NACD

INTERNET SECURITY ALLIANCE

2023

DIRECTOR'S HANDBOOK ON CYBER-RISK OVERSIGHT

About NACD

The National Association of Corporate Directors (NACD) is the premier membership organization for board directors who want to expand their knowledge, grow their network, and maximize their potential.

As the unmatched authority in corporate governance, NACD sets the standards of excellence through its research and community-driven director education, programming, and publications. Directors trust NACD to arm them with the relevant insights to make high-quality decisions on the most pressing and strategic issues facing their businesses today.

NACD also prepares leaders to meet tomorrow's biggest challenges. The NACD Directorship Certification® is the leading director credential in the United States. It sets a new standard for director education, positions directors to meet boardroom challenges, and includes an ongoing education requirement that prepares directors for what is next.

With an ever-expanding community of more than 23,000 members and a nationwide chapter network, our impact is both local and global. NACD members are driven by a common purpose: to be trusted catalysts of economic opportunity and positive change—in business and in the communities we serve.

To learn more about NACD, visit nacdonline.org

About the Internet Security Alliance

The mission of the Internet Security Alliance (ISA) is to integrate advanced technology with economics and public policy to promote a sustainably secure cyber system. The ISA board consists of cyber leaders (typically chief information security officers) from virtually every critical industry sector. For more than 20 years, ISA has created a comprehensive theory and practice for cybersecurity covering both enterprise risk management and government policy. ISA's consensus principles and practices, developed in collaboration with NACD and the World Economic Forum, are the foundation of this program and are contained in ISA's numerous Cyber-Risk Handbooks. The ISA board has created a companion book *Cybersecurity for Business* (with a foreword from NACD president and CEO Peter Gleason) that translates the board level principles into roles and practices for a corporation's management team

ISA has also defined a new approach to public policy on cybersecurity in its new book, *Fixing American Cybersecurity: Creating a Strategic Public Private Partnership.* Many of the proposals ISA makes in *Fixing American Cybersecurity* are integrated into the new National Cybersecurity Strategy recently released by President Biden.

More information regarding ISA can be found at isalliance.org.

Prepared by Larry Clinton
President and CEO
Internet Security Alliance

WITH SUPPORT FROM

Anton Marx
Internet Security Alliance

Katie Swafford
Senior Manager, Digital and Cybersecurity Content
NACD

Dylan Sandlin
Digital and Cybersecurity Content Lead
NACD

Table of Contents

Acknowledgments 4

Foreword 5

About the Handbook 7

Introduction 8

PRINCIPLE ONE: Cybersecurity as a Strategic Risk 13

PRINCIPLE TWO: Legal and Disclosure Implications 17

PRINCIPLE THREE: Board Oversight Structure and Access to Expertise 23

PRINCIPLE FOUR: An Enterprise Framework for Managing Cyber Risk 28

PRINCIPLE FIVE: Cybersecurity Measurement and Reporting 33

PRINCIPLE SIX: Encourage Systemic Resilience and Collaboration 38

Toolkit

TOOL A: Ransomware Readiness **41**

TOOL B: Assessing the Board's Cyber-Risk Oversight Effectiveness **44**

TOOL C: The Cyber-Insider Threat **48**

TOOL D: Supply-Chain and Third-Party Risks **51**

TOOL E: Incident Response **54**

TOOL F: Board-Level Cybersecurity Metrics **59**

TOOL G: Cybersecurity Concerns During M&A Phases **62**

TOOL H: Building a Relationship with the CISO **69**

TOOL I: Enhancing Cybersecurity Oversight Disclosures—10 Questions for Boards **76**

TOOL J: Securing Cloud Services **81**

TOOL K: Working with CISA and Having a Conversation with Your CISO **85**

TOOL L: Incident Response and Reporting to the FBI **91**

TOOL M: Board Decisions on General Use of AI **95**

TOOL N: US Secret Service's Role in Stopping Financial Loss **98**

Acknowledgments

NACD thanks the following staff (in alphabetical order) for their contributions to the creation of this resource for board members.

Ellen Errico
Art Director

Friso van der Oord
Senior Vice President, Content

Dylan Sandlin
Digital and Cybersecurity Content Lead

Margaret Suslick
Manager, Copy Editing and Knowledge Management

Katie Swafford
Senior Manager, Digital and Cybersecurity Content Lead

Larry Clinton acted as chief author of this Handbook and is president and CEO of ISA. He would like to thank the following authors for contributing to the Principles in this handbook: Eric Forni and Andrew Serwin, DLA Piper; Nick Sanna, RiskLens; and Andrew Cotton, EY. Authors of Tools are credited on the first page of each tool.

ISA Board Members

Wade Bicknell, MUFG N.A.
Robyn Boerstling, NAM
Ryan Boulais, AES Corp.
Jon Brickey, Mastercard
Larry Clinton, ISA
Deneen DeFiore, United Airlines
Jason Escaravage, Thomson Reuters
Tracie Grella, AIG
Michael Higgins, L3Harris
Patrick Hynes, EY
Shaun McAdams, Raytheon Technologies
Tim McKnight, SAP
Tim McNulty, Carnegie Mellon University
Greg Montana, FIS
Patrick Reidy, GE Aerospace
Richard Rocca, Bunge Ltd.
Nick Sanna, RiskLens
Richard Spearman, Vodafone
Dimitrios Stratakis, BNY Mellon
Ted Webster, Centene
J.R. Williamson Sr., Leidos

Contributors

(in alphabetical order by organization name)

Jen Easterly, Eric Goldstein, Matthew R. Grote, Bob Lord, Cybersecurity and Infrastructure Security Agency

Meredith Burkart, David Ring, and Joseph Szczerba, FBI

Camille Amberger, Iselin Brady, Roman Horoszewski, Emaline Keith, Kiyo Larson, Kaiya Luethje, Vincent Noteboom, Ashok Ramkumar, Tim Solanki, Dominique Eric Varier, Kyley Weigl, and Jakob Zemba, ISA Research Assistants

Elena Kvochko, SAP

Global Investigative Operations Center (GIOC), US Secret Service

Foreword

JEN EASTERLY
Director, CISA

SUSTAINABLE CYBERSECURITY: THINKING BIGGER IN OUR APPROACH TO RESILIENT INFRASTRUCTURE AND CUSTOMER SAFETY

Businesses around the world depend increasingly on technology, a digital revolution that has created both enormous rewards and exponentially expanding risks. The cyber-threat landscape we face today is more complex and dangerous than ever, with cybercrime expected to cost the world some $8 trillion dollars in 2023.[1] With corporate reputations and revenue on the line—and given the broader implications for our national security, economic prosperity, and public safety—*we must think differently*.

Consider this hypothetical—but very possible—scenario: Imagine that a CISO at a US pharmaceutical company recommends that the company fund a phishing-resistant multifactor authentication (MFA) tool for all employee accounts. Company leadership declines, calculating that the enhanced MFA would be more costly than warranted in the near term, based on their judgment about the likelihood of a cyberattack. The decision is reviewed and approved by the board. Later, when an attacker tricks a user into revealing their login credentials, data is exfiltrated and systems are shut down by ransomware, with the following cascading impacts:

- Delayed shipment of critical pharmaceuticals, resulting in delayed surgeries across the country
- Theft of sensitive customer data, resulting in identity theft and personal financial impact to millions of customers
- Theft of critical intellectual property, eventually sold to an overseas company owned by an adversarial nation, which brings several competing drugs to market years ahead of schedule, with downstream effects on market share
- Over time, the US health care system begins to rely heavily on the overseas company for the pharmaceuticals, which ultimately damages US competitiveness and its leverage in the event of a geopolitical conflict

From a short-term business perspective, the financial impacts of the cyberattack are tolerable, though the company, which finds itself in the headlines over a period of several weeks, takes a reputational hit. In the longer term, however, the attack results in significant harm to individuals, other businesses, national economic competitiveness, and technological innovation.

> We need a new model of sustainable cybersecurity. One that starts with a commitment at the board level to incentivize a culture of corporate cyber responsibility in which managing cyber risk is treated as a fundamental matter of good governance and good corporate citizenship.

For decades, cyber risk was considered part of information technology (IT) risk, and its oversight was largely delegated to engineering and security teams within an organization. More recently, however, in large part thanks to the five principles highlighted in previous versions of this thoughtful handbook, corporate leaders have begun to see cyber risk for what it is: a strategic, enterprise risk, which they—not their CISOs—own. Today, given our complex, dynamic, and highly interconnected environment, boards and company leadership must now consider the broader picture and the critical role they play in their company's and in society's resilience.

We need a new model of sustainable cybersecurity. One that starts with a commitment at the board level to incentivize a culture of corporate cyber responsibility in which managing cyber risk is treated as a fundamental matter of good governance and good corporate citizen-

ship, a recognition highlighted in these pages with the inclusion of a sixth core principle for board oversight—the need for boards to encourage systemic resilience through collaboration.

Board members have unique power to drive such a culture of corporate cyber responsibility:

- They should ensure that CISOs are fully empowered, with the influence and resources necessary to drive decisions where cybersecurity is effectively prioritized, not subordinated to cost, performance, and speed to market.
- They should ensure that their peers and the senior executives that they oversee are well-educated on cyber risk, that cybersecurity considerations are appropriately prioritized in every business and technology decision, and that decisions to accept rather than mitigate cyber risks are scrutinized and revisited often.
- They should review their company's cyber-risk management framework and ensure the development of a common set of standards which their businesses can use to determine and measure their exposure to cybersecurity risk.
- They should ensure that the thresholds for reporting potential malicious activity to senior management are not set too high; rather, they should be briefed on "near misses" as well as those intrusion attempts that succeed, as such near misses are among the most important signals to assess the quality of a company's defenses and its reaction to incidents.
- Finally, board members should actively champion a model of collaboration that presumes a default position in which information about malicious activity is shared proactively with expectations that government will be responsive and add value, and that industry will not suffer punitive sanctions for sharing.

As the nation's cyber defense agency, CISA's goal is to advance a new model of sustainable cybersecurity by working collaboratively with our partners to drive down risk to our nation, enabling the broader safety of consumers. Since our establishment in 2018, CISA has been expanding our resources and capabilities, as well as growing our field forces around the country. You can read more about our offerings in Tool L, including how to have a probing conversation with your CISO so that you can better understand how to support the cybersecurity team.

CISA commends NACD and the Internet Security Alliance (ISA) for producing this handbook. Not only is it chock-full of clear and practical suggestions that will enable an organization to create a modern and comprehensive cyber-risk program, but also and more important: it works. As detailed within, Cybersecurity at MIT Sloan found that adopting the measures featured in this handbook would materially reduce cyber events without significantly increasing cost. Separately, this handbook is clear evidence that robust public/private operational collaboration is the pathway to creating a sustainably secure cyber ecosystem. In this fight, we are all on the same side and must work together.

Safer and more resilient critical infrastructure is possible, but it requires us to take deliberate ownership for our collective cyber defense. Corporate cyber responsibility must be a key pillar of this effort.

ENDNOTE

[1] See eSentire's discussion of the *2022 Official Cybercrime Report by Cybersecurity Ventures*. (https://www.esentire.com/resources/library/2022-official-cybercrime-report)

About the Handbook

In 2014, NACD, in conjunction with AIG and the Internet Security Alliance, published the first edition of the handbook. Subsequent editions addressed the shifting cyber-risk environment and reflected increased governance expectations from key stakeholders, including investors and regulators.

This handbook is one of the very few sets of board oversight practices in the cybersecurity field that has been independently assessed and found to generate important, improved, security outcomes. PwC's review of the handbook noted that use of the handbook was related to improved budgeting as well as improved cyber-risk management, closer alignment of cybersecurity with business goals, and the generation of a culture of security within the organization. A study by Cybersecurity at MIT Sloan (CAMS) conducted in 2022 used a different methodology and found that "the CEO who follows the consensus Cyber Risk Principles is predicted to have up to 85% fewer cyber incidents . . . compared to the traditional CEO," and that adopting the principles "can significantly improve . . . cyber resilience without raising costs."[1]

This fourth edition retains the previously identified five core principles for board oversight of cybersecurity, with associated guidance that has been updated considering the changing cyber threat landscape. However, this edition adds an important sixth principle that NACD and ISA developed in conjunction with the World Economic Forum in 2020. The expanded set of principles covered in the handbook follow:

1. Directors need to understand and approach cybersecurity as a strategic, enterprise risk, not just an IT risk.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on board meeting agendas.
4. Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework and reporting structure with adequate staffing and budget.
5. Board-management discussions about cyber risk should include identification and quantification of financial exposure to cyber risks and which risks to accept, mitigate, or transfer, such as through insurance, as well as specific plans associated with each approach.
6. Boards should encourage systemic resilience through collaboration with their industry and government peers and encourage the same from their management teams.

This edition of the handbook offers new guidance for each of the principles and includes an extensive toolkit section to help boards and management teams adopt the principles. The tools focus on the role a director has in overseeing cyber-specific issues such as addressing insider threats, incident response, and third-party risk management and offers guidance for understanding new methods that management teams are using to measure cyber risk in empirical and economic terms.

While some language in this handbook refers to public companies, these principles are applicable to—and important for—directors of organizations of all types and sizes, including members of private-company and nonprofit boards. Every organization has valuable data and related assets that are under constant threat from cybercriminals or other adversaries. No organization is immune.

The six principles for effective cyber-risk oversight detailed in this handbook are presented in a generalized form in order to encourage discussion and reflection by boards of directors. Boards are encouraged to adapt these recommendations based on their organization's unique characteristics, including size, life-cycle stage, strategy, business plans, industry sector, geographic footprint, and culture.

ENDNOTE

[1] Internet Security Alliance, "As Cyber Attacks Increase, Here's How CEOs Can Improve Cyber Resilience," isalliance.org, November 17, 2022. (https://isalliance.org/as-cyber-attacks-increase-heres-how-ceos-can-improve-cyber-resilience)

Introduction

Since the release of the third edition of this handbook in early 2020, companies have been embattled by the challenges of working from home to protect workforces from COVID-19, systemic cyberattacks such as the SolarWinds incident, and the economic ramifications of Colonial Pipeline's struggle with a ransomware actor, to name only a few headwinds. Despite these significant events in the cyber-threat landscape and challenges facing organizations, some board-level oversight practices stand the test of time. Boards of directors, with their attending fiduciary duties, continue to be responsible for overseeing management's strategy and their approach to enterprise-wide risk, and cybersecurity matters inherently span the enterprise.

As cybersecurity challenges grow, the board's duties may also expand, as regulators and rule makers in state and federal governments scrutinize the role of the board in oversight of information security risks—and boards are rising to the challenge to provide sound oversight in this realm. According to the *2022 NACD Public Company Board Practices and Oversight Survey*, 83 percent of boards have significantly improved their understanding of cyber risk compared with two years ago.[1]

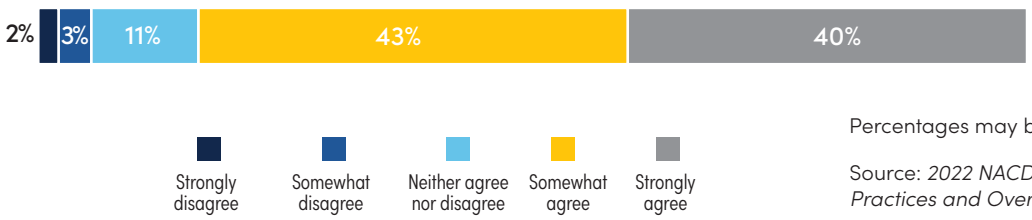
But directors do still feel the need for more expertise on boards. The survey also revealed an increase in boards' desire to recruit "cybersecurity-savvy directors," suggesting that while directors feel more confident in their understanding, boards are struggling to keep pace with overseeing the onslaught of changing cyber threats.

And keep pace they must, as the nature of corporate value also continues to shift away from the physical and toward the virtual. The rapid digitization of corporate assets has resulted in a corresponding transformation of strategies, business models, and attendant risks. Organizations are taking advantage of entirely new ways to connect with customers and suppliers, engage with employees, and improve the efficiency and effectiveness of internal processes. It has become a virtual necessity for most organizations to engage in digital transformation. The competitive need to deploy new and emerging technologies as a means to lower costs, improve customer service, and drive innovation is now felt more deeply by companies than ever before.

Adopting these technological innovations and capabilities may offer strong returns but can also increase cyber risk. They may also subject the organization to increased risk resulting from the loss of intellectual property such as trading algorithms, destroyed or altered data, decline in public confidence, and risk from evolving global regulatory sanctions that emerge in response to these incidents. In addition, attacks against organizations that are linked to critical infrastructure can result in a series of cascading consequences on other organizations in the supply chain that can lead to systemic risk. This edition of the handbook includes the adoption of a sixth principle, which highlights board members' responsibility to consider cyber risk in relation to the shared business ecosystem.

These competing pressures—competitive opportunity and potential risk exposure—mean that fiduciary and comprehensive oversight of cybersecurity at the board level is essential, requiring ongoing strategic dialogue with management.

FIGURE 1 MY BOARD'S UNDERSTANDING OF CYBER RISK TODAY HAS SIGNIFICANTLY IMPROVED, COMPARED TO TWO YEARS AGO.



Percentages may be +/- 100 due to rounding

Source: *2022 NACD Public Company Board Practices and Oversight Survey* (p. 6).

Surveys of global corporate leaders have consistently documented that, despite major efforts in recent years, cyber risk continues to be a growing concern that requires greater attention. According to the *2022 NACD Public Company Board Practices and Oversight Survey*,[2] business leaders rank changing cybersecurity threats among the top five topics that could impact their company in the coming year. Additionally, the World Economic Forum's *Global Risk Report 2023* again ranked cybersecurity failure and wide-spread cybercrime as top-ten critical global threats and as possible blind spots in risk perceptions.[3] The risk this year was the only technology risk that ranked in the top ten of a list of concerns dominated by environmental and societal risk categories.

The concerns of executives and board members the world over are warranted: the complexity of cyber threats has grown dramatically and continues to evolve. Corporations now face increasingly sophisticated threats that outstrip traditional defenses, and threat actors have become more diverse, including not only massive cybercriminal enterprises that are as sophisticated as major information security providers, but also ideologically motivated "hacktivists" and nation-states carrying out espionage campaigns. These diverse actors often collaborate, making assessment of cyber risk at all levels of the company more complicated.

Surveys of global corporate leaders have consistently documented that, despite major efforts in recent years, cyber risk continues to be a growing concern that requires greater attention.

WHAT'S ATTACKED AND WHY

One of the defining characteristics of cyberattacks is that they can penetrate virtually all of a company's perimeter defense systems, such as firewalls or intrusion-detection systems, and even access cloud-based data where companies are not directly managing security. Intruders look at multiple avenues to exploit all layers of security vulnerabilities, sometimes working patiently and covertly over months and years until they achieve their goals. The reality is that if a sophisticated attacker targets a company's systems, they will almost certainly breach them. As a result, modern cybersecurity practice goes beyond measures to keep the attackers out and includes methods utilized both to minimize impact and recover as quickly as possible.

In addition to the onslaught of attacks coming from outside of companies' lines of defense, insiders can become a threat to your company—intentionally or (most typically) by accident. While some third parties may prey on insecure systems (see Target's breach at the hands of an HVAC contractor), negligence or accidentally clicking on a phishing email link can account for other insider threats. This situation highlights the need for a strong and adaptable security program, equally balanced between external and internal cyber threats. Organizations cannot deal with advanced threats if they are unable to stop low-end attacks.[4]

Cyber extortion through ransomware attacks significantly increased as a key risk for organizations of all sizes in the COVID-19 era, but this risk will likely remain long after the world moves beyond the threat of COVID-19. (See Tool E–Incident Response.) Moreover, although many smaller and medium-sized companies have historically believed that they were too insignificant to be targets, that perception is wrong. One recent investigation found that 61 percent of small and medium-sized businesses had faced an attack in 2021.[5] Even before COVID-19, small and medium-sized businesses were the foremost victims. In addition to being direct targets, smaller firms are often an attack pathway into larger organizations via customer, supplier, or joint-venture relationships, making vendor and partner management a critical function for all interconnected entities.

CYBER THREATS BY THE NUMBERS

- Cybersecurity research statistics reveal that not only is the cybersecurity challenge stunningly large, but it is also growing massively on the global scale.
- Eighty-three percent of organizations reviewed in one study stated that their company has faced more than one breach before.[7] Sixty percent of these companies reported increasing prices to pass the cost of breaches along to customers.
- Global annual losses from cybercrime are estimated to reach $8 trillion in 2023 and are projected to rise to $10.5 trillion by 2025.[8]
- The United States is the costliest place in the world to face a breach.[9]
- According to one study by a penetration testing company, 93 percent of companies could be infiltrated by an outsider.[10]
- Email in 2022 was the primary point of entry for malware attacks.[11]
- The cost of credential theft increased from $2.8 million in 2020 to $4.6 million at the time that a study was published in 2022.[12]
- Ransomware attacks increased by 13 percent between 2020 and 2021—a larger jump than in the last five years combined.[13]
- On average, 2022 breaches were not detected until 207 days after the breach had occurred.[14]
- It typically took 70 days to contain a breach in 2022.[15]

No matter the perpetrator, the majority of cyber incidents are economically motivated.[6] Cyberattackers routinely attempt to steal, corrupt, or encrypt and hold hostage all manner of data. Typical targets include personal information, financial data, business plans, trade secrets, and intellectual property. However, any data of value or essential information system can be a target for a cyberattack.

THE ECONOMICS ARE EVOLVING

Cyberattackers generally have "first mover" advantage, meaning that cyber defenses tend to lag a generation behind the attackers. Why? The Internet was designed as an open system, which made the technology attractive as a means of innovation for companies and other enterprises. But the system itself was built without security in mind.

Meanwhile, the business model for cyberattackers is attractive. Bad actors can use the same attacks over and over across a worldwide list of targets, and the tools used in attacks can be relatively inexpensive or free to acquire—and highly profitable when executed properly. For example, a denial-of-service attack can be "outsourced" from a criminal provider or even acquired as a free, open-source tool found simply by searching for "DoS tool." One company's annual skim of the dark web found that the credentials to access a bank account with a minimum balance of $2,000 would set a small-time criminal back a mere $65.[16] At the scale of businesses, a hacker can purchase a distributed denial-of-service attack against premium protected websites for only $200.[17]

When it comes to defense, the economics is reversed. Information security is traditionally expensive, and it is difficult to demonstrate return on investment (ROI) for cyberattack prevention, but there is some hope: new tools and methods are emerging. A 2022 study conducted by IBM found that organizations that have implemented

a zero-trust architecture have an average of $1 million less in breach costs. The same study found serious returns on investment at companies that fully deployed security AI and automation, as well as incident response teams who were practiced and prepared to respond.[18]

There are costs and challenges associated with building and implementing a strong security program, and reporting and estimation on ROI is getting better every day. The sections covering Principles 4 and 5, as well as Tool F, describe how organizations can now perform more robust, empirical, and economics-based cyber-risk assessments as well as minimize the impact of successful breaches. By understanding cyber risk through the lens of ROI, organizations can better measure the impact of various attacks on their business. Such methods lead to a clearer calculation of the organization's cyber-risk appetite, which in turn supports the development of a more informed strategy and enhances the ability of the board to oversee security efforts. Board members need to ensure that management is fully engaged in making sure the organization's systems are as resilient and sophisticated as economically feasible and that they are apportioned to the risk.

Technologies such as mobile, cloud computing, and artificial intelligence can yield significant cost savings and business efficiencies, but they can also create major security concerns if implemented haphazardly.

BALANCING CYBERSECURITY WITH GROWTH AND PROFITABILITY

Like other critical risks that organizations face, cybersecurity cannot be considered in a vacuum. Members of management and the board must strike the appropriate balance between protecting the security of the organization and mitigating downside losses, while continuing to ensure profitability and growth in a competitive environment.

Many technology innovations and transformations that enhance profitability can also undermine security. For example, technologies such as mobile, cloud computing, and artificial intelligence, can yield significant cost savings and business efficiencies, but they can also create major security concerns if implemented haphazardly. Similarly, trends such as the move to remote work environments, on-demand access to data, Internet-of-Things integration, and the use of long, international supply chains may be so cost-effective that they are required in order for a business to remain competitive.

However, these practices can dramatically weaken the security of the organization. It is possible for organizations to defend themselves while staying competitive and maintaining profitability, but successful cybersecurity cannot simply be "bolted on" at the end of business processes. Security practices need to be woven into an organization's key systems, processes, strategy, and culture from end to end—and when done successfully, this integration can help organizations build competitive advantage.

To be effective, cybersecurity strategy must be more than simply reactive. Leading organizations must also employ an affirmative, forward-looking posture that includes generating intelligence about the cyber-risk environment and anticipating where potential attackers might strike, as well as subjecting their own systems and processes to regular, rigorous testing to determine vulnerabilities. As attackers adopt advanced technologies, organizations will need to employ the same capabilities to keep up with changing attack patterns.

