 9. The C-suite of the enterprise should mine incident logs and alerts of the historical activity and timeline for users (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020). This approach will enable the chief information officer, chief information security officer, and the chief executive officer to investigate the harmful behaviors of suspected violators. For instance, if the investigation of an insider attack involves the copy of a large number of proprietary computer-aided design files at off-hours, the investigation team should focus on the following: the encryption of the files weeks before the insider attack, the renaming of encrypted files will innocuous non-business names such as family_photos.zip, and the email communications associated with the copying of a large number of proprietary computer-aided design files. The aforementioned information will help the investigation team put together by the C-suite to my various instances in which the suspected user had carried out screen captures using their sensitive computer-aided design applications from the company's monitoring database (Cybersecurity and Infrastructure Security Agency, 2020). The screen captures may then be traced to outbound web-based email addresses to determine the actual screen capture and file modification prior to their encryption by the user. Quick Google searches on network traffic can be carried out by the investigation team to determine the number of employees involved in the theft of proprietary information. The C-suite may also search for other leading indicators like web traffic on a specific competitor's website, which indicates the possible motives for the theft of intellectual property data by the suspected or identified violators (Raytheon, 2009; Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 10. The C-suite must evaluate the occurrence of the insider attack in full context (Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020). Historically, the personnel in the security and information technology departments focus on searching the contents of several log files and carrying out detailed disk-level forensics after the occurrence of insider attacks. The long duration of this analysis delays the recovery of digital evidence and reduces the likelihood of the successful prosecution of identified violators. However, the development and application of modern visualization tools will enable the senior management to spot potentially harmful and malicious behaviors of users and reconstruct how the actual cybersecurity incident occurred. The reconstruction of the cybersecurity incident is quintessential to the identification of leading indicators of potentially harmful and malicious behaviors of users and facilitates the simple display of the outcome of the investigation to non-technical users (Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020). The visual representation of the cybersecurity incident also allows the senior management to take an active role in ensuring the cybersecurity of the organization.

Furthermore, the video presentation of cybersecurity incidents offers the following benefits from the investigations and monitoring standpoints: it enables the chief information officer, the chief information security officer, and the chief executive officer to parse out false positives, it helps the senior management to exonerate accidental behaviors or clear mistakes, provides digital evidence of discernible malicious or harmful activities, allows the documentation of actions for several components, and provides the enterprise with the facts required to make the most efficient and appropriate remediation. Common remediation approaches include the provision of training to enhance the awareness of employees, coaching of individual users, provision of operational interventions, modification of technological infrastructure, prosecution of identified violators, or the termination of the employment of identified violators. The C-suite of the organization may decide to rehabilitate, prosecute, or terminate the employment contract of violators. This decision is peculiar to the situation, organization, and individual involved in the cybersecurity incident (Raytheon, 2009; Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 11. The chief information officer, the chief information security officer, and the chief executive officer must isolate true trigger vents that led to the malicious behavior of insiders in the organization (Cybersecurity and Infrastructure Security Agency, 2020). In view of this, the investigation team must establish a correlation between various disparate events to reconstruct the timeline of the incident. For instance, if an investigation team analyzes the series of events that led to the copying of a large number of computer-aided design files to a USB device, the team will be able to view the actual data copied to the USB device and determine if the data was sent via email or through outbound communication channels. However, the aforementioned discovery is one of the numerous steps in the analysis of the multi-vector event. Therefore, the application of timeline reconstruction solutions that are centered on viewing outbound data streams or the content of a USB storage may be easily circumvented by malicious insiders. In order to prevent this, the C-suite must ensure that the investigation team identifies the real trigger or indicator of the user's malicious intention. In this context, the real trigger could be the insider's use of a screen capture within the computer-aided design application to avoid detection (Raytheon, 2009). Even though other steps taken by the user, such as the saving of the file using innocuous names, raise a red flag, what set off the alarm of malicious intention was the encryption of the files at odd hours. This knowledge may be used by the C-suite to determine the steps the organization must take to establish effective monitoring policies in the company. These policies will enable the chief information officer, the chief information security officer, and the chief executive officer to identify such events earlier and prevent the occurrence of the same or similar cybersecurity incident (Cybersecurity and Infrastructure Security Agency, 2020).