ENDNOTES

[1] NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 6. (https://www.nacdonline.org/insights/publications.cfm?itemnumber=73754)

[2] NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 4. (https://www.nacdonline.org/insights/publications.cfm?itemnumber=73754)

[3] The World Economic Forum, *Global Risks Report 2023* (Geneva, Switzerland: World Economic Forum, 2023), p. 6. (https://www.weforum.org/reports/global-risks-report-2023)

[4] For more information, see IBM's *Cost of a Data Breach: A Million-Dollar Race to Detect and Respond* (IBM, 2022). (https://www.ibm.com/reports/data-breach)

[5] See Verizon's *2022 Data Breach Investigations Report*. (https://www.verizon.com/business/resources/reports/dbir/)

[6] See Verizon's *2022 Data Breach Investigations Report: Results and Analysis–Intro to Patterns*. (https://www.verizon.com/business/resources/reports/dbir/2022/results-and-analysis-intro-to-patterns/)

[7] See IBM's *Cost of a Data Breach 2022: A Million-Dollar Race to Detect and Respond*. (https://www.ibm.com/reports/data-breach)

[8] Steve Morgan, "Cybercrime to Cost the World 8 Trillion Annually In 2023," posted on cybersecurityventures.com on October 17, 2022. (https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/)

[9] See IBM's *Cost of a Data Breach 2022: A Million-Dollar Race to Detect and Respond*. (https://www.ibm.com/reports/data-breach)

[10] See Positive Technologies' *Business in the Crosshairs: Analyzing Attack Scenarios*. (https://www.ptsecurity.com/ww-en/analytics/pentests-2021-attack-scenarios/)

[11] See Verizon's *2022 Data Breach Investigations Report*. (https://www.verizon.com/business/resources/reports/dbir/)

[12] See the *2022 Ponemon Institute Cost of Insider Threats: Global Report*. (https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats#:~:text=The%20cost%20of%20credential%20theft,spend%20the%20most%20on%20containment)

[13] See Verizon's *2022 Data Breach Investigations Report*. (https://www.verizon.com/business/resources/reports/dbir/)

[14] See IBM's *Cost of a Data Breach: A Million-Dollar Race to Detect and Respond* (IBM, 2022). (https://www.ibm.com/reports/data-breach)

[15] Ibid.

[16] Privacy Affairs, "Dark Web Price Index 2022," privacyaffairs.com, September 19, 2022. (https://www.privacyaffairs.com/dark-web-price-index-2022/)

[17] Ibid.

[18] See IBM's *Cost of a Data Breach: A Million-Dollar Race to Detect and Respond* (IBM, 2022). (https://www.ibm.com/reports/data-breach)

PRINCIPLE ONE

Cybersecurity as a Strategic Risk

Historically, instead of individual departments and functions being responsible for the security of the data they handled, the responsibility for information security was given to IT: a department that in most organizations is strapped for resources and must fight for talent from a pool too small to cover the need—all while lacking budget authority. Further, deferring responsibility to IT inhibited critical analysis of and communication about security issues and hampered the adoption of effective, organization-wide security strategies.

Over the past several years, the business community's increased level of awareness of the importance of information security in general and the cross-functional nature of cybersecurity in particular have helped to break down siloes and operationalize management of cyber risks as strategic risks. A joint 2021 report from the World Economic Forum, NACD, and the Internet Security Alliance found that "cyber threats are a persistent strategic enterprise risk for all organizations regardless of the industry in which they operate."[1] Effective organizational cybersecurity directly contributes to strategic value preservation and new opportunities for long-term value creation.

Given the value sustaining and creating potential of embedding cybersecurity into all corners of the enterprise, boards are dedicating increased attention toward cyber-risk oversight practices. According to the *2022 NACD Public Company Board Practices and Oversight Survey*, more than 80 percent of board members surveyed either somewhat or strongly agreed that their understanding of cyber risk has "significantly improved" over the past two years.[2] This increased awareness and energy directed toward board-level cyber risk is evidence that board members and business leaders are confronting the challenges posed by digital and technological transformation.

Executives and board members now recognize that cybersecurity is an integral element in the critical and challenging transformations required of their organization to grow and compete in the digital age. The key questions for the board are no longer limited to how technological innovation can enable business processes, but how to balance digital transformation with effective management of cyber risks that may compromise long-term strategic interests. And the smartest companies are including cybersecurity by design as part of their strategic value proposition.

Proper oversight begins with understanding that cyber risk is not limited to narrow technical domains but stretches throughout the enterprise and directly impacts key business outcomes. This includes discussing how the organization will strike the right balance between protecting digital assets and driving digital innovation. In one recent study, 79 percent of CEOs said that investments in long-term value creation initiatives were supported by investors.[3] On the other side of the same token, institutional investors and proxy advisors have turned a keen eye on disclosures about cybersecurity controls and governance, and are expecting companies to mitigate cyber risks both as a strategic enabler and as a means to retain and continue long-term value creation.[4] Business leaders and boards are increasingly focused on the concept of long-term value maximization and recognize that this strategy is paired with near-term risks and the potential for missed opportunities.

Boards and management teams should acknowledge the potential tension between the need for strategic innovation—increasingly fueled by digital transformation—and the imperatives of preserving security and trust. Recognizing the high stakes of successful digital transformation, we believe that cybersecurity should now be viewed as a means for a company to execute its strategy—digital or not. At its best, cybersecurity enables organizations to create long-term value and sustain trust with their customers and other key stakeholders.

INTERNAL CYBERSECURITY STRATEGY AND MANAGEMENT

Boards should understand and review the cybersecurity strategy and management processes that are applicable to the sustainability of their organizations. Board members should know what data is most important for the company to protect and ensure that management has vetted and understands a clear plan to detect, respond, and recover from cyberattacks. While protection should start with the data most critical to the organization, boards should also ask management about the process for identifying, measuring, and inventorying cyber risks across the enterprise, including how they work across business verticals, to help identify material vulnerabilities. These less obvious risks can still pose great threats to the integrity and security of the business due to the interconnected nature of modern organizations.

As hybrid work, the use of public clouds, and increasingly interconnected supply chains become more prevalent, organizations need to be prepared to manage a wider set of security exposures. With emerging disruptive technologies such as AI and quantum computing on the horizon, it is becoming more critical for boards and management to continually evaluate the effectiveness of their cyberse-

DEFINING ZERO TRUST

The zero-trust architecture concept was popularized by Forrester Research in 2010.[5] It has since become a leading approach to cybersecurity being adopted across a variety of industries and has been endorsed by the federal government in Executive Order 14028, *Improving the Nations Cybersecurity*.[6] In a memorandum announcing that the US Government was moving toward zero trust cybersecurity principles, Shalanda D. Young, then acting director of the Office of Management and Budget, said that "the foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access."[7]

By removing implicit trust with all actors, organizations must emphasize the effectiveness and robustness of their identity and access-management programs to establish the necessary roles, information access, and credentialing to appropriately monitor and govern access across the enterprise.

curity. It is worth noting that emerging technologies and security challenges can be met with emerging cybersecurity best practices such as embracing and implementing zero-trust architecture. It's up to management to ensure that the adoption of the right approaches are paired with emerging technologies that will drive value creation. (For a definition of zero-trust architecture, see Sidebar, page 14).

In leading organizations, management teams and boards are starting to integrate the adoption of emerging technologies and data capabilities into discussions about key strategies that cut across the entire organization. Cybersecurity must be part of the same dialogue. Nearly a third of boards address cyber-risk oversight at the full-board level, rather than with specific committees or groups.[8] This evolution is consistent with the realization that cybersecurity should be seen as an enterprise-wide strategy- and risk-management issue that should be addressed holistically and proactively when the board is making major strategic decisions.

CYBER RISK AND THE BUSINESS ECOSYSTEM

Activities such as product launches or production strategies that use complex supply chains spanning multiple countries and regions can magnify cyber risk. Similarly, mergers and acquisitions regularly require the integration of complicated information systems, often on accelerated timelines, and without sufficient time allocated to perform comprehensive due diligence. Specific guidance for board members in these situations is provided in the tools in this handbook, and particularly in Tool G.

Another obstacle companies face in creating a secure system is the degree of interconnection that the organization's networks have with its partners, suppliers, affiliates, and customers. Several significant cyberattacks did not actually start within the target's IT systems, but instead resulted from vulnerabilities in one of their vendors' or suppliers' systems. Mitigating a risk such as this requires partnerships across management teams and various departments, who must pressure suppliers and vendors to provide increased transparency and security for their products and services.

In addition, organizations are adopting new ways to manage data, (e.g., having some data residing on external networks or in public clouds), which not only can improve cost-effectiveness and efficiency, but can also introduce new risks. The hybridized work culture that was created out of necessity during the COVID-19 pandemic has endured, as off-premises, cloud-centered business operations have gained a permanent foothold. By out-

KEY CONSIDERATIONS FOR THE BOARD

- ☐ Hardwire cyber-risk considerations into key operational and strategic decision-making processes, including the adoption of cyber risk as a recurring agenda item for full-board meetings.
- ☐ View each major new digital transformation initiative through the lens of cyber risk.
- ☐ Analyze cybersecurity issues with respect to their strategic implications and as part of the total enterprise risk exposure.
- ☐ Analyze business strategy and business-model considerations with respect to cybersecurity issues.
- ☐ Ask executives to identify opportunities to use cybersecurity as a market differentiator and business driver.

sourcing data storage, companies have limited their ability to secure the data on their own terms. Companies are subject to service-level agreements made in partnership with the cloud provider that merit careful due diligence against corporate security policies in the contract negotiation phase. Boards need to have sufficient oversight to determine that their management teams are monitoring these services and taking adequate risk-management steps, such as understanding and monitoring the security controls provided by the cloud provider and the results of any third-party audits. (For more on security in the cloud, see Tool K).

ENDNOTES

[1] World Economic Forum, Internet Security Alliance, and NACD, *Principles for Board Governance of Cyber Risk* (Arlington, VA: NACD, 2021), p. 7. (https://www.nacdonline.org/insights/publications.cfm?ItemNumber=71795)

[2] NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 6. (https://www.nacdonline.org/insights/publications.cfm?itemnumber=73754)

[3] EY, *The CEO Imperative: Will Bold Strategies Fuel Market-Leading Growth?* (EY, 2022), p. 7. (https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/ceo/ey-ceo-survey-global-report.pdf)

[4] Orla Cox and Hetal Kanji, "Building Effective Cybersecurity Governance," posted on the Harvard Law School Forum on Corporate Governance November 10, 2022. (https://corpgov.law.harvard.edu/2022/11/10/building-effective-cybersecurity-governance)

[5] See *No More Chewy Centers: Introducing the Zero Trust Model* (Forrester Research Inc., 2010). (https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf)
And for more information about the zero-trust security model in general, please see the background available on Wikipedia. (https://en.wikipedia.org/wiki/Zero_trust_security_model)

[6] President Biden, *Executive Order on Improving the Nation's Cybersecurity*, posted on whitehouse.gov, May 12, 2021. (https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/)

[7] See the Office of Management and Budget's Memorandum for the Heads of Executive Departments and Agencies: Moving the US Government Toward Zero Trust Cybersecurity Principles (M-22-09), issued January 26, 2022. (https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf)

[8] NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 7. (https://www.nacdonline.org/insights/publications.cfm?itemnumber=73754)

PRINCIPLE TWO

Legal and Disclosure Implications

Directors overseeing cybersecurity should be prepared to navigate a broad range of sophisticated and evolving legal and regulatory risks. Boards, individual board members, and relevant executive officers should stay informed about the current cyber threat environment, as well as the compliance and liability issues facing their organizations and the specific industries within which they operate.

WHO IS PAYING ATTENTION?

Cybersecurity requirements vary at the local, national, and global level and are constantly evolving. Key trends include more stringent and detailed requirements for cybersecurity programs and technical defenses; heightened governance standards and executive accountability for cyber risk management; proliferating requirements for rapid regulatory reporting of cybersecurity events; and increased legal penalties. Against this backdrop, regulators, plaintiffs' attorneys, the media, customers, and investors are all increasingly scrutinizing companies' approaches to cybersecurity.

Evolving regulatory cybersecurity standards are informing the risks around both enforcement and litigation. Regulators across the world have brought enforcement actions, and they have achieved settlements with record-breaking fines—as well as novel injunctive and equitable relief—in the wake of data breaches and data mismanagement. Litigation in the United States is trending toward rising settlements and novel legal theories, including some supported by new state privacy legislation with private causes of action and statutory damages, including from the California Consumer Privacy Act.

In 2021 alone, more than 45 US states and territories introduced their own cybersecurity legislation, with 36 states enacting bills in the same year.[1] In 2022, the Federal Trade Commission updated information security requirements under the Safeguards Rule; the US Department of Health and Human Services' Office of Civil Rights issued guidance on recognized security practices for HIPAA-cov-

ered entities and business associates; the US Securities and Exchange Commission (SEC) proposed expanded rules for investment advisors and funds; and the New York Department of Financial Services (DFS) proposed an amendment to its cybersecurity regulations. Each of these developments increased requirements on cybersecurity programs and governance, and some explicitly addressed governance issues. For example, the DFS proposal intends to further clarify the role of senior management and corporate boards in cybersecurity policy and governance.[2] As the examples above illustrate, each industry faces increasing requirements from US federal regulators.

> The trend indicates that lack of effective cybersecurity oversight and appropriate board structures, practices, and responsibilities presents an opportunity for both regulators and investors to target boards.

The possible adoption of one forthcoming rule spans most industries, while those proposed at other agencies would be narrower in focus. The SEC proposed a rule in 2022 that it claims would, if passed, "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting" by public companies.[3] The SEC's public company proposal would require that specific information about cybersecurity programs and the board's oversight activities as well as the board's cyber expertise be disclosed in registrants' 10-Ks and 10-Qs.[4] Further, Congress and the executive branch of the federal government made strides toward passing, adopting, or ordering cybersecurity policy in 2022—including through passing into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[5]

Meanwhile, investors have not shied away from initiating cyber-risk-focused suits. Consistent with the Delaware Chancery Court's precedent around "mission critical risks," investors have recently brought *Caremark* suits against companies that experienced cybersecurity incidents and breaches.[6] While the court dismissed one of the suits,[7] it stated that cybersecurity can rise to the level of mission-critical risks in certain circumstances, thus requiring greater involvement of the board in its oversight. The trend indicates that lack of effective cybersecurity oversight and appropriate board structures, practices, and responsibilities presents an opportunity for both regulators and investors to target boards.

Investors also expect companies to be transparent about their cybersecurity processes in public filings and disclosures. The Council of Institutional Investors, a group that represents public, union, and corporate benefit plans, endowments, and foundations, has stated that, "Investors will have greater confidence that [a] company is not withholding information if it proactively communicates the process by which it assesses damage caused by a cyber incident and the methodology it uses to account for cyber incidents affecting data and assets. Communicating such a process will not reveal sensitive information about a company's cybersecurity efforts."[8] In response, some public companies are increasing their voluntary disclosures—in the proxy statement and elsewhere—about how the board is educated on, informed about, and structured for cyber-risk oversight. (See Tool J—Enhancing Cybersecurity Disclosures: 10 Questions for Boards.)

Outside of the United States, jurisdictions are increasingly adopting their own cyber regulations, such as the recently updated European Union Network and Information Security Directive (NISD2); the EU Digital Operational Resilience Act (DORA); data security and breach requirements, such as the General Data Protection Regulation (GDPR); and implementing member state legislation. As these requirements are enacted, interpreted by a variety of regulators, and occasionally challenged in court, the definitions within them may evolve. For example, in August 2022, the European Union's top court expanded the definition of sensitive information under GDPR.[9] Some of these requirements include governance structures, rapid notification of incidents, oversight of third-party vendors, disclosure of material cyber risks, and adequacy of controls. A growing list of nations are enacting laws similar to GDPR, including Australia, Brazil, South Africa, Israel, India, Japan, Argentina, and Egypt among others.[10]

Challenges to oversight of disclosures and compliance in varying jurisdictions include overlapping and conflicting rules and requirements, lack of coordination among rulemaking and legislative authorities, and different priorities driving the development of new regulations—including divergent views on fundamental issues such as the trigger for a reportable breach, requirements for data localization (if any), the right to deletion or "the right to be forgotten," or standards for reasonable information security programs. While directors do not need to have deep knowledge about this increasingly complex area, they should be briefed on a regular basis by inside or outside counsel, as well as by other substantive cybersecurity experts, about requirements that apply to the company. Reports from management should enable the board to assess whether the organization is adequately addressing these regulatory and legal risks.

UNDERSTAND THE CONSEQUENCES

High-profile attacks may spawn lawsuits, including SEC enforcement actions concerning public companies or SEC registrants; or public-company shareholder-derivative suits accusing the organization of mismanagement, waste of corporate assets, and abuse of control. Plaintiffs may also allege that the organization's board of directors neglected its fiduciary duty by failing to take sufficient steps to confirm the adequacy of the company's protections against data breaches and their consequences. Exposures can vary considerably, depending on the organization's dependence on technology, and are often shaped by the data, sector, and operating locations associated with the exposure.

The US business judgment rule may protect directors in private litigation, so long as the board has performed and documented reasonable oversight before and during investigative steps following a cybersecurity incident. Additionally, the Delaware Chancery Court's decision in *SolarWinds* may protect board directors from *Caremark* allegations so long as the board delegates committees with the responsibility to report on cybersecurity risks.[11] But company officers and/or directors may nonetheless face SEC scrutiny as it concerns the implementation of policies and procedures required by the federal securities laws.

Aside from strong governance and adoption of the best practices outlined in this handbook, there are other practices that can shield organizations from the negative consequences of legal and regulatory enforcement actions. The lead director and corporate secretary should maintain records in appropriate detail of boardroom discussions about cybersecurity and cyber risks. (See the "Board Minutes" sidebar on this page). The board itself should be tasked with staying informed about industry-, region-, or sector-specific requirements that apply to the organization. And, most important, the board should work in advance to understand and plan for what must be disclosed in the wake of a cyberattack and the timeframe in which

BOARD MINUTES

Board minutes should reflect the occasions when cybersecurity was present on the agenda at meetings of the full board and/or of key board committees, depending on the allocation of oversight responsibilities. Discussions at these meetings that should be documented in board minutes might include updates about specific risks and mitigation strategies, as well as reports about the company's overall cybersecurity program and the integration of technology with the organization's strategy, policies, and business activities. Further, board minutes should reflect the disclosure of cybersecurity related incidents, including a summary of how and whether to make disclosures consistent with reporting requirements. Regulators are unable to credit good-faith discussion and oversight of this risk if there is no documentation that it happened. Board minutes are one tool for documenting just what was discussed and at what point in time—and one tool that may mean the difference between a painful lawsuit or an easier resolution.

such reporting is required to take place. It is also advisable for directors to participate with management in one or more cyberbreach simulations, or "tabletop exercises," to better understand their roles and the company's response process in the case of a serious incident.

THE EVOLUTION OF SEC REGULATION

In 2018, the SEC unanimously approved interpretative guidance updating a similar publication released in 2011 by the Commission's Division of Corporate Finance. The update outlined guidance for publicly traded companies to disclose cybersecurity risks and material incidents, underscoring that cyber risks "pose grave threats to investors, our capital markets, and our country."[12] In a statement, former SEC Chair Jay Clayton urged companies "to examine their controls and procedures," not only to conform with securities law disclosure obligations but also keeping in mind financial and reputational considerations.[13] The guidance focused on the following core areas:

- **Pre-incident disclosure:** The SEC called for transparency around the identification, quantification, and management of cyber risk.
- **Board oversight:** The board's responsibility is to understand cyber risk and oversee it. The SEC advised companies to disclose, as part of their proxy statement, the board's role and engagement in cyber-risk oversight, and noted that the discussion "should include the nature of the board's role in overseeing the management of [cyber] risk."
- **Incident disclosure:** The SEC guidance urged companies to "inform investors about material cybersecurity risks and incidents in a timely fashion," yet it did not define parameters for materiality determination or how long a company could take to disclose the materiality of the incident to investors.
- **Controls and procedures:** The guidance stated that companies are expected to assess whether their enterprise-wide risk management processes are sufficient to safeguard the organization from cyber disasters.
- **Insider trading:** The SEC reminded directors, officers, and other relevant parties who are aware of a company's cyber vulnerabilities or a breach that they could be held liable for insider trading violations if they sell company stock, or instruct anyone else to do so, before such a breach or vulnerability is divulged.

This case reflects the importance of implementing a corporate governance protocol designed to ensure proper reporting channels on all issues, including those related to cybersecurity.

Since this guidance was released and the leadership of the SEC has changed hands, the agency has watched voluntary corporate disclosures and has taken actions against those who were not following guidance. In June 2021, the SEC announced a settled enforcement action against a company for disclosure controls and procedures violations related to a cybersecurity vulnerability.[14] Specifically, the SEC claimed that while the company furnished a Form 8-K detailing a cybersecurity event, the company's senior executives responsible for the public statements "were not apprised of certain information that was relevant to their assessment of the company's disclosure response. . . . " This case reflects the importance of implementing a corporate governance protocol designed to ensure proper reporting channels on all issues, including those related to cybersecurity. Similarly, in August 2021, the Commission announced a settled enforcement action against another public company for misleading investors about a cyberbreach.[15]

The SEC's focus on these matters is expected to increase going forward, and in 2022 the agency upped the ante

with proposed rules focused on standardizing disclosure practices because, according to the SEC, "disclosure practices are inconsistent" since the 2018 guidance was issued.[16] The proposed rules would make the following disclosure requirements:[17]

- Require current reporting about material cybersecurity incidents in SEC Form 8-K.
  - Reporting must be completed within four days of the company determining that the incident was material in nature.
  - Further disclosures are required if other incidents tied to the first reporting are deemed to make a larger collection of incidents material in aggregate.
- Require periodic disclosures regarding, among other things,
  - a registrant's policies and procedures to identify and manage cybersecurity risks;
  - management's role in implementing cybersecurity policies and procedures;
  - board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk; and
  - updates about previously reported material cybersecurity incidents.
- Require the cybersecurity disclosures to be presented in InLine eXtensible Business Reporting Language.

Although a final order on these proposals is not expected until mid-2023 at earliest and may change in scope from the proposed rule, the SEC's proposal reflects what it believes are the practices needed "to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents."[18] Consequently, companies should consider whether their current policies and procedures and their overall corporate governance structure would enable prompt and accurate disclosures if these rules are adopted by the Commission.

KEY CONSIDERATIONS FOR THE BOARD

- ☐ Board members should carry out regular sessions on legal, regulatory, or contractual trends and recent developments in cybersecurity.
- ☐ Consider whether any new business endeavors or partnerships generate new and differing legal obligations.
- ☐ Consider whether oversight responsibility for cybersecurity should reside with the full board or with a board committee.
- ☐ Consider whether the board has access to appropriate cyber expertise, either through its own composition or via access to management experts, consultants, and legal advisers, or a combination of these resources and assets.
- ☐ Ensure that management has developed the appropriate level of relationships and line of communications with relevant regulatory and enforcement entities.
- ☐ Ensure that the internal legal team has relationships with outside counsel to aid in special events such as incident response. Define the governance structure for disclosing material risks and actual incidents to regulatory authorities.
- ☐ Periodically review with management the information systems and controls related to cyber risks.

ENDNOTES

[1] National Conference of State Legislatures, Cybersecurity Legislation 2021, ncsl.org, Updated July 1, 2021. (https://www.ncsl.org/technology-and-communication/cybersecurity-legislation-2021)

[2] Wilmer Cutler Pickering Hale and Dorr LLP, "NYDFS Proposes a Second Amendment to its Cybersecurity Regulations" *Insights Blog*, wilmerhale.com, November 17, 2022. (https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/11172022-nydfs-proposes-a-second-amendment-to-its-cybersecurity-regulations)

[3] See SEC Fact Sheet 33-11038, *FACT SHEET Public Company Cybersecurity: Proposed Rules*, p. 1. (https://www.sec.gov/files/33-11038-fact-sheet.pdf)

[4] Sidley Austin LLP, "Newly Proposed SEC Cybersecurity Risk Management and Governance Rules and Amendments for Public Companies," *Data Matters Blog*, datamatters.sidley.com, March 11, 2022. (https://www.sidley.com/en/insights/newsupdates/2022/03/newly-proposed-sec-cybersecurity-risk-management-and-governance-rules)

[5] Cyber Incident Reporting for Critical Infrastructure Act of 2022, H.R. 2471, 117th Cong. (2022). (https://www.congress.gov/117/plaws/publ103/PLAW-117publ103.pdf)

[6] See https://cases.justia.com/delaware/supreme-court/2019-533-2018.pdf?ts=1560880896.

[7] Constr. Indus. Laborers Pension Fund v. Bingle, C.A. No. 2021-0940-SG (Del. Ch. Sept. 6, 2022) (SolarWinds). (https://courts.delaware.gov/Opinions/Download.aspx?id=337580)

[8] Council of Institutional Investors, *Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards* (April 2016), p. 5. (https://www.cii.org/files/publications/misc/4-27-16%20Prioritizing%20Cybersecurity.pdf)

[9] Catherine Stupp, "EU Court Expands Definition of Sensitive Data, Prompting Legal Concerns for Companies," *WSJ Pro Cybersecurity*, August 10, 2022. (https://www.wsj.com/articles/eu-court-expands-definition-of-sensitive-data-prompting-legal-concerns-for-companies-11660123800?mod=djemCybersecruityPro&tpl=cy)

[10] DLA Piper, "Data Protection Laws of the World," dlapiperdataprotection.com, accessed January 2023. (https://www.dlapiperdataprotection.com/)

[11] See *SolarWinds*, C.A. No. 2021-0940-SG (Del. Ch. Sept. 6, 2022) (holding that bad faith is not established where a cyber breach occurs in spite of a Board's subcommittee presentation of cybersecurity risk so long as that committee is not a "sham" committee); *In re Caremark Int'l Derivative Litig.* 698 A.2d 959 (Del. Ch. 1996).

[12] See the SEC's *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (p. 1), applicable February 26, 2018. (https://www.sec.gov/rules/interp/2018/33-10459.pdf)

[13] See the public statement by Chair Jay Clayton, "Statement on Cybersecurity Interpretive Guidance," February 21, 2018. (https://www.sec.gov/news/public-statement/statement-clayton-2018-02-21)

[14] US Securities and Exchange Commission, "SEC Charges Issuer with Cybersecurity Disclosure Controls Failures," press release no. 2021-102, June 15, 2021. (https://www.sec.gov/news/press-release/2021-102)

[15] US Securities and Exchange Commission, "SEC Charges Pearson plc for Misleading Investors About Cyber Breach," press release no. 2021-154, August 16, 2021. (https://www.sec.gov/news/press-release/2021-154)

[16] See SEC Fact Sheet 33-11038, *FACT SHEET Public Company Cybersecurity: Proposed Rules*, p. 1. (https://www.sec.gov/files/33-11038-fact-sheet.pdf)

[17] Ibid.

[18] See SEC Fact Sheet 33-11038, *FACT SHEET Public Company Cybersecurity: Proposed Rules*, p. 1. (https://www.sec.gov/files/33-11038-fact-sheet.pdf)

PRINCIPLE THREE

Board Oversight Structure and Access to Expertise

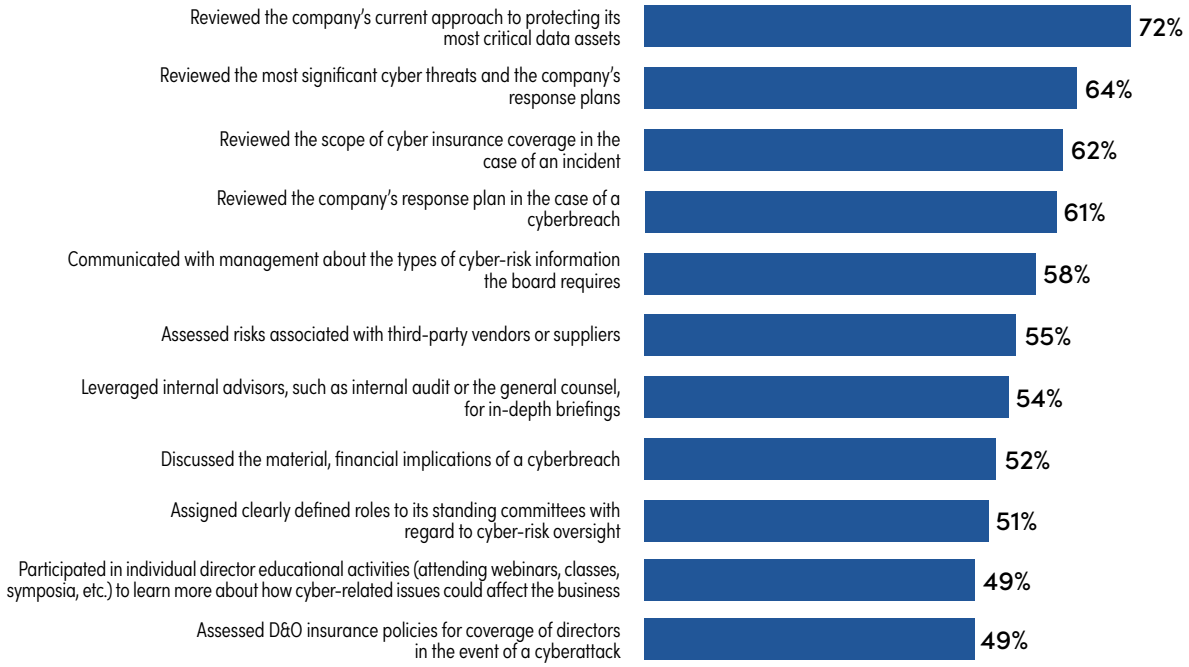
Given the strategic importance of cybersecurity and the breadth of threats facing organizations, directors need to move beyond merely understanding that threats exist and receiving related reports from management. Rather, boards need to employ the same principles of inquiry and constructive challenge that are standard features of board-management discussions about strategy and company performance and include cybersecurity oversight into boardroom operations planning.

As a director at an NACD forum hosted in 2014 observed, "Cyber literacy can be considered similar to financial literacy. Not everyone on the board is an auditor, but everyone should be able to read a financial statement and understand the financial language of business." Nearly a decade later, this statement continues to ring true, and boards are working hard to walk the walk. As discussed in Principle One, leading boards now understand that cybersecurity is not a discussion item to be addressed for a few minutes at the end of a board meeting. Rather, cybersecurity is an essential element of board-level oversight and needs to be integrated into early discussions about issues such as mergers, acquisitions, new product development, and strategic partnerships.

In the annual NACD survey of public company directors, 83 percent of respondents indicated that they believe that their board's understanding of cyber risk has significantly improved compared to two years ago.[1] Most boards have reviewed their company's response plans, received briefings from internal advisors, reviewed the company's data privacy protections, and communicated with management about cyber-risk oversight over the past year. More than 70 percent of boards reviewed their company's current approach to securing its most critical assets against cyberattacks within the past year. (See Figure 2, page 24.)

Boards and directors are elevating their understanding and education around the topic of cybersecurity, but there still exists a disparity between the board's ability and understanding and that of management that slows enterprise-wide oversight of cyber risks. To bridge this gap, boards need to access information provided not only from IT and technical operations but from a wide range of sources, including human resources, finance, public relations, legal/compliance, and others. Several models for soliciting a wide range of perspectives and inputs are discussed in Principle Four.

FIGURE 2 CYBER-RISK OVERSIGHT PRACTICES BY THE BOARD.



Source: *2022 NACD Public Company Board Practices and Oversight Survey*[2]

HOW CAN BOARDS ACCESS THE CYBERSECURITY INFORMATION THEY NEED?

There is no single approach that will fit the cyber-risk oversight needs of every company and board, but there are some common best practices for obtaining, understanding, and using the information needed. From the time that a board member joins a new board or committee, their onboarding process should include cybersecurity-specific briefings relevant to the oversight role they are serving. To bring a new director up to speed on the state of cybersecurity within the organization, as well as the board's oversight approach, the board can take these steps:

- Schedule a one-on-one briefing between the new director and the organization's chief information security officer (CISO) or equivalent officer responsible for cybersecurity.
- Provide a walk-through of the board's cybersecurity and crisis response playbooks.
- Have the new director attend a relevant committee's meeting, if the company has delegated cyber risk to a specific committee.
- Provide a vetted list of conferences, industry trade shows, and educational classes or certifications that other board members have found useful in elevating their knowledge of cybersecurity.
- A board can also schedule time with the new director and the relevant committee chair for an in-depth discussion on the specific areas of cybersecurity oversight mandated by the committee's charter.

Full-board operations will vary based on the organization's type, their cyber-risk oversight needs, and how they wish to operate within the confines of their charters. Some boards choose to conduct all cyber-risk-related discussions at the full-board level; others assign specific cybersecurity-related oversight responsibilities to one or more committees (audit, risk, technology, etc.); and still others use a combination of these methods. According to a 2022 NACD survey of publicly traded company directors, 47 percent of boards delegate cybersecurity

oversight tasks to the audit committee, while 32 percent oversee the risk as a full board and 13 percent delegate it to a risk committee.[3]

Whichever the operational model chosen by the board, clear expectations should be set with management about the format, frequency, and level of detail of the cybersecurity-related information the board wishes to receive. This should begin with using the cybersecurity expertise within the company to enhance directors' knowledge. For example, the organization's CISO, or other senior management official responsible for overseeing security, can help the board to better understand cybersecurity via regularly scheduled briefings and meetings. This leader will be able to bridge high-level strategic goals and metrics with board-appropriate information about the company's security approach.

While the board looks to these leaders for information, it is still the director's job to practice healthy skepticism. Directors should be aware of inherent bias on the part of management to downplay the true state of the risk environment—especially if they are not being held accountable to an objective and comprehensive enterprise risk management framework and reporting structure. (For more on this matter, see Principle 4.) Directors who build a strong relationship with their CISOs should look to the executive for help, and should trust, but verify, their statements and assessments.

The nominating and governance committee should ensure that the board's chosen approach is clearly defined in committee charters to avoid confusion or duplication of efforts. Committees with designated responsibility for risk oversight—and oversight of cyber-related risks in particular—should receive briefings on at least a quarterly basis. Depending on the board's cyber-risk oversight approach, the full board may also be briefed, no less often than once a quarter and as specific situations warrant.

In order to encourage knowledge-sharing and dialogue, some boards invite all directors to attend committee-level discussions on cyber-risk issues, or make use of cross-committee membership. For example, one global company's board-level technology committee includes directors who are experts on privacy and security from a customer perspective. The audit and technology committee chairs are members of each other's committees, and the two committees hold a joint meeting once a year for a discussion that includes a deep dive on cybersecurity.

Effective boards approach oversight of cybersecurity as an enterprise-wide risk-management issue. While including cybersecurity as a stand-alone item on board and/or committee meeting agendas is now a widespread practice, the topic should also be integrated into a wide range of issues to be presented to the board, including discussions of new business plans and product offerings, mergers and acquisitions, new market entry, deployment of new technologies, major capital investment decisions such as facility expansions or IT system upgrades, and the like. As corporate assets have increasingly become digital assets, virtually all major business decisions before the board will have cybersecurity components to them.

While the board looks to these leaders for information, it is still the director's job to practice healthy skepticism.

Management's reporting to the board on relevant cybersecurity matters should be flexible enough to reflect both the changing threat environment and evolving company circumstances and board needs. A brief of an NACD risk oversight advisory council highlighted several factors that may determine how management engages the board, including the maturity of the information security program, whether the engagement occurs during a "steady" state vs. after an incident, shifting regulatory requirements, and director tenure and expertise.[4]

Directors may refer to the tools at the end of this handbook to explore recommendations for how to approach key issues related to cybersecurity oversight, ranging from how to address issues related to crisis management (including incident response) to evolving security challenges, such as supply-chain risks and insider threats.

Boards should consider augmenting their in-house expertise by using a variety of methods to integrate independent expert assessments.

Those methods include these:

- Scheduling deep-dive briefings or examinations from independent and objective third-party experts validating whether the cybersecurity program is meeting its objectives
- Leveraging the board's existing independent advisors, such as external auditors and outside counsel, who will have a multi-client and industry-wide perspective on cyber-risk trends
- Participating in relevant director-education programs, whether provided in-house or externally
  - Many boards are incorporating a "report-back" item on their agendas to allow directors to share their takeaways from outside programs with fellow board members.

THE QUESTION OF ADDING A "CYBER EXPERT" TO THE BOARD

How best to organize the board to carry out oversight of cyber risk—and, more broadly, enterprise-level risk oversight—is a matter of considerable debate. The *Report of the NACD Blue Ribbon Commission on Adaptive Governance* recommended that cybersecurity, along with other disruptive risks, "[should] be a component of strategy discussions at the full-board level and may also appear on the agenda of key committees, depending on the way in which risk-oversight responsibilities are allocated."[5] As noted earlier in this principle, 47 percent of surveyed companies said that cybersecurity oversight was allocated to the audit committee—the committee which most often oversees complex audits of financial and compliance matters. As the mandate of this committee expands, organizations are seeking other means for oversight of this risk.

Some companies in recent years have considered whether to add cybersecurity and/or IT security expertise directly to the board via the recruitment of new directors. According to the *2022 NACD Public Company Board Practices and Oversight Survey*, 43 percent of surveyed companies displayed ambivalence about recruiting a cyber-savvy director to their board, while 42 percent either agreed or strongly agreed that adding this expertise would be worth-

SHOULD YOU HAVE A CYBER EXPERT ON THE BOARD?

Questions to Consider

- How are we defining a "cyber expert"? The first principle in this handbook is that cybersecurity is not simply an "IT" issue, but rather an enterprise-wide risk-management issue. So, is the board looking to add an expert in enterprise-wide cybersecurity issues? A former CISO? Consider the company's needs and strategy and align accordingly.
- Is this strategy really deferring to one individual a responsibility that the full board should undertake? Might it be more appropriate for the full board to increase their understanding of cybersecurity systems in a way that is similar to the understanding that non-lawyers and nonfinancial experts have of these systems?
- How does having a single cyber expert on the board mesh with the cross-functional cyber-management structures that are becoming increasingly common? (Consider reviewing the "Three Lines of Defense" model discussed on page 31.)
- Does placing a cyber expert on the board set a precedent for assigning seats to other specialized oversight areas?

while.[6] If the US Securities and Exchange Commission's proposed rule on cybersecurity is passed as it stood at the end of 2022, companies may be compelled by regulation to recruit someone with cybersecurity expertise onto their board. Leaving aside that there simply are not enough "cyber experts" to populate every board, and hence the degree of expertise among board candidates may vary considerably, there are several questions posed in the sidebar titled "Should You Have a Cyber Expert On the Board?" on page 27 that a board should consider before opting for this strategy.

KEY CONSIDERATIONS FOR THE BOARD

- ☐ Establish key cybersecurity structures, committee assignments, and a cadence for review of information, and ensure that cybersecurity oversight is a topic integrated into the onboarding of new directors.
- ☐ Ensure that the board has access to the appropriate expertise from inside and outside the company to help it perform oversight duties with confidence.
- ☐ Establish an organization-wide culture of cybersecurity culture from the boardroom and encourage collaboration across all stakeholders relating to and accountable for cyber risks.
- ☐ Take great care when considering the addition of a cybersecurity expert to the board to ensure that this person doesn't become the sole repository for cyber-risk oversight.

ENDNOTES

[1] NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 6. (https://www.nacdonline.org/insights/publications.cfm?itemnumber=73754)

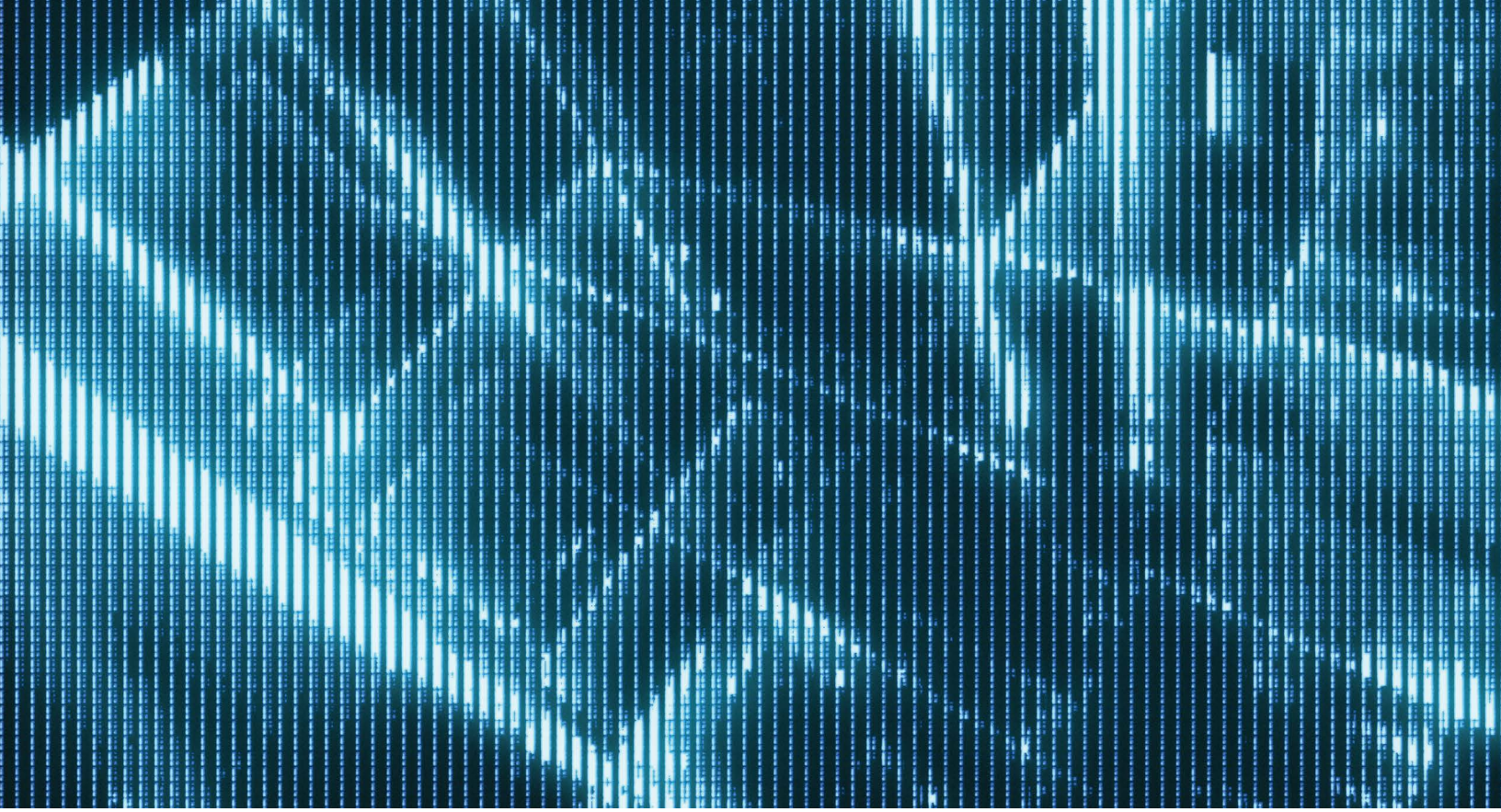
[2] Ibid.

[3] NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 7. (https://www.nacdonline.org/insights/publications.cfm?itemnumber=73754)

[4] NACD, *NACD Risk Oversight Advisory Council: Current and Emerging Practices in Cyber-Risk Oversight* (Arlington, VA: NACD, 2019). (https://www.nacdonline.org/insights/publications.cfm?ItemNumber=65591)

[5] NACD, *Report of the NACD Blue Ribbon Commission on Adaptive Governance* (Arlington, VA: NACD, 2018), p. 13. (https://www.nacdonline.org/insights/publications.cfm?ItemNumber=61319)

[6] NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 6. (https://www.nacdonline.org/insights/publications.cfm?itemnumber=73754)



PRINCIPLE FOUR

An Enterprise Framework for Managing Cyber Risk

In order for boards to engage in effective oversight of cyber risk, they need to fully understand the responsibilities that lie in the hands of management. As digital technologies increasingly underpin growth strategies, management has taken on the role of deploying, managing, and securing new digital capabilities across the organization. However, cyber-risk reporting structures and decision-making processes continue the legacy of siloed operating models. Management can no longer afford simply to delegate cyber-risk management to IT, or to each department and business unit independently.

Directors should seek assurances that management is taking an appropriate, enterprise-wide approach to managing cybersecurity risk. Specifically, boards should assess whether management has established both an enterprise-wide *technical framework* as well as a *management framework* that will enable effective governance of cyber risk. An integrated risk model should consider cyber risk not just as a technical problem unique and separate from other business risks, but rather as part of a comprehensive, enterprise-risk management program.

THE TECHNICAL FRAMEWORK

Complexity is an inherent feature of modern digital technology systems. As business and competitive pressures change, organizations demand that these complex systems be continually adapted and updated. This could mean adopting emerging technologies such as artificial intelligence (AI) and machine learning (ML), cloud, blockchain, the Internet of Things, or quantum computing to improve business practices and unleash innovation and growth. (See Tool K and Tool N for more on emerging technologies.) Directors cannot be expected to fully track and understand all these technologies and their implications for cyber risk. However, boards should expect from management that they implement and use the appropriate technical cybersecurity framework to defend company digital technology systems that the enterprise has come to rely on.

These frameworks vary in levels of granularity, as they list best practice activities along the various steps of the cyber-risk management process.

Multiple technical frameworks have been developed by various standards and industry organizations and act as sets of best cybersecurity practices. These frameworks vary in levels of granularity, as they list best practice activities along the various steps of the cyber-risk management process. Some organizations choose to adopt a single technical cybersecurity framework, while others will select specific aspects of various frameworks and adapt them to their unique business needs.

Once a cybersecurity framework has been adopted by the organization, directors should request regular updates from management on the progress made in implementing the selected set of best practices. Various tools have emerged that can help organizations demonstrate progress in implementing a cybersecurity framework:

- Some tools are more focused on technical implementation, helping track the progress of implementing various technical best practice activities along various scales of maturity and deployment.
- Other financially oriented tools measure the effectiveness of those best practices in reducing risk and can be used to prioritize those risks based on business impact.
- Greater detail on cybersecurity management and reporting is discussed in Principle Five.
- Here are some of the most used technical frameworks that management can select, adopt, and adapt:
- The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) "consists of standards, guidelines, and best practices to manage cybersecurity risk."[1] The NIST CSF's risk management process includes five key functions (identify, protect, detect, respond, and recover) and more than one hundred cybersecurity best practice activities.
- The International Organization for Standardization (ISO) created the ISO/IEC 27000 family of standards as a series of best practices to help organizations improve their information security through security controls within the context of an overall Information Security Management System, similar in design to management systems for quality assurance.[2]
- The Center for Internet Security's CIS Critical Security Controls include a list of 18 security controls with a prioritized set of actions to protect organizations and data from cyberattack vectors. These controls range from establishing an inventory of enterprise and software assets to incident response management and penetration testing.[3]
- The 15 PCI Security Standards by the PCI Security Standards Council are a set of best practices designed to help organizations "protect payment account data throughout the payment lifecycle and to enable technology solutions that devalue this data and remove the incentive for criminals to steal it."[4]

ESTABLISHING A MANAGEMENT FRAMEWORK FOR CYBERSECURITY

Principle One stressed the importance of viewing cybersecurity as a strategic and integrated enterprise risk. Directors should expect the implementation of an effective management framework for cybersecurity that requires the involvement of all relevant stakeholders across multiple business functions to ensure that all proper cyber-risk management activities are covered. While each organization will have unique operations, functions, and departments to account for, some examples of enterprise functions that can be part of a holistic cyber-risk management program follow.

- **Information Technology.** While this department covers many functions, information security in many organizations falls under IT. The security function is tasked with protecting the organization through the gathering of threat intelligence and the implementation of cybersecurity controls.
- **Risk.** Many organizations also have a risk function. This part of the organization is tasked with assessing its top cyber risks and insuring against catastrophic events.
- **Legal.** The legal department or outside counsel can help organizations address regulatory and shareholder obligations and concerns related to cyber risks.
- **Line-of-Business Executives.** The heads of research/development and of marketing and other line-of-business executives may also need to be represented. They are critical to cyber-risk mitigation as they plan to launch new digital products and need to understand how to achieve the right balance between enabling better, value-driving, customer experiences and protecting the business.
- **Finance.** The finance team likewise has a role to play as businesses assess the level of risk that they can tolerate versus the cybersecurity investments needed to protect important assets. Finance may also play a critical role in assessing the financial impact and materiality of potential or actual cybersecurity events.

No one cyber-risk model representing various functions and stakeholders will apply perfectly to all organizations. Recognizing that organizations will want to tailor their approach to fit their needs, we offer two different models which can be used as a starting point.

ISA–ANSI INTEGRATED APPROACH TO MANAGING CYBER RISK

One of the first multi-stakeholder models developed was created by the Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) in their joint 2008 publication, *The Financial Management of Cyber Risk: 50 Questions Every CFO Should Ask*.[5] This basic model stresses not only that multiple stakeholders ought to be involved in cyber-risk oversight, but also advocates for an identified leader—not from IT—who has cross-organizational authority. It also advocates for a separate cybersecurity budget as opposed to the traditional model of folding cybersecurity into the IT budget. The ISA-ANSI framework outlines the following seven steps:

1. Establish ownership of cyber risk on an inter-departmental basis. A senior manager with inter-departmental authority, such as the chief financial officer, chief risk officer, or chief operating officer (not the chief information officer) should lead the team.
2. Appoint an organization-wide cyber-risk management team. All substantial stakeholder departments must be represented, including business unit leaders, legal, internal audit and compliance, finance, human resources, IT (including information security), and risk management. If these roles do not exist in the organization, then their equivalents, or the appropriate designees, should be included.
3. The cyber-risk team needs to perform a forward-looking, enterprise-wide risk assessment, using a systematic framework that accounts for the complexity of cyber risk—including, but not limited to, regulatory compliance.
4. Be aware that cybersecurity regulation differs significantly across jurisdictions (among US states, between the United States and other countries, and from industry to industry). As noted in Principle 2, management should dedicate resources to tracking the standards and requirements that apply to the organization, especially as some countries aggressively expand the scope of government involvement into the cybersecurity arena.

5. Take a collaborative approach to developing reports for the board. Executives should be expected to track and report metrics that quantify the business impact of cyber threats and associated risk-management efforts. Evaluation of cyber-risk management effectiveness and the company's cyber resiliency should be conducted as part of quarterly internal audits and other performance reviews.
6. Develop and adopt an organization-wide cyber-risk management plan and internal communications strategy across all departments and business units. While cybersecurity obviously has a substantial IT component, all stakeholders need to be involved in developing the corporate plan and should feel that they have "bought in" to it. Testing of the plan should be done on a routine basis.
7. Develop and adopt a comprehensive cyber-risk budget with sufficient resources to meet the organization's needs and risk appetite. Resource decisions should consider the severe shortage of experienced cybersecurity talent and identify what needs can be met in-house versus what can or should be outsourced to third parties. Because cybersecurity is important across the enterprise, the budget for cybersecurity should not be exclusively tied to one department. Allocations for cybersecurity should be made in such areas as employee training, tracking legal regulations, public relations, product development, and vendor management.