Best Practice 12. The C-suite must use the knowledge acquired to build enterprise monitoring policies that are triggered by events such as the unscrupulous behaviors of malicious insiders (Raytheon, 2009; Hartline, 2017; Cybersecurity and Infrastructure Security Agency, 2020). This trigger must then be used to alert the senior management to enhance monitoring activities and escalate the investigation of the suspected violator. This policy must be deployed widely in the organization. In order to enhance the sensitivity of the policy to specific trigger events, the chief information officer, the chief information security officer, and the chief executive officer may include after-hours or odd hours qualifiers to minimize false positives (Cybersecurity and Infrastructure Security Agency, 2020).

How Will the Board Be Notified and Involved? How Will You Evaluate Impact?

The board of directors and the senior management must engage in critical conversation to develop effective measures to ensure the cybersecurity of the organization (Internet Security Alliance, 2020). The responsibility of the board of directors is to ensure that the senior management is prepared and has an effective plan to prevent and mitigate cyber-attacks. The board of directors must also make sure that the C-suite is preparing the entire organization for the eventuality of a cyber-attack. Furthermore, the board of directors must make sure the senior management has prepared practical solutions to detect cybersecurity incidents, stop cyber-attacks, mitigate the effects of cyber-attacks, and ensure that the company resumes its normal business operations as soon as possible (Internet Security Alliance, 2020). The impact of the cybersecurity measures developed by the senior management can be evaluated using cyber-metrics, key risk indicators, and KPIs. Effective metrics and indicators have already been discussed in this paper (Tunggal, 2021a).

What Are the Best Practices When It Comes to Outsourcing Cybersecurity to a Third-Party?

There are several advantages of outsourcing cybersecurity to a third party (Baker, 2016). Some of these advantages include cost savings and increased access to individuals with a higher level of expertise and more profound knowledge about cybersecurity compared to the experts available within the organization. However, there are certain risks associated with the outsourcing of cybersecurity to a third party. The C-suite must consider these risks before choosing a cybersecurity vendor. Some of the best practices the senior management can adopt to minimize the risks of outsourcing cybersecurity include the following (Baker, 2016):

1. The organization must never solicit the expertise of offshore cybersecurity providers.
   Despite the tempting price offers of offshore cybersecurity providers, organizations must not allow these providers to access their network or sensitive information. Cybersecurity providers must have full access to the internal system and data of the organization to carry out their duties. Considering the fact that there is no way to verify the skills, experience, education, and criminal background of offshore cybersecurity providers, it is a huge risk to allow such providers to have full access to a company's internal system and data. Moreover, if a data breach occurs as a result of soliciting the expertise of offshore cybersecurity providers, the organization does not have legal recourse against such providers.
2. Organizations should steer clear of cybersecurity providers that proffer solutions that are remote-based. Although some cybersecurity companies offer services that are remote-based and conducted via the Internet or telephone, the implementation of remote-based solutions cannot provide full protection of an organization's assets. Considering the fact that 50% of all cases of data breaches are due to negligence, malicious acts of insiders, or mistakes, remote-based solutions cannot prevent or mitigate such threats.
3. Organizations must beware of providers that claim their cybersecurity solutions offer 100% protection against data breaches. There is no such thing as a foolproof cybersecurity solution that prevents all forms of data breaches. Cybersecurity experts constantly engage in a never-ending war against cybercriminals to prevent cyber-attacks. However, as soon as cybersecurity experts fix a particular vulnerability, hackers dedicate their time to identifying the next vulnerability. Unfortunately, each new digital technology often presents new vulnerabilities that can be exploited by hackers. As a result, there is no such thing as an impenetrable cybersecurity system. Therefore, the C-suite of organizations should steer clear of cybersecurity providers that suggest

otherwise. Such providers may not be able to effectively respond or mitigate the aftermath of cyber-attacks.

4. The C-suite of the organization must make sure the cybersecurity provider has real-life experience in the prevention and mitigation of cyber-attacks. Some cybersecurity providers hire inexperienced graduates with little to no actual work experience in the protection of critical assets and infrastructures. The required cybersecurity expertise cannot be honed from reading books of peer-reviewed articles. The cybersecurity provider's team must comprise individuals who have the experience needed to grasp the nuances of real-life information security challenges and processes. Such security experts are less likely to make mistakes. Therefore, the senior management must ensure that the organization hires cybersecurity professionals with several years of experience in the protection of valuable assets and infrastructures.
5. The C-suite of the organization must also avoid hiring cybersecurity providers who claim to have hardware that can address all the security needs of the company. The management must understand that security hardware is not a universal solution to all cybersecurity issues. This type of hardware is simply used as a tool by cybersecurity professionals. The purchase of security hardware cannot replace the need for cybersecurity professionals in an organization.

In addition, the senior management should ask critical questions during the selection and evaluation process to ensure the selection of the right cybersecurity provider for the organization (Baker, 2016).

Are You Getting the Right Support and Funding to Address the Insider Risks within the Organization?

The board of directors must ensure they provide the senior management with the necessary support and funds to address insider risks within the organization (Internet Security Alliance, 2020). In view of this, the board of directors must allocate appropriate resources to support the development and implementation of insider risk management systems. The allocation of these resources should not be limited to the personnel in the information technology department. The board must ensure that allocations are made to fund product development, employee training, and the monitoring of compliance violations in the company. The budget of the board of directors should also include a talent review or succession plan, an assessment of the preparedness of successors, and determination of the need for the recruitment of personnel with the required skillset or additional employee training (Internet Security Alliance, 2020). In addition, the board of directors must allocate adequate resources towards the implementation of a well-constructed response plan to insider attacks (Rogers & Ashford, 2015; Bailey et al., 2020). The aforementioned strategies will increase the level of preparedness of the board of directors and the senior management to address insider risks.

What is the Cost to the Organization of Insider Risk and Insider Threat Investigations?

The board of directors and the C-suite must be aware of the cost to the organization of insider risk and insider threat investigations (Internet Security Alliance, 2020). It is estimated that the cost of an insider risk comprises the following components: direct cost, indirect cost, and lost opportunity cost. Direct cost pertains to the funds required to detect, investigate, mitigate, and remediate a data breach, while indirect cost is the value of employee time and resources of the organization spent on addressing insider risk. In contrast, lost opportunity cost is the number of losses in potential profits caused by the occurrence of a cyber-attack (Ekran, 2021). It is estimated that the cost of insider risks keeps increasing by the year. According to Ekran (2021), the average cost of insider risks increased by 31%, from $8.76 million in 2017 to $11.45 million in 2019. Organizations in North America are more exposed to the risks and consequences of insider attacks. In this region, it is estimated that the average cost of insider risks ranges from $11.1 million to $13.3 million. As a result, these companies spend about $513,000 to $756,760 on monitoring, investigation, cybersecurity incident response, escalation, ex-post analysis, containment, and remediation of insider risks-related incidents (Ekran, 2021). Similarly, the cost of insider threat investigations has increased over the years.

According to Epstein (2020), organizations have spent an average amount of $644,852 per incident across three categories of insider threats and seven cost centers. The three main categories of insider threats are credential theft, contractor or employee negligence, and malicious insiders. The seven cost centers are monitoring and surveillance, investigation, escalation, cybersecurity incident response, containment, ex-post analysis, and remediation (Epstein, 2020; Ekran, 2021). Epstein (2020) emphasized that the cost of insider threat investigations has increased by 86% in the past three years. It is estimated that the average cost of investigating insider threats is increased from $41,461 per cybersecurity incident in 2016 to $103,798 per cybersecurity incident in 2020. These investigations include activities that are required to uncover the scope, source, and magnitude of one or more cybersecurity incidents (Epstein, 2020).

Over the years, companies have sought effective ways to reduce the costs of insider threat investigations. Recommended ways in which the C-suite can help to tighten security practices in the organization and reduce the costs of insider threats investigations include the following (Epstein, 2020):