THREE LINES MODEL

A conceptual model for cybersecurity was created by the Institute for Internal Audit in 2013 called the Three Lines of Defense Model. The model, updated in 2020, stresses multiple independent functions within the organization having separate and complementary roles in assessing, managing, and governing risk.[6] The update eliminated the term "Defense" from its title, an indicator that the current model is focused more on the opportunities and value potential posed by risks.[7] The Three Lines Model moved beyond three defined lines of risk management and instead adopted a principle-based approach inclusive of governance structures.

In the first line, management owns the risk design, implements operations, and maintains a constant dialogue with the management lead for cybersecurity (typically the CISO). Each business line defines the cyber risk they face and weaves cyber risk into risk, fraud, crisis management, and resiliency processes.

Line two defines policy statements and the risk-management framework. It provides a credible challenge to line one and is responsible for evaluating risk exposure, so that the board can determine risk appetite. Line two should be established as a separate, independent function under management and should maintain communication with both the cyber-risk lead and internal audit.

Line three is internal audit. It is responsible for independent evaluation of both line one and line two, including assessment of roles and processes across lines one and two.

The current model identifies six key principles that were not included in the previous model:

1. Have the right structures and processes in place to ensure that cyber risk is appropriately managed through governance.
2. Ensuring that responsibility for cyber risk is appropriately delegated by the governing body and that management has the tools it needs.
3. Management's role is within both lines one and two. Second line roles can be assigned to specialists (e.g., a penetration tester) to challenge the first line.
4. Internal audit provides assurance and advice on the adequacy and effectiveness of governance and risk management.
5. The internal audit's independence is critical to its objectivity, authority, and credibility.
6. There must be collaboration among all roles to ensure success.

KEY CONSIDERATIONS FOR THE BOARD

- ☐ Boards should expect management to incorporate cyber risk into an enterprise risk-management approach.
- ☐ In order to provide full oversight of cyber risks, management should adopt both technical and management frameworks.
- ☐ There are several technical and management frameworks that can be adopted and adapted to the unique needs of an organization.

ENDNOTES

[1] National Institute of Standards in Technology, "Cybersecurity Framework: Framework Documents," posted on nist.gov in April 2018. (https://www.nist.gov/cyberframework)

[2] International Organization for Standards, "ISO/IEC 27000:2018," posted on iso.org in February 2018. (https://www.iso.org/standard/73906.html)

[3] Center for Internet Security, "The 18 CIS Critical Security Controls," posted on cisecurity.org. (https://www.cisecurity.org/controls/cis-controls-list)

[4] PCI Security Standards Council, "Standards Overview," posted on pcisecuritystandards.org. (https://www.pcisecuritystandards.org/standards/)

[5] ANSI and ISA, *The Financial Management of Cyber Risk* (ANSI, 2008). (http://isalliance.org/publications/1A.%20The%20Financial%20Impact%20of%20Cyber%20Risk-%2050%20Questions%20Every%20CFO%20Should%20Ask%20-%20ISA-ANSI%202008.pdf)

[6] Thomas Holland and Stacey Floam, "Three Lines of Defense: A New Principles-Based Approach," posted on guidehouse.com on February 10, 2021. (https://guidehouse.com/insights/financial-services/2021/public-sector/garp-three-lines-of-defense?lang=en#:~:text=The%20three%20lines%20of%20defense%20represent%20an%20approach%20to%20providing,relationship%20between%20those%20different%20areas)

[7] Jaclyn Jaeger, "Analysis: Comparing the IIA's new 'Three Lines Model' to the old one," posted on complianceweek.com on July 29, 2020. (https://www.complianceweek.com/risk-management/analysis-comparing-the-iias-new-three-lines-model-to-the-old-one/29252.article)

PRINCIPLE FIVE

Cybersecurity Measurement and Reporting

When NACD polled its members for its *2022 NACD Public Company Board Practices and Oversight Survey*, the report found that only 52 percent of boards are reviewing the potential material, financial implications of a cyberbreach on their companies—this compared to 72 percent who are reviewing the company's approach to protecting its most critical assets.[1] These findings support the claim that in most cases, management still reports on cybersecurity with imprecise scorecards such as "heat maps," where cyber risk is measured in colors or in high-medium-low terms; security "maturity ratings"; and highly technical data that are out of step with the metric-based reporting that is common for other enterprise risks.

These legacy practices do not allow management and the board to understand the materiality of cyber events and to properly assess the adequacy and cost-effectiveness of risk mitigation initiatives. According to a NIST publication focused on integrating cybersecurity into enterprise risk-management practices, "While qualitative methods are commonplace, companies may benefit from considering a quantitative methodology with a more scientific approach to estimating likelihood and the impact of consequences. . . . This may help to better prioritize risks or prepare more accurate risk exposure forecasts."[2] This does not absolve the board from gaining a basic understanding of the technical aspects of cybersecurity, which helps validate management's assumptions in quantifying the risk.

While cyber-risk management is a relatively young discipline compared to other forms of enterprise-risk management, expectations for mitigating and reporting on it should not be reduced. Management should deliver reports that are

- **transparent about performance**, with economically focused results based on easily understood methods;
- **benchmarked**, so directors can see metrics in context to peer companies or the industry; and
- **decision-oriented**, so the board can accurately evaluate management's decisions weighed against the defined risk appetite, including resource allocation, security controls, and cyber insurance.

As discussed in Principle 1, cyber risk should be discussed in terms of strategic objectives and business opportunities. In this context, every key performance and risk indicator should be tracked against a performance target or risk appetite, as proposed by management and approved by the board. Risk appetite statements should be defined in as clear, objective, and measurable a way as possible, while also accounting for subjective factors such as the economic environment within which the appetite was initially decided.

While this level of reporting is still aspirational for some companies, directors can drive their organizations forward by asking the following five questions and demanding answers that are backed by the sort of metrics and reports that we suggest in this principle and in Tool F.

1. How are we measuring the threat environment and how prepared are we to meet it?

The chief information security officer or chief risk officer should paint a picture of the threat environment (cybercriminals, nation-states, malicious insiders, etc.) that describes what's going on globally, in our industry, and within the organization. Examples of good metrics and reports include these:

- Global cyber-related financial and data losses
- Threats and new breaches within our industry that are most likely to introduce business, operational, and financial harm into our organization
- Trends in the types of hacker tactics (e.g., ransomware, leveraging zero-day vulnerabilities, etc.) and new attack patterns
- Cyber threat trends from information sharing and analysis centers (ISACs)[3]

2. What is our cyber-risk profile?

Boards should get cyber-risk assessments from independent sources. Useful sources of information include these:

- Independent security assessments (e.g., external consultants, law firms specializing in cybersecurity and privacy laws, and auditors)
- Independent security ratings of the company, benchmarked against peer organizations and used alongside other key risk indicators to augment understanding
- Third-party and fourth-party risk indicators

3. What is our cyber-risk profile as defined by management?

Management should provide assessments of the company's cybersecurity program that spans departments and functions, using tangible performance and risk metrics which may include these:

- A NIST-based program maturity assessment conducted by a third party
- The relationship between cyber-risk maturity and risk-mitigation prioritization
- Investments made to ensure business resilience
- Compliance metrics on basic cyber hygiene (the Five Ps): **P**asswords, **P**rivileged Access, **P**atching, **P**hishing, and **P**enetration Testing
- Percentage of critical systems downtime, and time needed to recover
- Mean time to detect and remediate cyber breaches

4. What is our cyber-risk exposure in economic terms?

The central question here is this: "What is the company's loss exposure to cybersecurity events?" In the past 30 years, we have seen that question answered in economic terms for every other risk discipline in enterprise risk management: interest rate risk, market risk, credit risk, operational risk, and strategic risk. Now we need to address that question for cyber risk. This expectation can also be found in the US Securities and Exchange Commission's guidance on cybersecurity disclosures and its focus on quantitative risk factors.[4]

Multiple cyber-risk quantification (CRQ) models have emerged that allow cyber-risk professionals to assess a company's cyber-loss exposure in financial terms.[5] Different frameworks and models have been adopted by a large number of companies and vendors, following recent

applied research in the domain that includes advancements in the cyber-insurance industry enabling alignment between the organization's cybersecurity strategy and established risk appetite.[6] Organizations should select an enterprise cyber-risk management approach that includes an understanding of the operational, financial, and business needs of the organization and alignment with their overall risk-management objectives. Companies should select the CRQ method, tools, and services that best meet their needs and that can provide defensible results. (See "Cyber-Risk Quantification Approaches and Methods," below, for definitions of two CRQ methods and questions directors can ask to assess the choice their organization has made.)

Regardless of the method or tools that fit your organization, in the current environment, directors should demand more robust reporting on metrics like these:

- Value of enterprise digital assets, especially the company's crown jewels
- Probability of cyber event occurrence and potential loss magnitude
- Potential reputational damage and impact on shareholder value
- Costs of developing and maintaining the cybersecurity program
- Costs of compliance with regulatory requirements (e.g., the EU's General Data Protection Regulation)

CYBER-RISK QUANTIFICATION APPROACHES AND METHODS

As cyber-risk quantification (CRQ) adoption and effectiveness increases, several models have emerged for calculating cyber risk in economic terms. Many of these approaches rely on two primary quantification methodologies: asset-based quantification and actuarial-based quantification. Both methods attempt to objectively quantify in economic terms a company's cyber-risk exposure, the likelihood of risk event, and the potential loss magnitude of a given incident.

Asset-Based CRQ

These models leverage an approach to cyber-risk management developed by several leading risk management frameworks such as ISO/IEC 27005. These models mostly perform risk analysis via an asset register alongside a risk register to then quantify a company's cyber-risk exposure in economic terms. While robust at the asset level, these models do not always evaluate risk to the organization and ecosystem.

Actuarial-Based CRQ

This approach leverages historical actuarial data related to breach and loss events to calculate cyber-risk exposure, potential loss magnitude, and likelihood of risk event. Cyber insurance actuarial data in this space is highly variable.[7] Additionally, this model is unable to account for zero-day attacks and newly discovered vulnerabilities as, by definition, they lack historical actuarial data on those methods of attack.

Questions directors can ask to better understand their organization's chosen approach and ensure it is best suited for their company's needs include these:

- Does the chosen CRQ model have any weaknesses? How is the cyber-risk management team mitigating what the model doesn't cover?
- Is the chosen model flexible enough that we are regularly updating it to address new vulnerabilities and recent cybersecurity events?
- Is the approach we are using in line with those of our sector and industry peers?

5. Are we making the right business and operational decisions?

As stated in Principle 1, cybersecurity is not simply a technology, security, or even a risk issue. Rather, it is a business issue and a "cost of doing business" in the digital economy. On the opportunity side, advanced technologies and digital innovations can help companies to offer new products and services, delight their customers, and streamline or disrupt the supply chain. As a top strategic issue, management should provide the board with risk and return metrics that can support effective oversight of business and operational decisions, such as risk-adjusted profitability analysis of digital businesses and strategies (including M&A), return on investment of cybersecurity controls and related technology investments, and cyber-risk insurance versus self-insurance.

Board-management discussions about cyber risk should include identification and quantification of those threats that can introduce material financial exposures to cyber risks and which inform risk acceptance, mitigation, or transfer decisions.

DEFINING RISK APPETITE

"Risk appetite" is the amount of quantifiable risk an organization is willing to accept in pursuit of strategic objectives. Thus, it should define the level of risk, through measurement, at which appropriate actions are needed to reduce risk to an acceptable level. When properly defined and communicated, it drives behavior by setting the boundaries for running the business and capitalizing on opportunities. A 2022 commission on the future of board practices also found that it is critical to risk oversight that the board and management "have an agreed and clearly defined risk appetite which provides guardrails for risk activity."[8]

A discussion of risk appetite should address the following questions:

- **Corporate values:** What risks will we not accept?
- **Strategy:** What are the risks we need to take?
- **Stakeholders:** What risks are stakeholders willing to bear, and to what level?
- **Capacity:** What resources are required to manage those risks?
- **Financial:** Are we able to adequately quantify the effectiveness of our risk management and harmonize our spending on risk controls?
- **Measurement:** Can we measure and produce reports to ensure that proper monitoring, trending, and communication of reporting is occurring?

"Risk appetite is a matter of judgment based on each company's specific circumstances and objectives. There is no one-size-fits-all solution."

Source: PwC, *Board oversight of risk: Defining risk appetite in plain English* (https://www.pwc.com/us/en/corporate-governance/publications/assets/pwc-risk-appetite-management.pdf).

KEY CONSIDERATIONS FOR THE BOARD

- ☐ Ensure the board understands those cyber threats that are likely to introduce material business, operational, and financial harm in order to inform effective risk mitigation strategies.
- ☐ Boards and management should come to an agreement on a cyber-risk appetite.
- ☐ It is important for cyber risk to be measured, benchmarked, and reported out in objective terms to the board in the language of business.

ENDNOTES

[1] NACD, *2022 NACD Public Company Board Practices and Oversight Survey* (Arlington, VA: NACD, 2022), p. 6. (https://www.nacdonline.org/insights/publications.cfm?ItemNumber=73754)

[2] Kevin Stein, et al., NIST CSRC, *NISTIR 8286: Integrating Cybersecurity and Enterprise Risk Management* (ERM) (Washington, DC: US Department of Commerce, 2020), p. 26. (https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf)

[3] To learn more about the National Council of ISACs, please see their web page, "National Council of ISACs" (accessed January 20, 2023). (https://www.nationalisacs.org/)

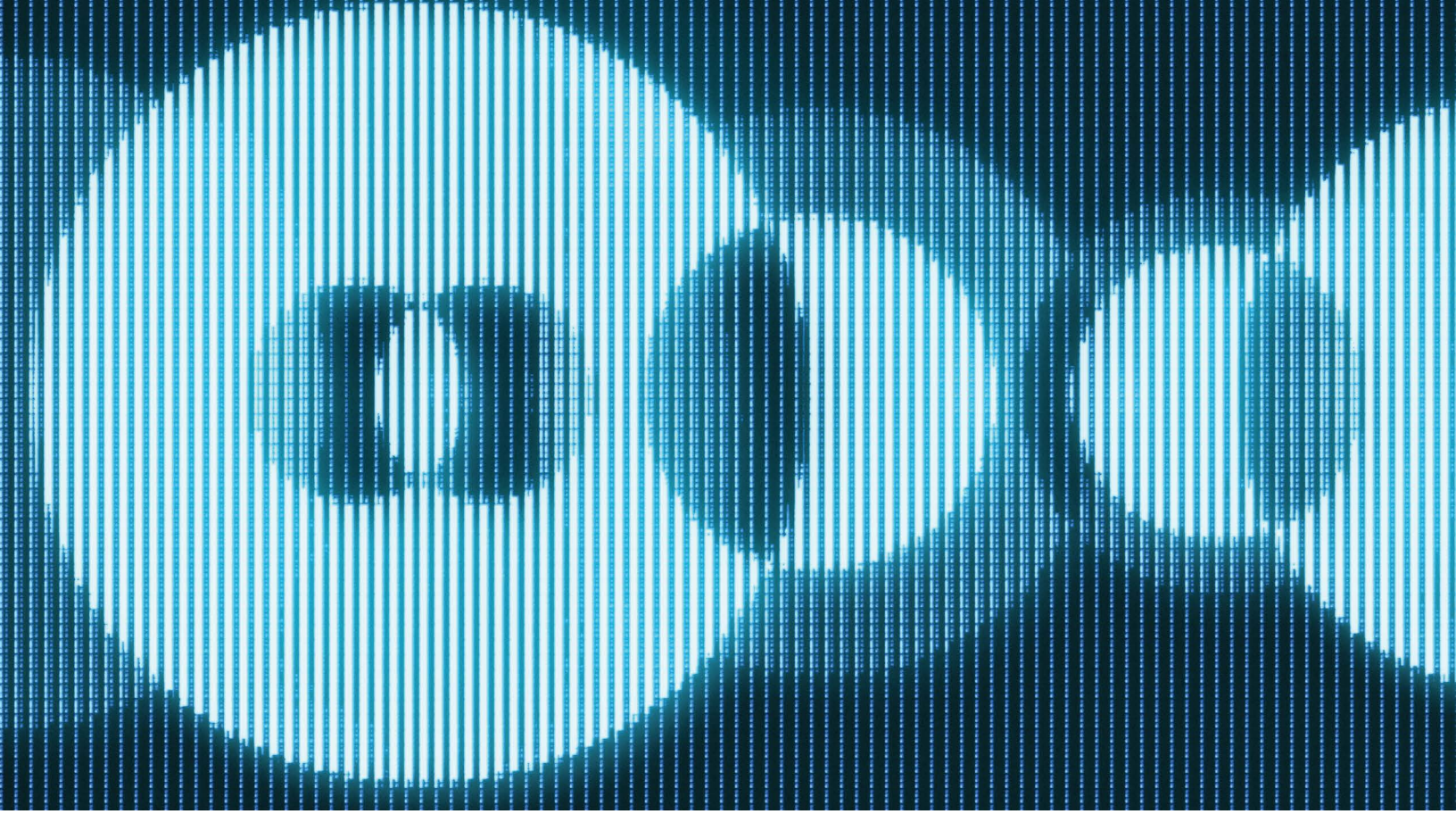
[4] See the SEC's *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* [Release Nos. 33-10459; 34-82746] (February 26, 2018), p. 15. (https://www.sec.gov/rules/interp/2018/33-10459.pdf)

[5] A variety of solutions exist, including the Factor Analysis of Information Risk (FAIR) methodology (https://www.fairinstitute.org/) and the Center for Internet Security Risk Assessment Method (CIS RAM, available at (https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method), which are considered non-proprietary, open-source models for quantifying risk. There is also a growing market of proprietary cyber-risk analysis models available.

[6] Notable CRQ publications include these: D. Hubbard, R. Seiersen (2016), *How to Measure Anything in Cybersecurity Risk*, Wiley; J. Jones, J. Freund (2015), *Measuring and Managing Information Risk: A FAIR Approach*, Butterworth-Heinemann; Ruan, K. (March 2017), "Introducing Cybernomics: A Unifying Economic Framework for Measuring Cyber Risk," Computers & Security, Volume 65, p 77-89, ISSN 0167-4048, (https://www.sciencedirect.com/science/article/pii/S0167404816301407?via%3Dihub)

[7] Unal Tatar et al., *Quantification of Cyber Risk for Actuaries: An Economic-Functional Approach* (Society of Actuaries, May 2020), p. 7. (https://www.soa.org/globalassets/assets/files/resources/research-report/2020/quantification-cyber-risk.pdf)

[8] NACD, *The Future of the American Board Report: A Framework for Governing into the Future* (Arlington, VA; NACD, 2022), p. 36. (https://www.nacdonline.org/insights/publications.cfm?ItemNumber=74136)



PRINCIPLE SIX

Encourage Systemic Resilience and Collaboration

In 2021, NACD, ISA, and the World Economic Forum, in collaboration with PwC, came together to unify their support for the previous five principles outlined in this handbook. The organizations also agreed that corporate governance had evolved in recent years, and that a new principle was necessary to encourage systemic resilience and collaboration around cybersecurity. The organizations made this declaration:

> "The highly interconnected nature of modern organizations means we run the risk of failures that spread beyond one enterprise to affect entire industries, sectors and economies. It is no longer sufficient just to ensure the cybersecurity of your own enterprise; rather, cyber resilience demands that organizations work in concert. Recognizing that only collective action and partnership can meet the systemic cyber-risk challenge effectively, senior strategic leaders must encourage collaboration across their industry and with public and private stakeholders to ensure that each entity supports the overall resilience of the interconnected whole."[1]

This principle is consistent with over-arching trends in corporate-governance best practice such as the ESG movement, which calls on organizations to understand their responsibilities to consider the *environmental, social, and governance (ESG)* impacts of their actions on a broader range of stakeholders. In 2019, the Business Roundtable issued a purpose statement that called on companies to go beyond shareholder primacy and consider the interests and expectations of other key stakeholders like employees, customers, and suppliers.[2] Given the interconnected nature of cyber risk when it spans disparate companies and industries operating on the insecure structure of the Internet, it is incumbent upon each organization to be "their brother's keeper"—in much the same way that the *E* in ESG relies on companies to come together to improve our ecological environment.

The defining characteristic of the Internet is the massive interconnection of multiple systems. Built without security in mind, this interconnection has been exploited since its inception and has in the past decade created effects that extend well beyond individual entities. In 2017, the NotPetya attack spread from a malware-infected system in Ukraine to paralyze global shipping and cause an estimated $10 billion in damages to a wide variety of industries, from pharmaceuticals to construction, from personal care to consum-

er foodstuffs. In 2020, malware was uploaded to much of the US federal government, including the Department of Defense; to 425 companies in the US Fortune 500; and to an as-yet-untold number of other customers worldwide by compromising an update installed by SolarWinds, a US-based technology infrastructure vendor. The extent of the damage likely to follow, or even the purpose of the attack, is still open to speculation, but the US Government Accountability Office has noted that the purpose of the attack on some sensitive organizations was espionage.[3]

While the number of these systemic cyberattacks is still comparatively small, some of the most sophisticated risk managers in the world are predicting that these events are merely the "canary in the coal mine" and the emerging expansion of technologies such as 5G mobile communications will likely enhance the opportunity for and the potential impact of systematic cyber events. Given the breadth of the type of victims that were the point of entry in recent systemic attacks, it is imperative for all organizations to secure themselves in order to secure the system at large.

The board of directors' oversight responsibility is to see that management provides an effective cyber-risk strategy, including improving the cybersecurity and resilience not only of their organization's systems, but also the security and viability of the cyber ecosystem of which they are a part. Much in the same way that effective cybersecurity risk management requires the breaking down of siloes within the organization, truly effective systemic cyber resilience can only be achieved by breaking down the barriers that exist to information sharing between organizations, law enforcement, regulators, and communities. Boards can explore ways that the company and its management can cooperate with information-sharing organizations and law enforcement within various tools in the toolkit.

KEY CONSIDERATIONS FOR THE BOARD

- ☐ Develop a 360-degree view of the organization's risk and resiliency posture to function as a socially responsible party in the broader environment in which the business operates.
- ☐ Develop peer networks that include other board members to share best governance practices across institutional boundaries.
- ☐ Ensure that management has plans for effective collaboration and information sharing, especially with the public sector, on improving security and resilience.
- ☐ Ensure that management takes into account risk stemming from broader industry considerations (e.g., third-party vendors and partners—(see Tool D for further details).
- ☐ Encourage management's participation in industry groups and knowledge and information sharing platforms such as sector-specific information sharing and analysis centers (ISACs) and/or cross-sectoral information sharing organizations (ISOs).

ENDNOTES

[1] See *Principles for Board Governance of Cyber Risk* (World Economic Forum, 2021), p. 12. (https://www.nacdonline.org/insights/publications.cfm?ItemNumber=71795)

[2] The Business Roundtable, "Business Roundtable Redefines the Purpose of a Corporation to Promote 'An Economy That Serves All Americans,'" posted on businessroundtable.org on August 19, 2019. (https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans)

[3] US GAO, "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (Infographic)," posted on gao.gov on April 22, 2021. (https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic)


TOOLKIT

TOOL A

Ransomeware Readiness

By Mike Woods, GE

WHAT IS RANSOMWARE, AND WHY IS IT UNIQUE FROM OTHER CYBER THREATS?

Ransomware is a tool for extortion. It is a type of malicious software (malware) used by threat actors to block access to data or systems. Ransomware encrypts its target until the victim pays a ransom, usually with specific deadlines and requirements to be paid in cryptocurrency. In 2021, it took on average one month for an organization to recover from a ransomware attack.[1] This means one month of lost opportunity, extra device costs, the ransom itself, and more. In 2021, the average cost to cover for an organization in the United States was approximately $1.4 million dollars.[2] With more than 150 active variants as of 2022, ransomware has become both cost-effective and a service-based attack for cyber criminals. According to Top10VPN's Hacking Tools Price Index, malware can be purchased for as little as $45.[3] As mentioned in the Principles section of this handbook, the economics of cybersecurity tend to be upside down, as the cost to commit an attack is far less expensive than the cost of securing against, mitigating, and insuring organizations. Cybersecurity insurance is costly; accordingly, boards should ensure their management teams have clear contingencies, situational awareness, and readiness to respond to an attack.

QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ON RANSOMWARE

Readiness

1. Is there a playbook for ransomware that includes responsibilities, processes, and expected outcomes?
   a. What role, if any, do you need the board and C-suite executives to play in light of an attack?
2. What are our cyber capabilities and/or countermeasures to deal with ransomware attacks? Boards should look for answers that may include the following:
   a. Use a backup system and routinely check it for data integrity and confirm it is operational.
   b. Participate in cybersecurity information sharing.
3. What percentage of coverage do these capabilities provide across our digital/IT estate?
4. Does our cyber insurance policy cover ransomware specifically? Here are some specific items to consider asking about:
   a. Premiums for ransomware policies have increased in recent years. Would it be more cost effective to self-insure? What advantages do formal insurance policies present to our organization's cybersecurity infrastructure?
   b. Some business policies such as extortion policies may cover losses related to ransomware. Does our policy have that coverage?
5. Are employees trained on how to identify and report if they suspect a ransomware event is occurring? Here are some follow-up questions boards can ask to gauge the depth of the program:
   a. Is our organization providing guidance on handling infected computers and turning off noninfected computers?

b. Have our front-line managers worked with IT and information security to communicate alternative methods for business-critical functions (e.g., email, payroll, production)?