1. The establishment of automated systems to detect insider-specific data breaches. This approach will empower the cybersecurity team to hasten the investigation process. The alerts generated by the automated systems will also help the senior management to pay close attention to specific insider activities, rather than wasting resources on monitoring various logs.
2. The senior management must build context into programs in an organized manner to foster the development of quick resolutions. The context must be organized in a way that is easy for technical and non-technical stakeholders to understand the timeline of the user. The senior management must also use contexts with data, endpoints, and applications related to alerts to kick off the investigation process. Reports generated automatically may also provide a summary of the situation that can be shared with human resources personnel, as well as business and legal counterparts. Therefore, the senior management should consider using automated systems to visually document the activities of the suspected or identified violator before and after the occurrence of an insider attack to obtain strong digital evidence.
3. The senior management must ensure that the personnel in the human resources department hire the right individuals to carry out in-house security investigations. The employment of the right individuals will reduce the cost of insider threat investigations accrued from the consultation of experts outside the company.
4. The senior management must also implement the right visualization tools to document the events that led to the insider attack. They must also create timelines that are easy to understand and visual activity replays that contain detailed information about the cybersecurity

incident. The information obtained from visual activity replays can be forwarded to the personnel in the human resources department and finance department for further investigation.

5. The C-suite of the organization can also reduce insider threat investigation costs by recording suspicious behaviors of insiders and automatically sending alerts of possible insider threats to the senior management and the board of directors.

Conclusion

Over the years, many individuals, governments, and enterprises have been victims of cyber-attacks orchestrated by cybercriminals. As a result, there has been an increased focus on the development and implementation of cybersecurity measures to prevent and mitigate cyber-attacks. However, the effective prevention of cyber-attacks depends on the understanding of the board of directors about cyber-risks management. The boards of directors must also have an in-depth understanding of their roles and responsibilities in cyber-risk management to effectively prevent or mitigate cyber-attacks. In view of this, this handbook documents the specific roles and responsibilities of the board of directors and top executives in addressing cyber-risk-related issues in an organization. The various laws and regulations on cyber-risk management and cybersecurity governance are also documented in this handbook. Furthermore, this handbook contains detailed information about the effective ways to establish cybersecurity governance and responses to questions the board should be asking the C-suite/CISO on cyber resiliency.

References

Accenture. (n.d.). *The cyber resilient enterprise.* Retrieved from https://www.accenture.com/_acnmedia/PDF-88/Accenture-Cyber-Resilient-Enterprise-US-Digital.pdf

Aguilar, L.A. (2014). *Boards of directors, corporate governance and cyber-risks: Sharpening the focus.* Retrieved from https://www.sec.gov/news/speech/2014-spch061014laa

Alina, C.M., Cerasela, S.E., and Gabriela, G. (2017). *Internal audit role in cybersecurity.* Retrieved from https://ideas.repec.org/a/ovi/oviste/vxviiy2017i2p510-513.html

American Institute of Certified Public Accountants. (2016). *Attestation standards: Clarification and recodification.* Retrieved from https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/SSAE_No_18.pdf

Arbuckle, A. (2017). *Let's close the cybersecurity knowledge gap in the boardroom.* Retrieved from https://www.securityweek.com/lets-close-cybersecurity-knowledge-gap-boardroom

Aria Cybersecurity Solutions. (2021). *The top 10 most significant data breaches of 2020.* Retrieved from https://blog.ariacybersecurity.com/blog/the-top-10-most-significant-data-breaches-of-2020

Bailey, T., Banerjee, S., Feeney, C., and Hogsett, H. (2020). *Cybersecurity: Emerging challenges and solutions for the boards of financial services companies.* Retrieved from https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity-emerging-challenges-and-solutions-for-the-boards-of-financial-services-companies

Baker, M. (2016). *5 best practices for outsourcing cybersecurity.* Retrieved from https://www.channelfutures.com/from-the-industry/5-best-practices-for-outsourcing-cybersecurity

BBC News. (2021). Meat giant JBS pays $11m in ransom to resolve cyber-attack. *BBC News.* Retrieved from https://www.bbc.com/news/business-57423008

Berman, M. (2018). *First, second, third, fourth and fifth parties: How to measure the tiers of risk.* Retrieved from https://www.ncontracts.com/nsight-blog/first-second-third-fourth-and-fifth-parties-how-to-measure-the-tiers-of-risk

Bianculli, L. (2021). *Ten common IT security risks in the workplace.* Retrieved from https://www.ccsinet.com/blog/common-security-risks-workplace/

Blonder, S.P. (2014). *How closely is the board paying attention to cyber risks?* Retrieved from http://www.insidecounsel.com/2014/04/09/how-closely-is-the-board-paying-attention-to-cyber