Backup and Recovery

1. How are our system backups maintained, tested, and measured for resiliency? Here's one follow-up question to consider asking:
   a. Does the implementation of backups include reporting, metrics, and ongoing monitoring requirements?
2. In the event of a ransomware attack, are we confident that our IT systems can be restored within our specified recovery plan objectives? Are we including third-party systems and capabilities (e.g., cloud-based software) within our recovery plan?
3. Do our system backup and recovery partners' response times align with our current timelines in our recovery plan?

Suppliers and Partners

1. Do we monitor critical third parties (those we share data with and/or have network connectivity to) for ransomware attacks? When receiving answers about this question, boards can look for details about the following:
   a. Whether we train supply-chain personnel to recognize cybersecurity risk and enable mitigation activities.
   b. Ensure third-party due diligence throughout the proposal, selection, and onboarding processes.
   c. Put a vendor-risk management framework in place with appropriate stakeholders involved and with a direct owner of this function.
2. Do we require specific ransomware and/or incident reporting from third parties within our contracts and agreements? Directors can consider asking for a follow-up:
   a. Is cybersecurity expertise leveraged during the negotiating and contracting process?
3. As part of our enterprise vendor risk management program, do we assess (and reassess incrementally) any third parties to understand their cyber-risk posture?

Response Exercises

1. Is there a clearly communicated line of accountability in the event of an attack? Are there plans for ransomware tabletops/simulation exercises so that our organization can form muscle memory around their role?
2. Are there clear thresholds related to the materiality of an attack, including triggers for engagement of senior management and/or the board?
3. Are we ready to coordinate with law enforcement in the event of a ransomware attack? Directors can ask senior management if their organizations have an established understanding of who to contact, based on the jurisdictions that they fall within:
   a. US state, local, tribal, and territorial government agencies can report ransomware attacks to the Multi-State Information Sharing and Analysis Center (MS-ISAC).

b. Other sectors and home users should report attacks to their local FBI field office or the Internet Crime Complaint Center (IC3).

4. Does management have a clear stance on paying or not paying a ransomware demand? If an incident causes management to recommend paying a demand, have we done a walkthrough with decision makers on how the process would work?
   a. Does the board know if the organization has appropriate access to a cryptocurrency wallet and cryptocurrency expertise to make a payment? This expertise may be available via a third party such as an insurer.

Communications

1. Is there a concise communications plan across cybersecurity and technology teams and senior management? Here are some items for boards to consider asking follow-up questions about:
   a. When and how will company officers and employees be notified of the disruption?
   b. When and how will business partners and key external parties be notified?
   c. Who will be responsible for preparing and delivering a public statement on the disruption?
   d. What will be the timeline for acting on regulatory, disclosure, or compliance requirements, and who will be involved?
2. Does the plan include holding statements for various audiences (e.g., employees, customers, regulators, media)?
   a. Keep company officers, employees, business partners, and the public informed as the incident investigation progresses.

ENDNOTES

[1] Sophos.com, "Ransomware Hit 66% of Organizations Surveyed for Sophos' Annual 'State of Ransomware 2022.'" (https://www.sophos.com/en-us/press-office/press-releases/2022/04/ransomware-hit-66-percent-of-organizations-surveyed-for-sophos-annual-state-of-ransomware-2022)

[2] Ibid.

[3] Simon Migliano, "Dark Web Market Price Index: Hacking Tools" updated on top10vpn.com on September 1, 2021. (https://www.top10vpn.com/research/dark-web-prices/hacking-tools/)

TOOL B

Assessing the Board's Cyber-Risk Oversight Effectiveness

By Jason Escaravage, Thomson Reuters

This tool helps directors identify which questions to ask themselves to assess their own understanding of the organization's cybersecurity and to ask senior management to assess their effectiveness, and outlines a numerical scale for assessing the board's cyber-risk oversight effectiveness.

Board leaders wishing to incorporate a cybersecurity component into their board's recurring self-evaluation can use the questions in the table below as a starting point.

QUESTIONS DIRECTORS CAN ASK TO ASSESS THEIR BOARD'S CYBERSECURITY UNDERSTANDING

1. **Who on our board possesses qualifiable cybersecurity expertise? What is that expertise?**
2. **Can all directors effectively contribute to a robust conversation with management about the current state of the company's cybersecurity? In which areas does our lack of knowledge/understanding of cyber matters prevent effective oversight?**
3. **Are we able to effectively interpret/assess management's presentations and their answers to our questions?**
4. **Do we thoroughly understand the most significant cyber threats to this business and what impacts they could have on the company's strategy and ultimately on its long-term growth?**
5. **Do we understand security-related legislation and regulation changes that could affect the company? What is the potential impact?**
6. **Do we know if an incident response plan and playbook(s) exist and what our role is, if any? Is there awareness around whether the company has insurance that covers cyber events, and what exactly is covered? Is there director and officer exposure if we don't carry adequate insurance? What are the benefits beyond risk transfer of carrying cyber-risk insurance?**
7. **Do we understand how materiality of an incident is determined, and by whom within our organization? Do we have processes in place for making the proper disclosures when a risk comes to fruition?**

CYBER-RISK OVERSIGHT EFFECTIVENESS ASSESSMENT TOOL

Use the numerical scale to indicate where the board's culture generally falls on the spectrum shown below.						**Action Item**
Statements Indicating Lagging Practices	**Range Indicator** (Circle Number Closest to Practice Maturity)					**Statement Indicating Leading Practices**	
We classify cyber risk as an IT or technology risk.	1	2	3	4	5	We classify cyber risk as an enterprise-wide risk.	
Our cybersecurity discussions with management focus primarily on reviews of past events (e.g., historical breach data).	1	2	3	4	5	The board reviews regular industry-related threat updates and participates in regular complex breach exercises, or tabletop scenarios applicable to real-world risks.	
The board receives information about cybersecurity exclusively from management.	1	2	3	4	5	Alongside information from management, the board receives firsthand information about cybersecurity from non-management sources.	
Information about emerging cyber threats or potential issues is filtered through the CEO.	1	2	3	4	5	The CEO encourages open access and communications between and among the board, external sources, and management about emerging cyber threats.	
The board relies on the expertise of one or two functional leaders/ experts in cybersecurity to evaluate management's plans and assumptions on cybersecurity risk and strategy.	1	2	3	4	5	The board is broadly educated on cybersecurity concepts and best practices, allowing all directors to engage in a discussion on cybersecurity with other board members and management.	

CASES IN POINT

Unidentified Risk During Acquisition Due-Diligence Led Marriott Directors to Face Violation of Security Law Claims and Personal Liability Lawsuits

In August 2018, Marriott International acquired Starwood Hotels and Resorts Worldwide for $13 billion to expand the hotel chain to the world's largest, merging loyalty programs as a differentiator for corporate travel departments.[1] However, Marriott's board failed to identify a data breach in the Starwood guest reservation database from 2014, resulting in the loss of sensitive data for more than 380 million people. Sensitive data included names, payment card data, passport information, travel companions, and home addresses. Even though the breach occurred two years prior to the acquisition, Marriott learned about the breach in September 2018, one month post acquisition.

All 50 states' and District Court Attorneys General the SEC, FTC, and US Senate and Congress committees, along with others, opened investigations. Marriott directors were personally named in US court filings, and they defended their oversight in court.[2] It was determined that the Marriott board acted in good faith to fulfill their oversight duties. However, the litigation inclusion of Marriott's directors with claims of violating the securities law related to data breaches and claims of personal liability demonstrate that all firms are expected to monitor cyber risk, and directors can be found liable if lack of oversight occurs.[3]

These lawsuits, fines, and consequent reputational damage could have potentially been avoided or more effectively managed if Marriott had identified this data breach during the acquisition due diligence process, prior to acquisition of Starwood.

Investors Sue SolarWinds Directors Claiming Failure to Monitor Known Cyber Risks

In the spring of 2020, SolarWinds sent out an update to its network-monitoring Orion software which was intended to deliver a routine fix of bugs and to patch errors within the software. However, malicious code was embedded into the update, creating backdoor access to customer systems. An estimated 18,000 businesses were affected, and the attack went beyond the private market to impact government agencies.

In November 2021, pension funds and individual shareholders filed a lawsuit claiming current and former board directors breached their fiduciary duty of care and loyalty by failing to monitor known security risks.[4] Heightened supply chain attacks occurring around the time of the cyberbreach bolstered claims, as plaintiffs viewed it was reasonable for directors to be familiar with the trend and to provide oversight given the current trend.

In October 2022, SolarWinds settled in court to pay shareholders $26 million, receiving notification of an SEC enforcement notice, alleging violations of US federal security laws with respect to cybersecurity disclosures and public statements, as well as its internal controls and disclosure controls and procedures.[5]

While the lawsuit settlement resolves claim against the company and named directors included in the class action litigation, the final settlement agreement has not been executed, and SEC enforcement is poised to continue. Director knowledge of cybersecurity and frequent reviews of cybersecurity risks and associated policies, processes, and controls proves to be key in providing adequate oversight.

ENDNOTES

1 Craig Karmin, "Marriott Completes Acquisition of Starwood Hotels & Resorts." the *Wall Street Journal*, September 23, 2016. (https://www.wsj.com/articles/marriott-completes-acquisition-of-starwood-hotels-resorts-1474605000)

[2] Review of In Re: Marriott International, Inc., Customer Data Security Breach Litigation. 2021. United States District Court for the District of Maryland, Southern District.

[3] Michal Barzuza and Ido Kenan, Barzuza, Michael, "Review of Delaware Court in Marriott Ruling: Directors Have Duty of Oversight in Cybersecurity," *CTech*, posted January 11, 2021. (https://www.calcalistech.com/ctech/articles/0,7340,L-3921397,00.html)

[4] JD Supra, "Shareholders Seek to Hold Current and Former SolarWinds Officials Liable for Massive 2020 Security Breach", posted on jdsupra.com on December 7, 2021. (https://www.jdsupra.com/legalnews/shareholders-seek-to-hold-current-and-2113517/)

[5] See SolarWinds Corporation's Form 8K, dated October 28, 2022. (https://d18rn0p25nwr6d.cloudfront.net/CIK-0001739942/61d90bcd-df38-4f4f-9f67-48760315061c.pdf)

TOOL C

The Cyber-Insider Threat

By Niall Brennan, SAP

Mitigation of the insider threat poses one of the greatest challenges to managing cyber risk. Precisely because the delivery of this threat involves leveraging the legitimate access of "trusted insiders" (employees, contractors, vendors, and others) to an organization's network, systems, and data, it can be harder to detect than other threats in which the forensic indicators of compromise are more immediate and obvious. This tool defines the insider threat and outlines the categories of insider incidents and the types of insider threat actors. Finally, it proposes questions that boards should be asking to ensure executive management is adequately addressing insider threats.

WHAT IS THE INSIDER THREAT?

CISA defines the insider threat as the potential for an individual or individuals with authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.[1]

The objectives of insider attacks can result in the following forms of harm to an organization:

- Sabotage
- Fraud
- Intellectual property theft
- Espionage
- Loss of share value
- Loss of consumer confidence

Insider attacks are generally carried out through the following types of actors:

- Careless or negligent employees
- Disgruntled or departing employees
- Malicious insiders
- Third-party partners

QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ABOUT INSIDER THREATS

Boards should start by understanding the possible risk associated with insider threats. What are the top risk scenarios involving insider threat?

- What is our probable loss exposure related to the insider threat scenarios?
- What are the most effective controls, and which ones should be prioritized?

Boards can follow up with more detailed questions regarding the organization's practices to defend against insider threats:

- Does the organization have a documented insider threat mitigation plan with clearly designated oversight, management, and reporting responsibilities?
- Who are the appropriate stakeholders to involve in the insider threat mitigation plan within the organization—information security, physical security, general counsel, human resources, corporate investigations, privacy, etc.?
- What manual and automated systems are in place to vet employees and identify anomalous, negligent, and/or malicious behavior throughout the employee life cycle?
  - Background checks during the recruitment and hiring process and during an employee's tenure
  - Onboarding procedures
  - Continuous monitoring
  - In-service training
  - Employee reporting mechanisms
  - Secure off-boarding procedures
- Is access to facilities, data, and systems properly aligned with each employee's respective job function (no more, no less than necessary to perform their functions)? Does the organization have an overall identity and access management program? What procedures are in place to ensure prompt adjustment of access privileges in the event of an employee's change in status (transfer, promotion, termination, etc.)?
  - What procedures are in place to detect and prevent activity which exceeds or otherwise falls out of scope with designated privileges?
  - Is physical access to the organization's space appropriately controlled to prevent unsanctioned removal of company assets, media, and/or data?
- Is there a data classification policy in place and enforced to ensure proper labeling and handling?
- Is there a comprehensive incident response plan in place involving all stakeholders (human resources, general counsel, compliance, security, and others) in the event of an insider incident?
  - Does it align with other internal incident response frameworks?
  - Are there in-house forensic capabilities, or is an outside firm on retainer?
  - Do appropriate relationships currently exist with law enforcement partners to assist with the response?
  - Do appropriate relationships exist with regulators that may require reporting about such incidents?
- Does the organization have a backup and recovery program? Could it recover its systems and critical data if access was hindered or data corrupted in the main system?
- Does the organization have strong controls around critical vendor relationships to prevent unauthorized access?

- How are third-party vendors monitored to control unauthorized access?
- For third-party cloud and software-as-a-service providers that are critical to business processes, what controls are in place to prevent unauthorized access while also enabling the business? (Reference Tool D, Supply Chain and Third-Party Risks, and Tool J, Securing the Cloud, for more in-depth practices, controls, and questions.)

- How does the organization measure the effectiveness of its insider threat mitigation plan? Does it periodically test the plan with internal assets and external parties to validate its effectiveness?
  - Does its insider threat mitigation plan maintain procedures to properly document incidents or insider threat activity?
  - Does it maintain metrics to identify and analyze patterns of insider threat activity to assist with reducing vulnerability?
- Does the organization have adequate programs in place to sensitize employees to insider risks and train them to detect, report, and mitigate potential incidents?
  - Do we have a security awareness program in place? Are we tracking metrics of this program to identify progress or problem areas?
  - Is there a disciplinary or continuing education framework for employees failing tests? Does it show improvement in employee behavior?

ENDNOTE

[1] See the cisa.gov web page, "Defining Insider Threats." (https://www.cisa.gov/defining-insider-threats#:~:text=The%20Cyber%20and%20Infrastructure%20Security)

TOOL D

Supply-Chain and Third-Party Risks

By Niall Brennan, SAP

The strength of an organization's cybersecurity can be completely undermined by the weakest link in its supply chain. At stake may be the company's profitability, reputation, and credibility.

Recent research highlights a 300 percent increase in supply chain cyberattacks in 2021 compared to 2020 levels.[1] For instance, attackers in the high-profile 2021 SolarWinds breach made use of these tactics to target many SolarWinds customers, dozens of them in the Fortune 500.[2] In an increasingly interconnected digital ecosystem, boards and cybersecurity leaders must prioritize addressing these risks to achieve true resilience.

Successfully competing in the digital age may require using a long and global supply chain, including the use of third-party technologies and software. While this business practice may generate strong economic advantages, these benefits need to be balanced with recognizing and overseeing potential security risks. A 2019 conference for directors on cybersecurity concluded that one of its key takeaways was that directors must "[r]emain familiar with the company's processes to identify, assess, and manage third-party and supply chain risks."[3]

This tool details questions that directors should be asking management to ensure adequate security measures are in place to address supply chain risks.

SUPPLY CHAIN AND THIRD-PARTY RISK MANAGEMENT QUESTIONS

1. **How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?**
2. **How much visibility do we currently have across our supply chain regarding cyber-risk exposure and controls? Which departments/business units are involved?**
3. **What will need to be done to fully include cybersecurity in current supply-chain and vendor/third-party risk management?**
4. **How are cybersecurity requirements built into contracts and service-level agreements? How are they enforced? Are our contracts and service-level agreements written to include requirements for the following:**
   - **a.** Written cybersecurity policies
   - **b.** Personnel policies, such as background checks, training, etc.
   - **c.** Access controls
   - **d.** Encryption, backup, and recovery policies
   - **e.** Secondary access to data
   - **f.** Countries where data will be stored
   - **g.** Notification of data breaches or other cyber incidents
   - **h.** Incident-response plans
   - **i.** Top cyber-risk assessment
   - **j.** Audits of cybersecurity practices and/or regular certifications of compliance

5. **How difficult/costly will it be to establish and maintain a viable cyber-vulnerability and penetration-testing system for our supply chain?**
6. **How difficult/costly will it be to enhance monitoring of access points in the supplier network?**
7. **Do our vendor agreements bring new legal risks or generate additional compliance requirements (e.g., FTC, HIPAA, CCPA, GDPR, etc.)? Are we indemnified against security incidents on the part of our suppliers/vendors?**

CASE IN POINT

Ransomware Attack Disrupts Global Supply Chains

Despite being warned by researchers of their software vulnerabilities, in 2021 a major US IT management firm suffered a ransomware attack on its virtual system administrator software.

Although the company initially said that only 0.1 percent of its clientele had been affected, the company's software was used by large IT companies that offered services to hundreds of small- and medium-sized businesses (SMBs). As a result, the company told nearly 40,000 customers to disconnect their services.[4] Given the large network created through managed service providers, nearly 1,500 businesses—predominately SMBs—had their operations disrupted worldwide by ransomware. The attack—arguably the largest ransomware attack yet—was successful in disrupting global supply chains over the long Independence Day weekend.

CASE STUDY: MAJOR AIRLINE RESPONDS QUICKLY TO THIRD-PARTY VULNERABILITY

In 2018, a major airline revealed that some consumer information had been compromised via a vulnerability in a third-party online chat support service.[5] In response to this breach, the airline launched a custom website outlining details of the breach and implemented a comprehensive communications campaign highlighting education and best practices.[6] The airline also worked with partners to analyze the breach, including identifying whether the vulnerability had impacted any part of the airline's own website or its own computer systems. Once the airline had successfully managed the fallout from the breach, the airline filed a lawsuit against the third-party service, citing that the third-party vendor had failed to comply with a contractual promise to notify the airline immediately should a breach occur.

ENDNOTES

[1] Aqua Security, "Aqua Security's Argon Experts Find Software Supply Chain Attacks More Than Tripled in 2021," posted on Info.aquasec.com on January 12, 2022. (https://info.aquasec.com/argon-supply-chain-attacks-study?utm_campaign=WP%20-%20Jan2022%20Argon%20Supply%20Chain%20Study&utm_source=PR_Argon_Study)

[2] Lily Hay Newman, "A Year after the SolarWinds Hack, Supply Chain Threats Still Loom." *Wired.* December 8, 2021. (https://www.wired.com/story/solarwinds-hack-supply-chain-threats-improvements/)

[3] Stephen Klemash, EY, "What boards are doing today to better oversee cyber risk," EY, 16 July 2019. (https://www.ey.com/en_us/board-matters/what-boards-are-doing-today-to-better-oversee-cyber-risk)

[4] Gerrit De Vynck and Rachel Lerman, "Widespread ransomware attack likely hit 'thousands' of companies on eve of long weekend," the *Washington Post*, July 3, 2021. (https://www.washingtonpost.com/technology/2021/07/02/kaseya-ransomware-attack/)

[5] Delta, "UPDATED: Statement on [24]7.ai cyber incident," posted on news.delta.com on April 7, 2018. (https://news.delta.com/updated-statement-247ai-cyber-incident)

[6] Anna Convery-Pelletier, "The Delta Airlines Security Breach: A Case Study in How to Respond to a Data Breach," the *Radware Blog*, October 24, 2018. (https://blog.radware.com/security/2018/10/the-delta-airlines-security-breach-a-case-study-in-how-to-respond-to-a-data-breach/)

TOOL E

Incident Response

By Greg Montana, FIS

Since not all incidents can be prevented, response is a critical component of a cybersecurity program. In 2022, the Cyber Incident Reporting for Critical Infrastructure Act went into effect, making reporting to the US Cybersecurity and Infrastructure Security Agency (CISA) mandatory for any cyberattacks against critical infrastructure organizations. However, having incident response capability is necessary for all organizations regardless of size or sector as virtually all organizations are now possible targets of cyberattacks. This tool outlines steps boards should take to ensure that their organizations have an effective incident response program.

The business capabilities and functions required to support incident response are these:

- **Governance:** Knowledge of assets and where they reside with appropriate controls and data protection, and with regular risk assessment and management; policies; and procedures
- **Protective Capabilities:** Policies, employee awareness, and education; control procedures to validate access; information protection procedures; and continual validation
- **Detection Capabilities:** Set of capabilities to detect anomalies and events, and continuous monitoring for effectiveness
- **Response:** Response playbook; regular cyber exercises; coordinated efforts across technology teams, business, legal, communication, and law enforcement
- **Recovery:** Speedy remediation and after-action improvement

Who to contact after a cyberattack:

- **Data forensics investigation team:** Within your organization this group may be called an incident response team or digital forensics team. Successful security programs may include internal teams and third-party incident responders on retainer.
- **Law enforcement:** Local law enforcement, FBI, Secret Service ECTF, Internet Crime Complaint Center, Federal Trade Commission
- **Insurance carrier**
- **Customers**
- **Businesses that might have been affected**
- **Your bank, credit bureaus, and financial services partners**

QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ON INCIDENT RESPONSE

These questions will help boards of directors ask senior management the right questions to ensure that incident response and supporting capabilities can withstand a cyber incident and create both a speedy path to business service recovery and a timely response to customers and the market.

1. **The Incident Response Plan**
   a. Is there a clear incident playbook with definitions of roles, responsibilities, processes, and communication lines between business units? For publicly traded companies, is there a clear method outlined and practiced for assessing, determining, and disclosing the materiality of an incident?
   b. How is the incident response plan being tested and then updated, based on results from reports, exercises, and simulations?
   c. How is the incident response plan measured against the risk appetite of the company's overall business plan?
2. **Communication and Authority**
   a. What are the escalation criteria for notifying senior leadership and the board?
   b. Who has the final decision-making authority within each business unit and among senior leadership on how to respond during an incident?
   c. How is the feedback mechanism to higher management organized relative to the importance of specific systems for day-to-day operations?
3. **Exercises and Simulations**
   a. Are there organizational resiliency tests using large risk scenarios through table-top exercises, common threat simulations, and penetration testing?
   b. What is the frequency of table-top exercises? When do these occur, and are they general or attack specific?
   c. Are our HR and PR responses also being accounted for within exercises and simulations?
4. **Information Sharing**
   a. Are there established relationships in place with the intelligence community, relevant law enforcement, and key regulators?
   b. Who has the task of maintaining a relationship with relevant governmental agencies?
   c. Have information-sharing relationships been established through information sharing and analysis centers (ISACs) and consortiums and with other companies?
5. **Compliance and Reporting**
   a. Does the organization have notification and mandatory reporting obligations (e.g., regarding regulations of the US Securities and Exchange Commission, the General Data Protection Regulation, the Department of Defense and Defense Security Service for cleared contractors, and the federal government)?
   b. Who holds the highest authority within the organization in verifying that our incident response accounts for regulatory requirements?
   c. How are we maximizing our ability to share incident report data with our competitors and the regulators without disclosing any confidential company data?
6. **Disclosing Incidents**
   a. What are the criteria and what is the process for disclosing incidents to investors?
   b. How can we represent not only the cyber incidents but also the effectiveness of our incident response in our quarterly report or other relevant documents?
   c. What is our specific plan to disclose a disruption both internally and externally?

7. **Mitigating Losses**
   - **a.** What can we do to mitigate the losses from an incident?
   - **b.** Does senior management know who has the authority to swiftly disable large groups of machines or servers if they are infected by malware?
   - **c.** What reporting mechanism is in place to ensure we are investing sufficient resources into our data recovery capacity?
8. **Measuring Incident Response Effectiveness**
   - **a.** What are the critical, key performance indicators used to measure incident response effectiveness (e.g., time to detect and time to respond)?
   - **b.** What kind of metadata monitoring, collecting, and reporting mechanism is in place? What is the cost of this mechanism, and what benefit has it returned?
   - **c.** Do we simulate how long a recovery procedure would take and what kind of cost the business would incur?
9. **Post-Incident Response**
   - **a.** What key steps do you follow after a critical incident?
   - **b.** What steps do you follow to ensure this type of incident doesn't occur again?
   - **c.** How are we educating our employees to be more aware of our policies, procedures, and reporting mechanisms?
   - **d.** Do we require a post-mortem evaluation based on findings of the forensics investigation as part of the incident response plan?