Bonime-Blanc, A. (2016). *A strategic cyber-roadmap for the board: From sit-back to lean-in governance.* Retrieved from https://www.wlrk.com/docs/TCB strategiccyberroadmap.pdf

Chan, J. (2018). *7 ways to bridge the cybersecurity skills gap.* Retrieved from https://www.insightpartners.com/blog/7-ways-to-bridge-the-cyber-security-skills-gap/

Cheng, J.Y., and Groysberg, B. (2017). *Why boards aren't dealing with cyber threats.* Retrieved from https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats

Cybersecurity and Infrastructure Security Agency. (2020). *Insider threat mitigation guide.* Retrieved from https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf

Deloitte. (2016). *Cybersecurity: The changing role of the board and the audit committee.* Retrieved from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-cyber-security-noexp.pdf

Downs, F. (2020). *Top cyberattacks of 2020 and how to build resiliency.* Retrieved from https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency

Ekran. (2021). *Insider threat statistics for 2021: Facts and figures.* Retrieved from https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

Epstein, J. (2020). *The skyrocketing costs of insider threat investigations.* Retrieved from https://www.proofpoint.com/us/blog/insider-threat-management/skyrocketing-costs-insider-threat-investigations

Ernst and Young Center for Board Matters. (2017). *Board matters quarterly.* Retrieved from https://www.wlrk.com/docs/EYboardmattersquarterly january2017.pdf

Ernst and Young Center for Board Matters. (2018). *2018 proxy season review.* Retrieved from https://www.wlrk.com/docs/EY2018proxyseasonpreview.pdf

FCPA Corporate Enforcement Policy. (n.d.). Retrieved from https://www.justice.gov/criminal-fraud/file/838416/download

Financial Stability Board. (2013). *Principles for an effective risk appetite framework.* Retrieved from http://www.financialstabilityboard. org/wp-content/uploads/r_131118.pdf?page_moved=1

Fruhlinger, J. (2021). *The CIA triad: Definition, components, and examples.* Retrieved from https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

Governance and Standards Division. (2017). *Cybersecurity governance guidelines.* Retrieved from https://www.moheri.gov.om/userupload/Policy/Cyber%20 Security%20Governance%20Guidelines.pdf

Gupta, P.P., and Leech, T. (2015). *The next frontier for boards: Oversight of risk culture.* Retrieved from https://www.wlrk.com/docs/pdfdownload.pdf

Hartline, C. (2017). *Examination of insider threats: A growing concern*. Retrieved from https://www.proquest.com/openview/6325a7855e9c0b71fe1bb212618b2b19/1?pq-origsite=gscholar&cbl=18750

Harvard Business Review. (2021). Questions every board should be asking about insider cybersecurity risks. *Harvard Business Review*. Retrieved from https://hbr.org/sponsored/2021/06/questions-every-board-should-be-asking-about-insider-cybersecurity-risks

Herjavec Group. (2017). *2017 cybercrime report*. Retrieved from https://www.wlrk.com/docs/2017CybercrimeReport.pdf

Hess, S., and Morton, S. (2020). *Cybersecurity: Setting the tone at the top*. Retrieved from https://www.commercialriskonline.com/cyber-security-setting-the-tone-at-the-top/

In the Court Chancery of the State of Delaware. (2009). *Opinion*. Retrieved from https://www.wlrk.com/docs/3338-CC.pdf

In the Court Chancery of the State of Delaware. (2011). *Memorandum opinion*. Retrieved from https://www.wlrk.com/docs/5215-VCG.pdf

Internet Security Alliance. (2020). *Cyber risk oversight handbook*. Retrieved from https://isalliance.org/isa-publications/cyber-risk-oversight-handbook/

Kalakuntla, R., Vanamala, A.B., and Kolipyaka, R.R. (2019). Cybersecurity. *Holistica*, 10(2), 115–128.

Lipton, M., Niles, S.V., Miller, M.L., Lipton, W., and Katz, R. (2018). *Risk management and the board of directors*. Retrieved from https://corpgov.law.harvard.edu/2018/03/20/risk-management-and-the-board-of-directors-5/

Malla Reddy College of Engineering & Technology. (2020). *Digital notes on cybersecurity*. Retrieved from https://mrcet.com/pdf/Lab%20Manuals/IT/CYBER%20SECURITY%20(R18A0521).pdf

Metivier, B. (2018). *Cybersecurity roles and responsibilities for the board of directors*. Retrieved from https://www.tylercybersecurity.com/blog/cybersecurity-roles-and-responsibilities-for-the-board-of-directors

Morgan, S. (2016). *Cyber crime costs projected to reach $2 trillion by 2019*. Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/

National Association of Corporate Directors. (2016). *NACD public company governance survey*. Washington, DC: NACD.

National Association of Corporate Directors. (2017). *Report of the NACD blue ribbon commission on risk governance: Balancing risk and reward*. Retrieved from https://www.wlrk.com/docs/1605831_1.pdf

National Institute of Standards and Technology. (2014). *Framework for improving critical infrastructure cybersecurity*. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology. (2020). *Cybersecurity framework version 1.1: Manufacturing profile*. Retrieved from https://www.nist.gov/news-events/news/2020/10/cybersecurity-framework-version-11-manufacturing-profile-nistir-8183

NTT Group. (2016). *Global threat intelligence report*. Retrieved from https://scadahacker.com/library/Documents/Threat_Intelligence/NTT%20-%20Global%20Threat%20Intelligence%20Report%20-%202016.pdf

Olavsrud, T. (2016). *Companies complacent about data breach preparedness*. Retrieved from https://www.cio.com/article/3136651/companies-complacent-about-data-breach-preparedness.html

Panda Security. (2021). *11 emerging cybersecurity trends in 2021*. Retrieved from https://www.pandasecurity.com/en/mediacenter/tips/cybersecurity-trends/

Pande, J. (2017). *Introduction to cybersecurity*. Retrieved from https://uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

Protiviti. (2016). *Arriving at internal audit's tipping point amid business transformation*. Retrieved from https://www.wlrk.com/docs/2016internalauditcapabilitiesandneedssurveyprotiviti.pdf

Raytheon. (2009). *Best practices for mitigating and investigating insider threats*. Retrieved from https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/iis/documents/content/rtn_iis_whitepaper-investigati.pdf

Rogers, G., and Ashford, T. (2015). *Mitigating higher ED cyber-attacks*. Retrieved from https://files.eric.ed.gov/fulltext/ED571277.pdf

Roland, L.T., and Humes, S.J. (2014). *Before rolling blackouts begin: Briefing boards on cyber attacks that target and degrade the grid*. Retrieved from https://open.mitchellhamline.edu/cgi/viewcontent.cgi?article=1565&context=wmlr

Securities and Exchange Commission. (2017). *FAST act modernization and simplification of regulation S-K*. Retrieved from https://www.sec.gov/rules/proposed/2017/33-10425.pdf

Seema, P.S., Nandhini, S., and Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering*, 7(11), 125–128.

Singh, S. (2019). *Cyber insecurity is harming emerging markets*. Retrieved from https://globalsecurityreview.com/cyber-insecurity-harming-emerging-markets/

Tunggal, A.T. (2021a). *14 cybersecurity metrics + KPIs you must track in 2021*. Retrieved from https://www.upguard.com/blog/cybersecurity-metrics

Tunggal, A.T. (2021b). *Why is cybersecurity important?* Retrieved from https://www.upguard.com/blog/cybersecurity-important

Turton, W., and Mehrotra, K. (2021). *Hackers breached colonial pipeline using compromised password*. Retrieved from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

U.S. Securities and Exchange Commission. (2011). Retrieved from https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Vanguard. (2017). *An open letter to directors of public companies worldwide*. Retrieved from https://www.wlrk.com/docs/2017VanguardOpenLettertoBoards.pdf

Vigliarolo, B. (2021). *NIST cybersecurity framework: A cheat sheet for professionals*. Retrieved from https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/

Vittorio, A., and Holland, J. (2021). *Rippling cyberattacks force corporate boards to rethink risk*. Retrieved from https://news.bloomberglaw.com/privacy-and-data-security/rippling-cyberattacks-force-corporate-boards-to-rethink-risk

Waldman, A. (2021). *10 of the biggest cyber-attacks of 2020*. Retrieved from https://searchsecurity.techtarget.com/news/252494362/10-of-the-biggest-cyber-attacks

Index