CASE IN POINT

POOR INCIDENT RESPONSE

Poor incident response to a cyberattack can be characterized as vague and downplayed media responses to a hacking event, which merely stimulates questions and fear among company customers and the general public. The progression of one such event follows:

- A hacker organization conducted a cyberattack on a third-party service company, gaining access to a computer that contained customer information of its lead providing company, an identity and access manager.[1]
- After five days of access, from January 16–21, 2022, the providing company discovered the breach and closed off access. The hacker organization informed the public of the data risk to the customers due to the cyberattack two months later, on March 22, 2022. The providing company held their response to the occurrence until a week later, on March 29, 2022.[2]
- The provider apologized for notifying its customers late.[3]
- After investigation, the provider reported that the damage was not vast, doubling down on the fact that transparent customer communication is vital even after "small" attacks.[4]
- The provider then cut off all ties with their third-party processing company.[5]

- A year after the report of the cyberattack, the provider then found itself to be the recipient of a class-action lawsuit, due to the small attack possibly impacting 366 corporate clients (2.5% of its customer base).[6]

Good Incident Response

A good incident response will include a rapid incident response plan that acts to contain and prevent cyberattacks from occurring once an attack has been detected. Additionally, a good response will illustrate the importance of public transparency of the cyberattack. A company that is attacked might even provide information about the tactics and techniques of their cyberattack. Although the monetary damage due to a company's cyberattack isn't clear (presumably because it was well mitigated), company stock might decline when revealing a vulnerability, but this leads to only up to an average 4 percent drop with 40 percent of businesses stock prices unaffected. The impact of disclosing an incident is slightly greater. Upon disclosing an incident, companies see stock prices that drop more than 5 percent, but 63 percent of businesses recover that value in less than a month after making the news of the attack public.[7]

Summary:

- A software provider effectively communicated with the public after a cyberattack by an infamous hacking organization, ensuring that the breach was minimal, with only a single employee account being compromised.[8]
- The provider stated that their cybersecurity team was on the case immediately after the hackers disclosed their attack and stated that the provider's cybersecurity experts were able to stop the hack mid-operation.[9]
- The hacked company then shared information with the public regarding the tactics the hackers used to conduct their attacks.[10]
- The software provider then revealed that their cybersecurity teams had been "studying" the hacking organization and the attack techniques that the hacker group had used in the past.[11]

ENDNOTES

[1] Charlie Osborne, "As Lapsus$ comes back from 'vacation,' Sitel clarifies position on data breach," posted on zdnet.com on March 30, 2022. (https://www.zdnet.com/article/as-lapsus-comes-back-from-vacation-sitel-clarifies-position-on-data-breach/)

[2] Faife, Corin. 2022. "Okta sys security protocols limited hack, but response came too slow" The Verge. Retrieved from: https://www.theverge.com/2022/3/23/22992894/okta-hack-cso-security-protocol-sitel-lapsus; Kan, Michael. 2022. "Okta Says Hack From LAPSUS$ Group May Have Ensared 366 Brands" *PC Magazine*. Retrieved from: https://www.pcmag.com/news/okta-says-hack-from-lapsus-group-may-have-ensnared-366-brands.

[3] Liam Tung, "Okta: We made a mistake over Lapsus$ breach notification," posted on zdnet.com on March 28, 2022. (https://www.zdnet.com/article/okta-we-made-a-mistake-over-lapsus-breach-notification/)

[4] Corin Faife, "Okta says security protocols limited hack, but response came too slow," posted on theverge.com on March 23, 2022. (https://www.theverge.com/2022/3/23/22992894/okta-hack-cso-security-protocol-sitel-lapsus)

[5] Robert Lemos, "Okta Wraps Up Lapsus$ Investigation, Pledges More Third-Party Controls," posted on darkreading.com on April 20, 2022. (https://www.darkreading.com/cloud/okta-wraps-up-lapsus-investigation-pledges-more-third-party-controls)

[6] The Gross Law Firm. (2022). "Shareholder Alert: The Gross Law Firm Notifies Shareholders of Okta, Inc. of a Class Action Lawsuit and a Lead Plaintiff Deadline of July 19, 2022 – (NASDAQ: OKTA)" Cision PR Newswire. Retrieved from: https://www.keloland.com/business/press-releases/cision/20220608NY82425/shareholder-alert-the-gross-law-firm-notifies-shareholders-of-okta-inc-of-a-class-action-lawsuit-and-a-lead-plaintiff-deadline-of-july-19-2022-nasdaq-okta/; Gately, Edward. 2022. "Okta Data Breach Could Impact Hundreds of Corporate Customers" Channel Futures. Retrieved from: https://www.channelfutures.com/security/okta-data-breach-could-impact-hundreds-of-corporate-customers; Barsky, Noah. 2022. "Okta's Fearful Cyber Response Worse Than Hackers' Peek – How 3 Tempting Tech Crisis Shortcuts Cost More" *Forbes*. Retrieved from: https://www.forbes.com/sites/noahbarsky/2022/06/01/okta-fearful-cyber-response-worse-than-hackers-peek/?sh=222740d05ab7.

[7] Kelly Sheridan, "Do Cyberattacks Affect Stock Prices? It Depends on the Breach," posted on darkreading.com on April 27, 2021. (https://www.darkreading.com/threat-intelligence/do-cyberattacks-affect-stock-prices-it-depends-on-the-breach)

[8] Alexander Culafi, "Microsoft confirms breach, attributes attack to Lapsus$," posted on techtarget.com on March 23, 2022. (https://www.techtarget.com/searchsecurity/news/252515022/Microsoft-confirms-breach-attributes-attack-to-Lapsus)

[9] Pete Swabey, "Microsoft confirms Lapsus$ breach and reveals hacking group's tactics," posted on techmonitor.ai on March 23, 20222. (https://techmonitor.ai/technology/cybersecurity/microsoft-confirms-lapsus-breach-and-reveals-hacking-groups-tactics)

[10] ibid.

[11] Microsoft, "DEV-0537 criminal actor targeting organizations for data exfiltration and destruction," posted on microsoft.com on March 22, 2022. (https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction)

TOOL F

Board-Level Cybersecurity Metrics

By J. R. Williamson, Leidos, and Michael Higgins, L3Harris

Boards use metrics to help inform their strategic and oversight functions on finance, market competition, marketing sales, etc. Similarly, oversight of various forms of enterprise risk such as market risk, credit risk, and operational risk have also evolved and progressively moved from qualitative assessments to quantitative assessments. This tool describes how the board can use metrics to assess the effectiveness of cybersecurity programs and offers advice on how boards can leverage them to conduct oversight of their organization's cybersecurity programs.

METRIC FOCUS AREAS

Boards should expect metric-based reporting to focus on strategic, operational, financial/economic, and benchmark figures.

Strategic Metrics

Directors should ask management about strategic metrics related to the company's approach to security and risk.

- Which strategic metrics are most critical to our organization?
- How are we measuring those security and risk indicators that have the greatest impact on our outcomes as an organization?

Operational Metrics

Operational metrics provide little strategic context or information about performance and risk position.

- Operational metrics can still be helpful in assisting the board in understanding critical compliance issues and stimulating useful discussions about trends, patterns, root causes, and benchmarking.

Developing Cyber Economic Metrics

Cyber risk is now an accepted board-level conversation. For boards to better understand cybersecurity data, it helps to translate the data into financial metrics. Directors will need to work with management to determine the most relevant information, given their organization's unique environment.

Benchmark Data

Third-party benchmarking data can be useful for assessing performance against peers and within your industry.

- Most benchmarking data is operational and may not contain appropriate strategic context on its surface. Boards should ask management how this data applies back to overall cybersecurity or the organizational strategy.

STRATEGIC METRICS VERSUS OPERATIONAL METRICS

Directors should focus on strategic metrics about the company's approach to cybersecurity and risk that are provided by the company's management. While the focus should remain on strategic risks, certain operational metrics can be helpful in assisting the board in understanding critical compliance issues and stimulating useful discussions about trends, patterns, and root causes. Operational metrics can also

be helpful with benchmarking when they provide strategic context or information about the impact on business performance and strategic risk positions. It is the role of management to avoid using overly technical concepts and to translate them in business impact terms that the board understands and can use as part of its oversight role.

Below are more detailed questions board members should be asking management to ensure proper metrics are being collected on the enterprise's cyber risk, grouped in five categories as outlined in Principle 5. Directors will work with management to determine the level of depth required, depending on each organization's size and circumstances.

1. What is the threat environment we face?
Cyber risk leaders should provide the board of directors with an understanding of the threat environment that the company faces. Examples of good questions to ask include these:

- What are the top threats faced by our industry?
- How impactful have these threats been to our peers?
- How many cyber incidents has our company experienced in the last reporting period?
- Are there any new emerging threats that are affecting our business performance (e.g., trends in ransomware, zero-day-attacks, new attack patterns)?
- Are our threat intelligence capabilities adequate, and how do they compare to our peers?

2. What is our risk profile looking from the outside in?
Boards should get an assessment of the company's security posture from independent sources. Here are some questions that boards should ask:

- What is our vulnerability rating as measured by one of the leading security rating vendors?
- How does our rating compare against the industry benchmark?
- What are the security ratings of our strategic partners and suppliers?
- What are the findings of the latest penetration testing performed by our external provider?
- How mature are our cyber-risk management practices as assessed by a leading cyber consultancy?
- Are there any outside sources for assessing our security posture that we may not be including? What about our audit firm?

3. What is our cyber-risk profile as defined by management?
Boards should expect management to provide metrics assessing the status and the performance of their cybersecurity program. Boards can ask questions like these:

- How are we performing against basic cyber-hygiene compliance metrics related to the "five Ps" (passwords, privileges access, patching, phishing, and penetration testing)?
- How mature are our cybersecurity practices as measured against a list of established best practices? (For example: NIST CSF, NIST800-53, CIS Controls/NAS9933, CMMC)

- What is the percentage of critical systems downtime and time to recover?
- What is the mean time to detect and remediate cyber breaches?
- What percent of our supply chain failed our cybersecurity assessment?
- Are these metrics acceptable or not? How are they trending? What are our target goals?

4. What is our cyber loss exposure in economic terms?

As cyber risk has emerged as one of the top enterprise risks for most companies, boards and regulators are increasingly expecting companies to assess the frequency and the materiality of cyber events, and to express cyber risk in financial terms, similarly to the other forms of enterprise risk. Questions that the boards can ask are questions like these::

- What are our company's key assets ("crown jewels") and how do we measure their value?
- What are the top cyber risks we have as a company?
- What is the probable frequency and the probable magnitude of these top cyber events?
- What cyber risk quantification model or models are we using to assess cyber risk? Have these models been independently validated?
- What are the forms of loss that we can experience, and how are we measuring and reporting on those losses? (For example, productivity, response costs, replacement costs, fines and judgements, reputational loss)
- What is the level of risk that we can tolerate as a business, and how are we tracking against it?
- Is our cybersecurity spending adequate given the threats we face and our risk appetite targets?

5. Are we making the right business and operational decisions?

Boards must understand the cyber-risk implications of strategic business decisions, as they support digital growth or transformation initiatives. Good questions to ask can include these:

- What is the cyber risk that we can incur in launching this new business initiative (such as the launch of a new digital product, moving to the cloud, etc.)?
- What processes have we established related to making cyber-risk acceptance, cyber-risk remediation, and cyber-risk transfer decisions?
- What cyber-risk scenarios should we mitigate with internal controls and which ones should we insure against?
- How much cyber insurance do we need? Does the proposed cyber insurance policy cover us adequately? How has the changing cyber insurance market impacted our risk exposure?
- What is the cyber loss exposure associated with the new company acquisition? (Reference Tool G for more in-depth discussion of cyber-risk oversight of mergers and acquisitions).
- What is the return on investment for our cybersecurity program?
- Which key controls are most cost effective? Which ones are the least cost effective? Are there any (possibly older/outdated) initiatives eating up resources that would be better spent elsewhere?

TOOL G

Cybersecurity Concerns During M&A Phases

By Andrew Cotton, EY

This tool reviews cybersecurity risks at key stages of a merger or acquisition transaction and provides suggested questions for board members to discuss with management at each stage.

INTRODUCTION

Over the past few years, numerous high-profile cybersecurity incidents have emerged during or after large mergers and acquisitions (M&A) deals. These incidents have raised concerns among corporate executives, investors, and regulators.

Corporate executives and M&A professionals will point to improved processes and outsourced services to identify and prevent security issues. However, despite heightened awareness and the existence of various vendors who can assist in the cybersecurity elements of the M&A process, the cyber risks for acquirers are only increasing. This is due to factors such as increased online connectivity within companies and with their suppliers and customers in addition to a more distributed workforce, digital transformation, and increased cloud adoption. All of the above serve to increase the attack surface, resulting in an elevated threat environment.

The decision makers in an M&A transaction often tend to approach the strategy, finance, legal, or operational risks before accounting for cyber risks. As noted by Rob Gurzeev of TechCrunch,[1]

> "With limited time and little background in cybersecurity, M&A teams tend to focus on more urgent transactional areas of the deal process, including negotiating key business terms, business and market trend analysis, accounting, debt financing and internal approvals. With only 2-3 months to evaluate a transaction before signing, cybersecurity typically only receives a limited amount of focus. . . . [I]t's no coincidence that a recent poll of IT professionals by Forescout showed that 65% of respondents expressed buyer's remorse due to cybersecurity issues. Only 36% of those polled felt that they had adequate time to evaluate cybersecurity threats."[2]

Timely identification of cyber risks allows appropriate quantification of the valuation considerations, including estimated onetime and recurring costs to remediate cyber vulnerabilities or gaps in regulatory compliance. It also enables renegotiation of deal terms that either build the cost of remediation into the arrangement price or provide for insurance or other means of clawback if the identified vulnerability becomes an incident.

During each phase of the transaction, directors should expect to receive from management as much certainty and quantification as possible about the scale of inherited risks.

WHEN IT COMES TO CYBER-RISK ASSESSMENT, EARLIER IS BETTER

Early investigation and identification of the target company's cyber posture and risks are critical during the M&A process. Surprisingly, a 2020 report by IBM shows more than half of surveyed companies do not perform their cybersecurity assessments until after the completion of due diligence.[3] In fact, the ear-

lier that cybersecurity assessment takes place during the M&A process, the more comprehensive will be the remediation opportunities available to the acquirer.

When companies conduct a risk assessment, they should be aware of these facts and potentialities:

- A cyberattack may have already resulted in the loss of the target company's intellectual property, thus reducing the value of the company.
- A cyberattack that occurred prior to closing, regardless of when it was detected, could expose the acquirer to investigation costs, financial liability, regulatory penalties, or reputational damage.
- Attackers might still be in the acquiree's network, creating a risk of the attacker migrating into the acquirer's network.
- The acquired company may be targeted immediately after the announcement. Additionally, the subsequent integration of the acquiree's legacy systems or applications may introduce malware and or other vulnerabilities to the acquirer.

QUESTIONS FOR DIRECTORS TO ASK MANAGEMENT

Transaction life cycle phase	Questions for directors to ask management
Strategy and target identification	▶ Have we evaluated all relevant publicly available information on the target's cyber "history"? Possible sources include ratings, news stories, and publicly available regulatory filings, for instance. ▶ What is the company's cyber reputation as perceived by customers, suppliers, and other key stakeholders? ▶ What is the range of the potential financial impact of the identified cyber risks? ▶ What cyber-related legal and regulatory requirements are applicable to the company?
Due diligence and deal execution	▶ Have we conducted a detailed cybersecurity assessment? What did it cover? What were the findings? How did the findings stack up against our own standards? ▶ What measures will we and other key parties (target company, advisors, etc.) be taking to guard against the risk of cyberattacks during the transaction process?
Integration	▶ What cybersecurity issues have arisen that were not previously identified? ▶ What is the status of key milestone attainment? ▶ Have our new employees been trained to our standards for cybersecurity?

Directors should expect management to conduct a cyber-risk assessment for each phase of the transaction life cycle to confirm systems and processes are secure, and to quantify the risks that may impact the company *after* the deal closes, impacting revenues, profits, market value, and brand reputation.

The table on page 63 outlines a few suggested steps that directors can ask members of management at each phase of the deal cycle. Further details are provided on the following pages.

STRATEGY AND TARGET IDENTIFICATION PHASE

The risk of attack may start even before an official offer or merger announcement is made. Sophisticated attackers look for hints that a company is considering a merger, acquisition, or divestiture. They may be tipped off by industry chatter, a slowdown in a company's release cycle, staff reductions, or data leakage through social media channels.

The fact gathering in the earliest stages of the transaction should involve legal, corporate development, and security specialists. This process should identify and evaluate all relevant publicly available information on the target's cyber "history," including any disclosed or rumored undisclosed breaches. By using analytics to monitor social media, the acquirer can also access real-time information on how a target's cyber reputation is perceived by customers and its marketplace.

During the strategy and target identification phase, management should therefore gain an understanding of cyber risks associated with the target company and can perform the following analyses even before direct engagement with the target company:

- **Model the financial impact of identified cyber risks:** Risk factors, vulnerabilities, and consequences need to be analyzed and quantified. This should include cyber-risk models that can reflect not only the impact on a company's return on invested capital, but also the results of loss of competitive advantages, costly remediation, fines, and possibly years of litigation, depending on what was stolen.
- **Understand the cybersecurity regulatory environment of the target company:** Cybersecurity regulations at the state level in the United States vary widely, and each industry faces an increasing number of US federal regulators. Breaches of the European Union's Global Data Protection Rule (GDPR) can lead to potentially massive penalties (up to 4% of a company's revenues), representing a significant risk that boards should understand before moving forward with any acquisition involving access of data of European individuals.

The most fundamental step for managing information and privacy risks related to the transaction is understanding what types of data the target organization creates, receives, and collects as part of its business processes.

As a starting point, companies should consider requesting the target's data inventory that identifies the types of data that are most critical to the target organization (e.g., intellectual property, financial documents); require special handling or protection (e.g., personal data); or are required by law or regulation (e.g., records).

Organizations are increasingly using advanced text analytics and various artificial intelligence technologies to inventory and classify data. Search criteria and predictive analytics are established to explicitly identify types of data and where the data is stored.

Knowing what data the target organization holds is of limited use unless management also knows where it is. Devices that are commonly not identified include laptops and phones. Organizations that cannot efficiently locate personal data will be hard-pressed to demonstrate compliance with privacy regulations.

Protecting the privacy of customer and employee data is impossible without appropriate technical and organizational security measures. The target should have controls in place to ensure that personal data is safeguarded from unauthorized access, processing, destruction, and damage.

Finally, the acquirer should understand the target's controls over disposition of data once it exceeds retention requirements and need not be preserved under any legal hold.

DUE DILIGENCE AND DEAL EXECUTION PHASES

During these phases, cybersecurity due diligence is critical. Significant identified problems would call for negotiation of a reduction in purchase price to cover costs of necessary remediation. Depending on the risks identified, the board may request that management address identified matters through a transitional services arrangement with each party's responsibilities clearly identified, may defer approving the transaction until remediation is complete, or may decide to back out of a transaction if the identified risks are too great to scope or assume. Due diligence teams can identify cyber risks by conducting a tailored cybersecurity assessment designed to identify these issues:

- Insufficient investments in cybersecurity infrastructure, as well as deficiencies in staffing, policies, etc.
- Lax cultural attitudes toward cyber risk
- Cybersecurity-related terms and conditions in customer and supplier contracts that have a potential financial impact or that could result in litigation for noncompliance
- Noncompliance with cybersecurity-related data privacy laws or other applicable regulations and requirements
- Recent data breaches or other cybersecurity incidents

The acquirer's assessment would review the security architecture, conduct forensic analysis on key network devices, and review logs looking for any indication the target might already be compromised. It should also include a review of recent or ongoing breach responses, tools, policies, and regulatory positions to identify security gaps, risks, and potential liabilities.

Acquirers may consider establishing a contingency fund to be held in escrow for potential exposures that may occur after closing. Where there has been a recent breach, the assessment should also reveal if the target has appropriately remediated to prevent a recurrence. Boards should not, however, assume that on-site assessments are guaranteed to identify all deficiencies. The nature of due diligence means the assessment team may not be given access to interview key security personnel who are not aware of the potential acquisition. Additionally, the assessment represents only a snapshot in time and may well lack historical context of past issues.

Prioritization will certainly be a necessary key judgment. Some issues may need to be addressed immediately if the acquired company is going to be integrated within the short term. If the entity is to be run as a separate, wholly owned subsidiary, however, the target's risks may potentially be "quarantined."

Acquirers should fully understand the target company's requirement for domestic and global compliance and reporting. The acquirer must not only understand any new regulatory requirements, but must also demand information on any recent, current, or anticipated engagements with regulators due to cyber incidents.

Acquirers should consider conducting "dark web" (anonymously run and difficult-to-access websites favored by hackers) searches about the target, their systems, data, and intellectual property. This helps identify whether the company is already on attackers' radars, whether its systems or credentials are already compromised, or whether its sensitive data is for sale or being solicited.

Acquirers should also consider engaging vendors specializing in researching malware infections to look for infections in the target company and for any holes in their defenses that are visible from the outside. This cybersecurity hygiene-related information is publicly available and can be used to compare one company to another, allowing management to save time and energy by not pursuing companies whose risk profile is unacceptably high.

Evolution in the legal landscape must be taken into account for effective due diligence. For example, the US Securities and Exchange Commission's 2018 Cybersecurity Guidance states that companies should consider disclosing risks arising from acquisitions in the Risk Factors section of their periodic filings. Moreover, a proposed SEC rule that could be adopted in 2023 includes instituting a four-day timeframe after a determination that the incident is material for publicly disclosing significant cybersecurity incidents. Understanding the acquiree's processes for internal escalation and evaluation may help determine if such a timeframe would be achievable.

After the public deal announcement and before close and subsequent integration, new threats may emerge. Malicious actors know that there will be security audits in this period and an associated granting of temporary network access to outsiders. They may look to take advantage of the situation to penetrate networks in this period.

INTEGRATION PHASE

Once the organization has made the decision to acquire, it needs a plan to remediate compliance concerns, address risk exposure, and integrate security operations—where appropriate. This starts with a consolidated technology, security, and operations road map.

Acquirers should consider the merits of maintaining discrete operations with separate business and operating models. If the assets of the target will merge with core business operations, then integration is called for.

Aside from traditional post-deal integration challenges related to people, processes, systems, and culture, an additional cyber risk accrues to both companies on the day the deal is announced. On Day One, they become a target for social engineering attacks by those seeking to use the acquiree as a back

door into the parent. Attackers will also seek to take advantage of the inconsistencies that exist between the platforms and technology operations of the two companies. The sooner the parent company can integrate the target company into their security environment, the better.

Many integration activities are complex and could take a year or more to complete. Integration teams need to have the cyber expertise to address these issues:

- Security gaps identified during preceding phases
- Prioritization of remediation activities based on potential impact of identified gaps
- Prioritization of integration activities
- Employee training on newly integrated systems

Over the first six months post integration, boards should pay particular attention to integration project milestones slipping due to lack of funding, which is often a result of overly optimistic cost estimates. Such underestimation is common when estimates are created from incomplete knowledge inherent in a closely held due diligence process.

However, there must also be a Day One integration plan to extend as much of the acquirer's cyber protections as possible to the target company immediately. At a minimum, the plan should include these steps:

- Exchange of threat information to include Internet domains to be blocked.
- Conduct employee awareness training emphasizing the risk of phishing attacks mimicking emails from the new parent company and other new risks. As companies combine their IT departments, hackers may use this time to impersonate administrators.
- Perform a much deeper on-site assessment to further refine risks and integration costs.
- Reengagement with the open-source research vendors recommended during due diligence to identify spikes in indicators of cyber risk—a sudden increase in hygiene-related traffic after an announcement could be an indirect measure of other malicious activity.
- Ideally, routing the target company's email through the parent company's email screening process if that capability exists is desirable.

During this phase, it is also important to perform an operation-focused gap analysis to determine if one company has certain cyber capabilities or processes that the other does not have or that the combined organization could benefit from long term. If this is the case, the transaction is an ideal time for business changes or transformational activities to add value to the combined organization.

Acquirers should consider the benefits of leveraging cloud services to integrate the combined companies' applications and data faster. This can result in more rapid realization of synergies, less reliance upon third-party services, and potentially a reduction in overall risk through an organization hosting its own data applications.

CONCLUSION

Cybersecurity diligence during M&A calls for a two-pronged approach. Companies must conduct rigorous due diligence on the target company's cyber risks and assess their related business impact throughout the deal cycle to protect the transaction's return on investment and the entity's value post transaction. In addition, all parties involved in the deal process need to be aware of the increased potential for a cyberattack during the transaction process and should vigilantly maintain their cybersecurity efforts. Applying this two-pronged approach during M&A will serve to ultimately protect stakeholder value.

ENDNOTES

[1] Rob Gurzeev, "It's time to better identify the cost of cybersecurity risks in M&A deals," posted on techcrunch.com on September 10, 2020. (https://techcrunch.com/2020/09/10/its-time-to-better-identify-the-cost-of-cybersecurity-risks-in-ma-deals/)

[2] Forescout Technologies, *The Role of Cybersecurity in Mergers and Acquisitions Diligence* (Forescout Technologies, 2019). (https://www.forescout.com/resources/cybersecurity-in-merger-and-acquisition-report/)

[3] Julian Meyrick, Julio Gomes, Nick Coleman, and Stephen Getty, *Assessing Cyber Risk in M&A: Unearth Hidden Costs Before You Pay Them* (IBM Corporation, 2020) (https://www.ibm.com/downloads/cas/RJX5MXJD)

TOOL H

Building a Relationship With the CISO

By J. R. Williamson, Leidos

INTRODUCTION

As corporate information security functions mature, board directors must ask themselves how they can effectively communicate with the security team. The individual occupying the lead position, typically the chief information security officer (CISO), manages vast numbers of operational, reputational, and monetary risks. The scope and importance of the CISO's work behooves directors to form a candid relationship with this functional leader in the interest of performing effective cyber-risk oversight. Accordingly, many board members are establishing an ongoing relationship with the CISO not only through full-board and committee meetings, but also outside the boardroom.

Different organizations and business processes require unique strategies and assessment depending on inputs like size, industry, value, risk tolerance, and threats. To help the board assess risk the CISO should have clear and consistent communication with the board that conveys the health and maturity of the cybersecurity program and calibrates risk tolerance for the corporation. This will also help the CISO effectively manage cybersecurity governance, performance, and risk management.

The board building strong working relationships with the CISO and their cybersecurity team goes hand-in-hand with establishing a strong culture of cybersecurity throughout the company—and including within the board itself. Having a visible relationship between the board and the CISO makes it very clear to the whole company that cybersecurity is worthy of their time. Today's CISOs need to be much more than just technical specialists in "security." To be effective, they need to be program managers, people developers, relationship builders, culture leaders, risk managers, strategists, industry luminaries, and growth oriented.

This tool offers guidance on how boards can more effectively establish a relationship with their organization's CISO and security team in order to establish an agreed-upon risk tolerance profile for the organization, and assist in defining a requisite culture of cybersecurity. The questions below are stated as if a board member were asking the CISO a question. Most questions are followed by a bullet explaining the "why" behind the question to be asked. Because not every question will have relevance for every organization, directors should select those most appropriate to the issues and circumstances at hand.

UNDERSTAND THE CISO'S ROLE AND MANDATE

To build an effective relationship, the board needs to understand what the CISO does, what challenges they are facing, and what resources and support they have available to most effectively meet the needs of the corporation.

- What is your charter and scope of authority in terms of resources, decision rights, budget, staffing, and access to information? How does this compare to leading practice in our industry and generally?
  - Answers to these questions will help the director asking the question, and the board, establish a strong understanding of the CISO's role and the tools they have at their disposal to effectively manage cybersecurity risk. That's the first step in relating to them: building advocacy and trust.

- Who are you reporting to now, and has that changed in the past five years?
  - There is no clear industry consensus on this topic. By far, the largest percentage report to the CIO, although there is a growing perspective that reporting to the CIO might not be the right answer. It is certainly true that a CIO might well have a conflict of interest between IT service delivery pressures, cost, customer experience, and security. Those factors need to be weighed against the value of having the CISO's supervisor being able to understand the technology and business risks and being capable of arbitrating trade-offs without escalating issues to the CEO for resolution. Some technology-oriented companies are now having the CISO report to the chief technology officer (CTO) to help ensure that cybersecurity is not just another risk management issue, but is also more directly incorporated into product development life cycles and portfolio strategies, frequently as a differentiator among the company's market competitors. Ultimately, the age-old tension between user experience and security remains, regardless of whom the CISO reports to, and an enlightened CISO understands that all solutions need to be both safe and performant. A key consideration for CISO reporting lines is whether or not that person has a strong voice on the executive leadership team to advocate appropriately for security. If the person representing the CISO at the executive level cannot influence the CEO and CFO, a security program cannot succeed.
- How is the organization's cybersecurity budget determined? What is its size and how does this figure compare with leading practice in a company's particular industry and generally? Is the level of funding aligned to the desired performance maturity for the information security program? Is the level of funding commensurate with the expected risk profile for the company?
  - Comparing these figures with industry spending trends is probably the best way to understand the adequacy of funding. CISOs will not typically ask the board for funding—that is a responsibility for management to address—but directors can certainly do their homework to understand whether or not the CISO's role can actually be effective given the funding levels provided by the organization and influence the CEO and CFO as required.
- How much of the security infrastructure is outside of your budget or directive authority as CISO?
  - Threats always evolve faster than the budget cycle. If a CISO is in the position of frequently asking others in the IT organization to upend their annual plans to accommodate emerging security needs, the chances of the changes being rejected are increased. Conversely, the more the CISO is in a position to make budget trade-offs internally in real time, the more rapid the response and the lower the risk. This situation is particularly true outside upper management, where the lines of business frequently have more decision-making authority for product security trade-offs. For this reason, many leading organizations are approaching cyber-risk budgeting on a team basis as opposed to strictly as part of the IT budget.
- Which security tools or other investments were below the "cut" line in the budget?
  - Management is always eager to tell a board what they are doing, but are less eager to discuss what they are not doing. A conversation about what fell below the cut line and what decision process was used to evaluate trade-offs will always be illuminating. This conversation should

be anchored in planned risk-reduction initiatives and maturity road maps for appropriate decision calibration. Directors should be cautious about putting the CISO into a difficult spot with their CEOs and CFOs regarding spending decisions, but should certainly consider asking questions about how priorities are being resourced and in what time frame. The CISO will likely consider the board as an ally in building consensus on critical priorities, which will build trust and strengthen the relationship versus putting the CISO in an awkward position of pointing any fingers at the CEO or CFO for failure to fund a critical security project that is aligned to a key enterprise-risk-reduction initiative.

- What role do you, as the CISO, play in the organization's enterprise risk management (ERM) structure and in the implementation of ERM processes?
  - Directors should probe to see if the CISO is just a contributor to the ERM process, or if they are part of the adjudication and risk decision making. What role, if any, do you as CISO play beyond setting and enforcing cybersecurity policies on the enterprise network and related control systems?
  - For example, does your CISO hold accountability for adjudicating cybersecurity risk associated with the organization's brand? If applicable, is the CISO part of the attestation for the annual Sarbanes Oxley filing, or only the CIO? Is the CISO accountable for the Securities and Exchange Commission (SEC) Form 10-K portion related to cybersecurity posture assessment for the year, or for any specific Form 8-K filings (in partnership with the legal department)?
- As CISO, do you provide input on the development process for new products, services, and systems? How about on the design of partnership and alliance agreements, etc., such that cybersecurity is built in rather than added on after the fact?
  - Your CISO's answer will be revealing about the extent to which the information security program is operational within the lines of business applications.
- As CISO, do you have a role in evaluating the cyber risk of acquisitions during due diligence? How about in the acquisition of new products or development of new business strategies—are you able to state strategic concerns about supply chain cybersecurity during discussions about those decisions?
  - Whether the company is acquiring another business, or entering into a new business agreement to acquire new software, CISOs should be involved in vetting cyber risk.
- Does the CISO get invited to meet with key external customers to either support a sales/capture activity or as a trusted advisor to the customer on matters of cybersecurity? How strong are your relationships among the C-suite and the executives and leaders of other key business functions in the company?

SPEND TIME WITH THE CISO AND THE CYBERSECURITY TEAM OUTSIDE OF THE BOARDROOM

With packed board meeting agendas, it is unrealistic to think that the board can get sufficient insight into a company's cybersecurity posture through quarterly presentations. Board members should arrange to visit the security team and receive orientations firsthand from personnel situated on the front lines of cybersecurity. These sessions will provide valuable insights and learning opportunities for board members far beyond what they could obtain from highly scripted board presentations. The security team will appreciate it, too, since visits like this can increase its visibility, raise morale, and reinforce the need to focus on this area. The board's greater familiarity with the team's mission and key security leaders will pay huge dividends when a crisis occurs. A crisis is the wrong time for directors to get acquainted with the CISO and key staff, their programs, and their relationship network across industry, customers, suppliers, and partners that may be able to help.

- Many security teams routinely produce internal reports for management and senior leadership on cyberattack trends, incidents, and threats. Directors can discuss with the CISO, corporate secretary, and board leaders whether this information might be relevant and useful to include in board materials.
- CISOs spend a great deal of time assessing risk, building threat models, and conducting exercises to test the effectiveness of cybersecurity controls. This is a great area for directors to engage the CISO and their team outside of the boardroom, not only to directly deepen their engagement but also to indirectly learn about potential future business risks that might not normally come up during a more formal briefing to the board.

CISO AS COMPLIANCE CZAR?

All CISOs have to become compliance experts, but nobody really likes talking about compliance! Engaging the CISO to better understand the cyber regulatory landscape that the business is facing is one way to wade into that conversation and deepen the relationship with the board. In the United States and other places around the globe, there is increasing cybersecurity legislation that has to be considered, understood, influenced, and addressed tactically and strategically across the enterprise (e.g., the White House through executive orders, specific US Government Agencies and Departments regulatory requirements, as well as state and local regulatory expectations). The CISO should be conversant in these regulations and how their team is working to build compliance into other security practices. For more on the nuances of compliance, review Principle 2.

ASSESS THE CYBERSECURITY CULTURE

CISOs and their security teams occupy one of the most high-stress positions in an organization. In many companies, the threat never really stops, so there is an expectation of being available 24/7/365. Too often, these cybersecurity teams do not receive adequate internal support and are blamed when there are system failures or performance issues that they did not cause. Low morale not only leads to high turnover but also frequently leads to lower efficiency and increased risk. Partnership and support is essential for a healthy environment where these highly skilled workers can be effective and thrive. Questions for CISOs aimed at assessing the cybersecurity culture follow.

- How does your broader team collaborate with other departments and corporate functions on cybersecurity-related matters?
  - The CISO's answers will indicate how fully the security function and other departments cooperate and coordinate, including with:
    - IT operations to ensure that service capabilities and business applications are both performant and safe;
    - business development regarding due diligence on acquisition targets and partnership agreements (provide reusable cyber capabilities if cyber risk is a key aspect of the bid);
    - internal audit regarding the evaluation and testing of control systems and policies;
    - human resources for cyber workforce strategy, organization-wide cybersecurity culture and training, and employee development;
    - technology development of cyber proof points for our own cyber products and capability requirements for research and development;
    - purchasing and supply chain regarding cybersecurity protocols with vendors, customers, and suppliers; and
    - legal regarding compliance with regulatory and reporting standards related to cybersecurity, as well as data privacy.
- What direct support do you receive from the CEO, CIO, and senior management team, or are they only called onto the carpet when something breaks or a major breach has occurred?
- How do you measure and/or track maturity?
  - Boards should not assume that high-performing organizations track maturity in only one way, or that the measure of a mature cybersecurity program occurs by simply counting all the tools that they have deployed or how many people that they have on their team. Maturing cybersecurity programs focus not just on defensive technology, alerting, and incident response; they also focus on improving processes that help to incorporate standard cybersecurity practices throughout all of the critical business workflows and activities. They focus on talent, risk, and culture. They have a mindset of continuous improvement and innovation. The board can tap into this understanding to help build synergy and partnership with the CISO on moving the needle on key enterprise risks.

- Do you or the information security team participate in cybersecurity information-sharing initiatives (e.g., industry-focused, cyber-community-focused, or public-private partnerships)? How is the information that is gathered from participation in such initiatives used and shared within the organization to improve understanding and capability maturity?
  - As challenges increase in complexity and scale, industry cooperation and information sharing about threats will become a valuable tool in the CISO's kit.
- Do you or a partner in your team have relationships with public-sector stakeholders such as law enforcement agencies (e.g., FBI, INTERPOL, US Secret Service, DHS/CISA, NSA), regulatory agencies' cybersecurity divisions, the US Computer Emergency Response Team (US-CERT), etc.?
  - Similar to cooperation with private industry partners, cooperation before an attack happens is becoming a pillar of sound security practices. See Principle 6 for more reasons to engage in cooperative relationships with these agencies.
- How often do you chat with CISO peers in your network about the challenges they are facing? What kind of peer exchange groups do you participate in that touch on risks facing our industry?
  - Cyber capability can definitely be a competitive differentiator for companies in cyber product markets, but when it comes to dealing with common adversaries across any industry, it is important that the CISO and their team establish very strong, noncompetitive relationships with peer companies for threat intelligence information sharing for collective defense. These relationships are essential for both program and cultural maturity at all levels of the cybersecurity team, and work toward cooperative security.

DEEPEN THE RELATIONSHIP: MAKE THE CISO A STRATEGIC PARTNER

Like with all strategic partnerships, the relationship with the CISO needs to address the three "Cs": communication, collaboration, and coordination. These Cs enable the context for establishing independent roles but with shared benefits to the organization for managing contributions to stated strategic outcomes and risks. Start with a discovery session to gain a deeper understanding of what the risks are and align those to the board's strategic outcomes—this is where we can identify the partnership opportunity.

As noted earlier, one of the ways to engage strategically on information security topics is to focus on maturity and not just capability. CISOs tend to talk about capabilities, so getting them to talk about the overall information security program forces the conversation away from technology and more toward people, process, and purpose. Ultimately, the tools available will not make your program mature. Rather, it's the people and the processes, and how effective we are in using those to address business risks and strategic outcomes, that lead to success.

- Where have we made the most progress on cybersecurity in the past 12 months, and to what factor(s) is that progress attributable? Where do our most significant gaps remain, and what is our plan to close those gaps? Are the gap closure plans getting appropriately resourced, or are those falling below the line of budget affordability? With whom is the CISO partnering to affect needed change throughout the organization? Is their relationship network up to the task?

- What is our cybersecurity workforce strategy? Do we have a strategy to recruit, retain, develop, and grow our personnel? With a decades-long war on cyber talent, mature programs are the ones that focus on talent and creating a culture where that talent can thrive and not just survive. When people are happy, they bring their whole selves to work, and that energy and commitment can really drive maturity around the mission.

The effectiveness of the program is the key metric. Once an organization has a well-educated and motivated workforce, it can turn its attention to process maturity. An organization can be very good at what they do, but may not be very efficient or consistent in how they do it. Here is one area where you can focus on process performance with the CISO and their team to align with board objectives on performance and strengthen the cybersecurity program by aligning it with board performance objectives. In addition to implementing more automation to free up personnel to work on harder, human-powered activities, one area to focus on in this category is analyzing where we have "escapes" in the cybersecurity program—weaknesses in the program where effectiveness has eroded. Where are those exceptions that are driving the most risk? CISOs live these issues every day and have a stong interest in engaging with the board to help determine where the lines should be drawn in the sand for shared accountability and/or risk acceptance with the other corporate functions and lines of business.

- What organizations or locations have been exempted from one (or more) cybersecurity control for business reasons?
  - For example, directors may hear CISOs mention topics such as critical applications only being patched during quarterly maintenance windows, research organizations bypassing Internet filtering, or factory systems not being scanned. While directors may not be familiar with the technical reasons behind why these are poor practices, they should understand that such exceptions to policy and controls increase the overall risk to the enterprise. Regardless of whether such exceptions are valid, management and the board need to be aware of the scope of the risk.

Finally, engage with the CISO as an expert, not just in the information security technologies arena, but also in emerging trends that could influence the competitive marketplace. Is there potential leverage for what we do internally to aid our external pursuits? Are there key external partners that can help us be successful? These types of conversations lead to a more strategic dialogue with the CISO on how they can partner with the board to achieve these shared outcomes/objectives.

TOOL I

Enhancing Cybersecurity Oversight Disclosures—10 Questions for Boards

By Robyn Bew, EY

Note: This tool was adapted from How Cyber Governance and Disclosures are Closing the Gap*, a publication released by EY's Center for Board Matters, September 2022.*

This tool provides questions for directors to consider in preparing proxy statement or other disclosures related to the board's oversight of cybersecurity. It includes proxy statement disclosure data from US large-cap companies between 2018 and 2022, which boards can use for benchmarking purposes.

Cybersecurity remains front and center on corporate agendas, as risks and regulatory requirements both continue to proliferate. In global surveys of CEOs and business leaders, cyber incidents are consistently named as a top threat to business, edging out pandemic-related health risks, supply chain disruptions, and even macroeconomic volatility.[1]

Investors and other stakeholders are paying attention, seeking more information on how boards and company leaders are overseeing and managing cyber risks. BlackRock, the world's largest asset manager, has stated, "[We believe] that data security is a material issue for more and more companies and regularly [engage] boards and management teams regarding the oversight and management of data privacy and security, crisis preparedness and response as well as related company disclosures."[2] In 2021, Institutional Shareholder Services (ISS) added 11 factors concerning oversight and management of information-security risk to its Governance QualityScore rating methodology.[3] And in March 2022, the US Securities and Exchange Commission (SEC) proposed new rules that would require expanded cybersecurity-related reporting by public companies, including board oversight disclosures (see sidebar below).

THE SEC FOCUSES ATTENTION ON BOARD-LEVEL CYBERSECURITY OVERSIGHT

On March 9, 2022, the SEC released proposed rules that would enhance and standardize public-company cybersecurity disclosures. Elements of the proposed rules that related to board oversight include new disclosures on these topics:

- How cyber-risk oversight responsibilities are assigned at the board and committee levels
- How frequently the board is informed about cybersecurity matters
- Whether and how the board considers cybersecurity risks in conjunction with business strategy, financial oversight, and broader risk management oversight
- The cybersecurity expertise resident on the board, if any, and the nature of such expertise

The proposal includes numerous other reporting requirements around cybersecurity incidents, incident materiality, company risk management and strategy, and management-level cybersecurity governance. The SEC stated in early January 2023[4] that it is aiming to publish a final rule by April 2023.

EY's Center for Board Matters has tracked large-cap companies' proxy statement disclosures related to cybersecurity oversight since 2018. The Center has seen steady and significant increases in disclosures in several key areas, including

- **Director skills and expertise:** disclosed by 61 percent of Fortune 100 companies in 2022, up from 35 percent in 2018;
- **Frequency of management reporting to the board:** disclosed by 68 percent in 2022, compared to 36 percent in 2018; and
- **Identification of a "point person" reporting to the board**, such as a chief information security officer: disclosed by 49 percent in 2022, up from 23 percent in 2018.

These increases in voluntary disclosures indicate that companies are responding to investor and stakeholder interest in how their boards are overseeing areas that are vital to the firm's business strategy and risk profile. Figure 1 (see page 78) contains more detailed findings from our large-cap company analysis, including references to oversight-related disclosures that are included in the SEC's proposed rules and ISS's list of risk factors.

Directors can use the 10 questions below to help inform boardroom discussions about opportunities to enhance cybersecurity-related communications with investors and other stakeholders.

1. **Do we understand the priorities of our company's major investors and other key stakeholders (suppliers, customers, employees, regulators, etc.) as they relate to cybersecurity, data privacy, and other key technology risk and strategy issues?**
2. **What feedback has senior management and/or investor relations received from our major investors? What questions are our top shareholders asking about how the company approaches information security and data privacy?**
3. **How is the company using disclosures to effectively communicate the rigor of our cybersecurity risk management program, and related board oversight activities, to investors and other stakeholders? What changes would be required in order to comply with relevant pending regulatory requirements, such as the SEC's proposed rules on cybersecurity disclosures issued in March 2022?**
4. **Is cybersecurity mentioned in the risk oversight section of the proxy statement?**
5. **Do we describe which board committee or committees have responsibility for oversight of cybersecurity matters? Do we describe how the full board is involved in cybersecurity oversight, in addition to the activities of key committees?**
6. **Is cybersecurity included in our board skills matrix, or other description of skills resident on the board? Do we identify one or more directors as having cybersecurity expertise, and the criteria by which the board defines such expertise? How does professional cybersecurity experience, credentials, or other knowledge appear in directors' biographies? Do we disclose any education board members receive on cybersecurity topics, such as briefings from external advisors, law enforcement, or other third-party experts?**
7. **Do we describe how the board and/or key committees receive information from management about cybersecurity matters? Do we describe how the board and/or key committees consider**

cybersecurity matters as part of their deliberations on strategy, financial oversight, and enterprise risk management?

8. How does the relative prominence and/or specificity of the cybersecurity risk factors in our quarterly and annual reports compare with those in our current enterprise risk assessments?
9. How do we describe cybersecurity risk management activities, including these:
   - **a.** Policies and procedures
   - **b.** Response planning, disaster recovery, or business continuity
   - **c.** Simulations and tabletop exercises related to cyberattacks or breaches
   - **d.** Education and training efforts
   - **e.** Information-sharing with industry peers, law enforcement, etc.
   - **f.** Use of an external independent advisor to support management and/or attest to cybersecurity assessment findings
10. How do our disclosures on board cybersecurity oversight compare to those of our competitors and industry peers?

FIGURE 1 FORTUNE 100 COMPANY CYBERSECURITY DISCLOSURES, 2018–2022

The following data is from an analysis of the 74 companies on the 2022 Fortune 100 list that filed Form 10-Ks and proxy statements in 2018, 2019, 2020, 2021, and 2022 (through May 31, 2022). Areas of focus were referenced in the SEC proposed rules and/or by ISS in its list of Governance QualityScore cyber risk factors released in February 2021.

Percentages based on total disclosures for companies. *Some companies designate cybersecurity oversight to more than one board-level committee.

Area of focus	Topic	Disclosure	2022	2021	2020	2019	2018
CATEGORY: BOARD OVERSIGHT							
	Risk oversight approach	Disclosed a focus on cybersecurity in the risk oversight section of the proxy statement	95%	88%	89%	86%	76%
SEC ISS	Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	88%	89%	86%	81%	72%
		▶ Disclosed that the audit committee oversees cybersecurity matters	70%	69%	68%	62%	57%
		▶ Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	28%	28%	24%	26%	18%

Area of focus	Topic	Disclosure	2022	2021	2020	2019	2018
SEC ISS	Director skills and expertise	Cybersecurity disclosed as an area of expertise sought on the board or cited in at least one director biography	61%	65%	57%	49%	35%
		▶ Cybersecurity disclosed as an area of expertise sought on the board	46%	42%	36%	27%	20%
		▶ Cybersecurity cited in at least one director biography	51%	55%	46%	39%	28%
SEC	Management reporting structure	Provided insights into management reporting to the board or committee overseeing cybersecurity matters	74%	65%	61%	58%	54%
		▶ Identified at least one "point person" (e.g., the chief information security officer, chief information officer)	49%	41%	35%	32%	23%
SEC ISS	Management reporting frequency	Included language about frequency of management reporting to the board or committee(s)	68%	54%	47%	43%	36%
		Disclosed reporting frequency (e.g., annually, quarterly)	39%	31%	15%	15%	11%
CATEGORY: STATEMENTS ON CYBERSECURITY RISK							
	Risk factor disclosure	Included cybersecurity as a risk factor	100%	100%	100%	100%	100%
		Included data privacy as a risk factor	99%	99%	99%	97%	93%
CATEGORY: RISK MANAGEMENT							
SEC ISS	Cybersecurity risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures, and systems	99%	97%	93%	91%	85%
		Disclosed alignment with external framework or standard	18%	9%	3%	3%	1%
		Referenced response readiness, such as planning, disaster recovery, or business continuity considerations	66%	65%	61%	57%	53%
		Stated that preparedness includes simulations, tabletop exercises, or response readiness tests	9%	5%	7%	3%	3%
		Stated that the company maintains a level of cybersecurity insurance	51%	43%	36%	36%	31%
		Included cybersecurity in executive compensation considerations	7%	11%	5%	1%	0%

Area of focus	Topic	Disclosure	2022	2021	2020	2019	2018
ISS	Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	45%	36%	30%	26%	18%
	Engagement with outside security community	Disclosed collaborating with peers, industry groups, or policymakers	15%	12%	11%	12%	7%
SEC ISS	Use of external advisor	Disclosed use of an external independent advisor	28%	22%	15%	12%	15%
		▶ Disclosed board engagement with an external independent advisor	7%	7%	4%	3%	1%
		▶ Disclosed the external advisor provided attestation	14%	8%	4%	4%	4%

ENDNOTES

[1] See the *Allianz Risk Barometer 2022* (Allianz Global Corporate and Specialty SE, 2022), p. 3 (https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2022.pdf), and Tim Human, "CEOs name cyber-risk as top threat in 2022, survey finds," *Corporate Secretary*, Feb. 2, 2022. (https://www.corporatesecretary.com/articles/technology-social-media/32890/ceos-name-cyber-risk-top-threat-2022-survey-finds).

[2] BlackRock Investment Stewardship, *Our approach to data privacy and security* (BlackRock Inc., 2022), p. 2. (https://www.blackrock.com/corporate/literature/publication/blk-commentary-our-approach-to-data-privacy-and-security.pdf)

[3] Chuck Seets and Pat Niemann, "How cyber governance and disclosures are closing the gaps in 2022," posted on ey.com. (https://www.ey.com/en_us/board-matters/how-cyber-governance-and-disclosures-are-closing-the-gaps-in-2022)

[4] See more about the proposed rulings at this URL: https://www.reginfo.gov/public/do/eAgendaMain?operation=OPERATION_GET_AGENCY_RULE_LIST&currentPub=true&agencyCode=&showStage=active&agencyCd=3235&csrf_token=3E2CBC6FB8F5C172183CFD451BB972376A7E3CEC1B3F3B25CAC19245031A81368C69BF9DA8091F129A9842E-71542A76E8F2

TOOL J

Securing Cloud Services

By Vinay Puri and Jason Escaravage, Thomson Reuters

Adoption of cloud computing services (or "the cloud") continues to expand rapidly across industry. As companies migrate legacy capabilities and services to these new environments, they must develop new programs and capabilities to manage emerging cloud-centric risk patterns. This tool provides a high-level overview of the risks and a set of questions to help board members evaluate management's approach to securing their new cloud services.

Understanding the full spectrum of cloud services is challenging, as they come in many shapes and sizes. Cloud services can be a single virtual whiteboard application that allows remote workers to collaborate, a fully managed enterprise resource planning (ERP) platform, or a massive-scale hosting environment that replaces an organization's data centers. Whatever the application, what makes the cloud different is it puts a tremendous amount of power in the hands of each engineer or developer, allowing them to "point, click, and configure" individual cloud services to meet their business need. Unfortunately, this flexibility also creates risks where a single change or misconfiguration can inadvertently create a weakness that exposes the cloud services, the processes they enable, or the data they manage to risk.

Common patterns of cloud risks or threats include these:

- **Misconfigured resources**: Inappropriate configurations can lead to access by unauthorized third parties; consume expensive processing resources, causing unplanned costs; or add unapproved applications to the company's cloud environment, creating license risks.
- **Data leak or breach**: Failure to encrypt, secure, or properly manage cloud-based data storage or processing resources can expose sensitive data and trigger data breach notifications.
- **Malware infections**: Malicious software installed on unprotected cloud resources can spread "up-stream" into the organization's data centers due to connectivity between the cloud and data environments physically located within an organization's premises.
- **Insufficient identity and access management controls**: Gaps in managing user identities and confidential information across services can expose corporate assets that are lacking appropriate authentication and access management controls.

CASE IN POINT

A US-Based Financial Corporation Exposed 100+ Million Personal Records Due to a Misconfigured Cloud Resource

A large financial corporation agreed to pay $190 million to settle a class-action lawsuit that customers filed against the firm after a hacker broke into its cloud-computing systems and stole their personal information.

The hacker broke into the company's cloud-computing systems and stole files containing the customers' personally identifiable information (PII), including credit card applicants, payment card transaction history, contact information, and credit scores, along with more than 100,000 Social Security numbers. The unauthorized access took place on March 22–23, 2019, when the attacker exploited a firewall misconfiguration which permitted commands to reach the impacted server. Overall, the cyberattack exposed the personal data of more than 100 million customers.

Source: "Capital One Settles Class-Action Cyber Lawsuit for $190 Million" Jennifer Surane on Bloomberg, December 23, 2021.

QUESTIONS BOARDS SHOULD ASK MANAGEMENT ABOUT THEIR CLOUD SECURITY STRATEGY AND CONTROLS

The questions below are designed to help directors gain an understanding of their organization's cloud computing strategy and the programs, controls, capabilities, and resources that the organization and its management have employed to mitigate the risks associated with the strategy.

1. **Are we adopting cloud-first strategy (i.e., all new assets in the cloud) or hybrid strategy (where we have some assets in cloud and some in traditional data centers)?** Additional follow-ups include these:
   - **a.** What percentage of our total assets are based in the public cloud today versus our existing data centers (e.g., 50-50%, 70-30%, 90-10%?)? What is our forecast over the next three years?
   - **b.** What percentage of our revenue-generating assets are hosted in public cloud environments today, and what is our forecast over the next three years?
2. **What were the major factors that drove the decision to migrate and expand adoption of cloud services?**
   - **a. Elasticity:** Was the ability to rapidly scale to support increasing customer demands, integrate new acquisitions, or expand to new geographies critical to the decision?
   - **b. New Innovations:** Was there the desire to take advantage of the cloud service providers' investments in emerging capabilities and services?
   - **c. Compliance and Security:** Did the significant investment in security controls and existing compliance with prevailing standards and frameworks (e.g., ISO, NIST, FISMA) that cloud providers are held to play a role in the decision?
   - **d. Reduce Cost by Divesting Our Expensive Data Centers:** Were we able to increase capacity requirement with this choice? Did it allow the reduction of constant technology changes (hardware and software refreshes), data center contract renewals, and other challenges?
3. **What types of business processes are we using cloud-based resources to create or refine?** Is it our plan to
   - **a.** use limited Software as a Service (SaaS) for employee productivity and back-office processing;
   - **b.** use cloud services to store, process, and manage our sensitive confidential information;
   - **c.** host, process, and control our customers' sensitive information in cloud services, and/or
   - **d.** exit our current data centers and shift all hosting services to public cloud service provider environments?
4. **Do we understand our SaaS ecosystem, and how and where each cloud service provider is storing our sensitive data for each of these functions?**
   - **a.** Corporate Systems (e.g., ERP, HR, Payroll)
   - **b.** Productivity Tools (e.g., MS Office, Google Suite)
   - **c.** Sales & Marketing (e.g., pricing, orders, etc.)
   - **d.** Customer Master Data (e.g., customer lists)
   - **e.** Products and Applications (hosted environments)

5. **What's is the organization's strategy for partnering with major cloud service providers (CSPs)?** Items to consider are listed below:
   a. How are we avoiding CSP concentration risk? What percentage of our services are deployed in AWS, Azure, the Google Cloud Platform, and/or other cloud environments?
   b. Are all our cloud services in one cloud environment that is hosted in one geographic location or are they dispersed geographically? How is the organization avoiding the risk of data centers being concentrated in one locality?
   c. What security certifications and accreditations do our CSPs maintain?
   d. Do we have a decision tree that would suggest the best CSP provider for our organization?
6. **What level of support have we contracted with our core cloud service provider (e.g., Platinum, Gold, etc.)?**
   a. Does that support level meet the demands of our risk appetite?
   b. Do we have well defined SLAs to meet the optimum level of service availability?
7. **Do we have clear roles and responsibilities defined between the organization, the CSPs, and third-party vendors?** Are contracts for services aligned to a shared security responsibility model?
8. **How is the organization managing top cloud security threats and risks including, but not limited to, data exposure?** Some tactics that boards can ask about include these:
   a. Data protection and compliance programs driven by staff
   b. Embedding industry aligned, cloud security framework-based requirements in the contracts
   c. Managing and tracking cloud spending via cloud cost management tools
   d. Building strategic partnerships for faster access to capabilities
9. **How are we governing CSPs?** Tactics for boards to listen for when management discusses CSP governance include audits/review, quarterly business reviews, and service reviews by contract service level agreements.
10. **Does our organization have the right expertise in cloud to support the business and cloud strategy?** Directors and management should scan the talent in the organization to see if it retains leaders with deep experience in cloud and if the organization provides programs to incubate and maintain internal talent, such as online subscription-based training and certification-based programs and attendance at vendor conferences with training programs.
11. **How does our cloud strategy support our customers' needs while also enabling our organization's workforce to better serve themselves and others?** Some benefits of cloud computing to the workforce and customers include the following:
    a. Brings the organization closer to users/customers
    b. Supports data localization laws and regulations
    c. Enables hybrid working in a secure way
    d. Breaks the barrier of cost around training IT and security staff on management of on-premises data servers

12. **How are we measuring our cloud spend and savings generated?** Consider asking management if the following standards are being met during measurement:
    a. Processes are established to monitor trends and modify the license agreement
    b. Enforcing tagging standards across the organization
    c. Persistent tracking with a cloud cost management tool that is also shared with users to monitor their own cloud consumption and spend

TOOL K

Supporting National Security, Working with CISA, and Having a Conversation with Your CISO

By CISA Staff

Cybersecurity is a shared responsibility. This tool will help board members understand their role in supporting national security and the role of the Cybersecurity and Infrastructure Security Agency (CISA) in supporting industry. In addition, the tool includes questions to guide a conversation with your chief information security officer (CISO) that can help your organization to go a level deeper and shed additional light on the company's security program.

NATIONAL SECURITY IS A SHARED RESPONSIBILITY

Now, more than ever, cyber risk extends beyond the boundaries of an enterprise to affect other companies and the functions of society. As highlighted by Principle 6, it's critical for businesses to embrace corporate cyber responsibility as a matter of good governance and to collaborate closely and continuously with the government and industry partners to address cyber risks, particularly those with national security and societal implications.

WORKING WITH CISA

As the nation's cyber defense agency, CISA provides an array of services to help companies address cyber risks:

- **Stay aware of national-level developments and threat activity.** CISA offers alerts regarding nation-state threat activity[1] and vulnerabilities that threat actors are currently exploiting.[2] Sign up to stay aware of imminent risks.
- **Ensure best practices to drive down cyber risk.** CISA's Cybersecurity Performance Goals (CPGs) help organizations understand what security practices will be most impactful and address aggregate risk for the nation.[3] These CPGs can be particularly useful to help your company assess the security of small and medium companies in your supply chain.
- **Collaborate for the national defense.** Collaborating on cyber defense operations ensures that we are taking a team approach to countering threats. As part of its Joint Cyber Defense Collaborative, CISA offers an operational collaboration partnership to exchange cyber defense information and participate in cyber defense planning and exercises. Consider joining CISA's program[4] or an industry-led Information Sharing and Analysis Center (ISAC).[5] These partnerships enable organizations to share visibility on threat activity, vulnerabilities, analysis of risks and mitigations, as well as to jointly plan defensive actions and risk mitigations.
- **Report incidents to help protect others.** Let CISA know if your company has experienced a cyber incident, so that we can issue a technical alert to help others defend themselves from similar threats.[6] In some nationally significant cases, CISA may provide incident response services. Additionally, anyone who has experienced a cybercrime can report it to the FBI online or contact a local FBI field office.[7]

- **Build connections with the federal government.** Your company can maintain a person-to-person relationship with CISA through our regional offices[8] located across the nation. These advisors can connect your company with CISA's services and resources, as well as provide a direct point of contact in times of emergency.

DESIGNING AND DEPLOYING TECHNOLOGY SECURELY

Today, almost all companies are technology companies, since they offer some sort of networked product or service such as online shopping, smart devices for home and enterprises, online business-to-business solutions, health-care services and devices, smartphone apps, and other online services. As such, the products and services they develop or use for their customers are woven into the fabric of the economy and therefore have an outsized impact on national security. Technology products and services can create both benefits and risks. We need to better balance the shared responsibility between providers and customers. In particular, technology vendors should take ownership of the security outcomes of their customers. Customers of technologies must also play an active role by demanding product safety. Products that prioritize customer safety will have features such as these:

- **Multifactor authentication (MFA).** The lack of MFA is a common attack vector, but many customers don't enable it. For customers using these products, especially enterprise customers, MFA should be the default (if not using a Single Sign-On provider), not an option they have to hunt for. Systems should firmly nudge users toward enrolling in MFA, like your car nudges you if you don't buckle up. That's doubly true for system administrators who are high-value targets.
- **Use and write secure software.** Most security vulnerabilities stem from a type of coding error related to "memory safety." Every vendor writing software should establish policies for writing new software in a memory-safe language and publish a "memory safe road map". They should also publish Software Bills of Materials.
- **Prioritize secure default configurations**. Technology companies should offer important security features at no extra charge, especially MFA and Single Sign-On (SSO) integration. Rather than publishing a "hardening" guide that customers must implement at their own expense to make the products less dangerous, tech companies should ship products with secure defaults. Boards can ask their IT and Security teams for information about how much time and money they spend hardening products.

HAVING A CONVERSATION WITH YOUR CISO

Even as more board members recognize that cyber risk is indeed a business risk and a matter of good governance, they can still find the subject matter intimidating and opaque. It's important that board members foster a close working relationship with their chief information security officer to both help them become more cyber literate as well as to understand how to best empower the CISO team. To that end, the following questions can be used to spark a deeper conversation with the CISO to help directors

learn more about the effectiveness of a firm's security programs. These questions are meant to be asked in a spirit of genuine inquiry and learning. Should any of these questions reveal gaps in the security program, the overall team can help to understand why and plot a new path forward.

1. Questions to ask about your organization's email system

a. What percentage of users do not need to use multifactor authentication (MFA) when logging in?
b. How many system administrators are there?
c. How many administrators do not need to use MFA when logging in?
d. Which executives do not need to use MFA to log in?

Why is it important? Many compromises involve credential phishing at some point in the attack chain. Yet many organizations have not yet deployed MFA to 100 percent of staff and 100 percent of system administrators, even for critical systems like email. This disconnect often has roots ranging from employee or executive resistance, to lack of MFA support in legacy systems, or in prioritization.

Helpful answer: Given today's threat landscape, enterprises should have already made MFA the default for all staff and privileged users, especially system administrators. At a minimum, the security team should be able to provide the percentages and a list of exempted users without much effort.

The ideal answer is that all systems are behind a central login portal, and that portal requires MFA for all users.

Answers that require more investigation: For a variety of reasons, there may be user accounts that are permanently exempted from the MFA policy and that is often unmanaged risk. The team should evaluate the resultant risk as part of the overall risk program.

2. Questions to ask about your identity system:

a. What are our greatest weaknesses?
b. What systems are not yet protected by being behind our identity system?

Why is it important? The identity and access management (IAM) system is part of the foundation of a security program. You can't secure your assets if you don't know who is on the network. A compromise of the identity system would have catastrophic implications for all other company systems, like email, file storage, HR systems, financial systems, and so on.

Helpful answer: Because IAM systems are so critical, the security team should be able to talk about a range of topics, starting with configuration management. Many products, including IAM products, are delivered to the customer with surprisingly unsafe defaults. The team may talk about that fact, and possibly their experience with the vendor's hardening guide.

Security staff may talk about the challenge of working with HR to ensure staff are properly offboarded when they leave and discuss minor incidents or near misses when that didn't happen. They may talk about how they monitor for unauthorized logins and about the limits of those approaches.

The team will generally have a punch list of products that are not behind the IAM system and a road map for migrating them to that central service.

Answers that require more investigation: IAM systems are hard to build and maintain securely and require good partnerships with teams like HR (for employee onboarding/offboarding) and Procurement

(which often handles vendor accounts—another gap worthy of discussion). If the CISO doesn't mention some of these struggles, they may need to do some additional research.

3. Questions about changes your CISO would like to see

- **a.** If the board and management could eliminate (or at least take ownership for) employee push-back, what two changes (across people, processes, technologies) would you make to dramatically improve our security posture?
- **b**. How would those changes raise the cost of attack?

Why is it important? There is a general tendency for security teams to try to secure existing products and workflows, usually by adding security tools. The goal is to secure the organization without disrupting users and workflows. While this approach can work, it has its limits. To achieve higher levels of security, organizations may need to consider radically refactoring their workflows and tools. To use a car analogy, it may not be possible to add airbags, collapsible steering columns, and crumple zones to a car from 1960. A redesign is what gives you those safety measures.

The board can generate conversations and interest in ideas that might encounter employee resistance but could dramatically improve the security posture. A security team might not be empowered to work against company culture, but a CEO might be able to manage it.

One minor example: security keys can eliminate credential phishing (even MFA-bypass attacks) but may cost money, require employee training, and server reconfigurations. It may be challenging for the CISO to drive the cultural change alone, and they may not have raised the issue. Discussing these "big bet" ideas should be a natural part of board conversations.

If you were building the company from scratch, would you build it the way it currently exists? Would you secure it in the same way? The answer is probably no. Discussing the delta between those two models can be illuminating.

Helpful answer: Some CISOs have their big-bet ideas already documented. Most should be able to create such a deck in conjunction with other teams.

Answers that require more investigation: Company culture and technical debt limit how much an organization can refactor at any given point in time. Yet security and partners in CIO and CTO organizations generally understand those limits. Dig deeper if the answers you get indicate comfort with the status quo and current trajectory for improving the organization's security posture.

4. Questions about the security posture

- **a.** Knowing everything you know about our security posture and the broad spectrum of attackers in play, how do you think someone could break in to steal data from the company?
- **b**. If our adversaries had a budget of one million dollars to hire a crew with specific talents, who would they hire and for what tasks?

Why is it important? We frequently hear the phrase "think like a hacker," but even security professionals can find it hard to constantly adopt that mindset. How might someone chain together seemingly unrelated and minor vulnerabilities into a major intrusion?

Helpful answer: If the CISO can refer to previous information they've presented and connect the dots, you have a successful answer.

Possible answers:

> "As I mentioned before, our call-center network is connected to our production network, so a compromise of any one system there gives an attacker access to networks containing our customer data. It's not uncommon for criminals to bribe call center employees, or to have an accomplice get a job in a call center for just this purpose. They very well might start there."
>
> "We just acquired that small company and haven't imposed our security controls on them yet. Their network is separate, but they have privileged access in our development environment. Not only might we not be able to prevent the attack, but we also probably couldn't detect it. That might be a good attack path for an attacker."

Answers that require more investigation: Every security professional should have several ideas on how such an attack might happen. If the CISO doesn't have any ideas or is overly confident in the security posture of the company, it may be because they are overly focused on building defenses and need to spend time thinking from the opponent's perspective. Conducting a tabletop exercise can generate creativity and deeper insights, as one example of a way to view the security program from the perspective of a hacker.

The proposed attacks should be relatively simple and not rely on advanced attacks using multiple zero-day vulnerabilities. When they are compromised, most organizations are not attacked by intelligence agencies spending millions of dollars. Far too many organizations are compromised because they ran unpatched software, didn't segment their networks, did not implement MFA, and allowed users to run arbitrary software on their laptops.

The Cybersecurity and Infrastructure Security Agency (CISA) is the newest agency in the federal government, established in 2018 to be America's Cyber Defense Agency. We serve as the National Coordinator for critical infrastructure security and resilience, leading the effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. As the majority of our nation's critical infrastructure is owned and operated by the private sector, operational collaboration is foundational to our efforts. We work with a wide array of partners across the globe—from every industry, to federal, state, local, tribal, territorial and international governments, to non-profits, academia, and the research community—connecting them together and to the resources, tools, and information that will help them fortify their security and resilience against current and emerging threats.

ENDNOTES

[1] See the "Cybersecurity Alerts & Advisories" web page posted on cisa.gov. (https://www.cisa.gov/uscert/ncas/alerts)

[2] For more information, see the "Known Exploited Vulnerabilities Catalog" web page posted on cisa.gov. (https://www.cisa.gov/known-exploited-vulnerabilities-catalog)

[3] Please see CISA's "Cross-Sector Cybersecurity Performance Goals" web page. (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)

[4] To learn more about the program, visit CISA's "Cyber Information Sharing and Collaboration Program (CISCP)" web page. (https://www.cisa.gov/resources-tools/programs/cyber-information-sharing-and-collaboration-program-ciscp)

[5] To learn more about the program or to join your sector's ISAC, visit CISA's "National Council of ISACs" web page. (https://www.nationalisacs.org/)

[6] To report an incident, visit the "Report to CISA" web page. (https://www.cisa.gov/report)

[7] Report a cyber crime to the FBI by filing a complaint via the "Internet Crime Complaint Center (IC3)" web page. (https://www.ic3.gov/)

[8] For a list of CISA's regional offices, visit CISA's "CISA Regions" web page. (https://www.cisa.gov/about/regions)

TOOL L

Incident Response and Reporting to the FBI

By Pranav Shah and Patrick Kyhos, FBI

The benefits of reporting a cyber incident to the FBI are more evident today than ever before. The FBI's well-trained workforce expands across the nation and the globe, and is able to assist your organization with a cyber incident within one hour within the continental United States and within one day in more than 70 countries. With that speed, we bring unique investigative and intelligence-derived insights to mitigate the threat your organization is facing.

In response to a reported cyber incident, the FBI may be able to take the following actions:

Identify and stop the activity.

- **Information sharing:** FBI agents who are familiar with patterns of malicious cyber activity can work with your security and technical teams to help you quickly identify threats and understand the context of the incident.
- **International partnerships:** The FBI has Cyber Assistant Legal Attachés around the world and can leverage the assistance of international law enforcement partners to locate stolen data or identify the perpetrator.
- **Recovery Asset Team (RAT):** The FBI's RAT was established in February 2018 by the FBI's Internet Crime Complaint Center (IC3) to streamline communication with financial institutions and assist with the recovery of funds for victim companies that made transfers to domestic accounts under fraudulent pretenses. In 2018, in its first year, the RAT recovered 75 percent of transferred funds.
- **Apprehend or impose costs on cyber actors:** The US Department of Justice (DOJ) and FBI can bring forth indictments and other deterring actions to degrade cyber actors' capabilities.

Seize or disrupt the actor's technical infrastructure.

- The DOJ and FBI have a mounting record of successful court-authorized operations to disrupt cyberattacks, counter ransomware, or neutralize botnets that have hijacked millions of innocent computers worldwide. The DOJ and FBI's unique authorities allow actions to be taken against the cyber actor's technical infrastructure that private companies cannot legally take on their own.

Share valuable insights from other investigations that may help mitigate damage and prevent future incidents.

- Disclosing information about an incident to the FBI enables investigators to make connections among related incidents.
- This enhances the FBI's abilities to share valuable insights and information regarding the perpetrator's tactics, tools, and techniques. Such information may allow you to better protect your company's network and assist the FBI in identifying and warning you (and others) of future malicious activity.

Support your organization's data-breach response.

- Under many state laws, law enforcement may be able to temporarily delay otherwise mandatory state data-breach reporting when law enforcement determines doing so is appropriate to pursue leads.

- Proactive reporting to law enforcement may help your organization deal with government regulators such as the Federal Trade Commission, which has declared that it will look more favorably on a company that has reported a cyber incident to law enforcement and cooperated with the investigation than it will look on companies that have not.
- If an incident becomes public, cooperation may strengthen your organization's position with shareholders, insurers, lawmakers, and the media.

WHEN SHOULD MY ORGANIZATION REPORT A CYBER INCIDENT?

The DOJ and FBI encourage companies to identify and develop a relationship with their local FBI field office prior to an incident. Organizations should report a cyber incident as soon as the incident is verified. This should be done in as timely a manner as possible to enable the best possible attribution of an attack—since speed is often the critical element of a credible attribution. Additionally, reporting to the FBI avails the organization of protections provided to victims and witnesses.

Any report should be done in coordination with the organization's legal team to comply with the statutory and regulatory requirements, as applicable. Entities that own or operate critical infrastructure will be required to report certain cybersecurity incidents and ransomware payments to federal agencies, specifically CISA, per the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Proactively building relationships with key government agencies, a relationship with your sector risk management agencies, and the FBI provide companies with a dedicated point-of-contact if an incident should occur and provides access to FBI cyber mitigation resources.

Electronic evidence dissipates over time, so speed is essential in a cyber-intrusion investigation. Enlisting the FBI's help during an incident enables quick investigative action and allows the preservation of evidence, which increases the odds of a successful prosecution or other action to disrupt the perpetrators.

WHAT SHOULD BE REPORTED?

An array of technical data and incident information can prove helpful for investigators, including these:

- Indicators of compromise (IOCs), ie. threat actor IP addresses.
- Threat actor tactics, techniques and procedures (TTPs)
- Threat actor communications, e.g., ransom notes, TOR addresses
- A time line of the event
- The nature of the incident
- A point of contact for regular communication with investigators
- Logs from the affected machines
- Images of the affected machines
- Actions that have been taken
- Forensic reports from any incident response firm that has been contracted

HOW WILL THE FBI PROTECT MY ORGANIZATION'S INTERESTS AND INFORMATION?

Federal law enforcement agencies investigating cyber incidents seek first and foremost to assist victim entities as well as identify and apprehend those responsible for a cyber incident.

The FBI is not a regulatory agency and efforts are directed toward the actions on the system/network of the intruder and not a judgment or analysis of the adequacy of the defenses in place.

Often, the FBI requires only technical details about an intrusion (e.g., malware samples) to advance its investigation, not privileged communications or other documents or communications unrelated to the incident. The FBI will work closely with a victim company's counsel to address concerns about access to information.

The FBI is mindful of the reputational harm that a cyber incident can cause a company or organization. As such, the FBI does not publicly confirm or deny the existence of an investigation and will ensure that information that may harm a company is not needlessly disclosed.

The FBI prioritizes causing as little disruption as possible to normal business operations. On-site investigations are carefully coordinated with your company to minimize the impact, including, for example, by working around your organization's schedule and minimizing system downtime.

HOW DO I CONTACT THE FBI TO REPORT A CYBER INCIDENT?

- Local FBI Field Office: https://www.fbi.gov/contact-us/field-offices
- The FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/
- Online Tips and Public Leads Form: https://tips.fbi.gov/
- FBI Tip Line: 1-800-CALL-FBI (1-800-225-5324)
- International FBI offices: https://www.fbi.gov/contact-us/legal-attache-offices
- National Cyber Investigative Joint Task Force (https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force)
  - NCIJTF CyWatch 24/7 Cyber Center: To contact CyWatch, please call 1-855-292-3937 or email cywatch@ic.fbi.gov

WHERE CAN I FIND OUT MORE?

- InfraGard: https://www.infragard.org/
  - InfraGard is an association of people and organizations who represent businesses, academic institutions, state and local law enforcement agencies, and others, dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard has more than 80 chapters across the United States.

Domestic Security Alliance Council (DSAC):

- DSAC is a partnership between the US government and the US private industry that enhances communication and the timely and effective exchange of security and intelligence information between the federal government and the private sector.

The Department of Justice:

- The Computer Crime and Intellectual Property Section (CCIPS) and Computer Hacking and Intellectual Property (CHIP) Program provide a network of federal prosecutors trained to pursue computer crime and IP offenses in each of the 94 United States Attorneys' Offices. CCIPS produced the *Best Practices for Victim Response and Reporting of Cyber Incidents* as a resource: (https://www.justice.gov/criminal-ccips/file/1096971/download).

The National Security Cyber Specialist (NSCS) is a nationwide network of the DOJ headquarters and field personnel trained and equipped to handle national security-related cyber issues. It includes specially trained prosecutors from every US Attorney's Office, along with experts from the National Security Division and the Criminal Division. To contact a NSCS representative, email DOJ.Cyber.Outreach@usdoj.gov or NSCS_Watch@usdoj.gov.

TOOL M

Board Decisions on the General Use of AI[1]

By Simon Sun and Larry Clinton, ISA

Much like the Internet itself artificial intelligence (AI) and machine learning (ML) are already becoming ubiquitous tools in many organizations. In 2021, private investment in AI totaled around $93.5 billion—nearly double the investment in 2020.[2] Also, as with the Internet, the use of AI and ML tools can provide dramatically enhanced business opportunities in terms of efficiency, innovation, and customer service. At the same time, the use of AI and ML can create vast new risks in terms of cybersecurity. The National Security Commission on Artificial Intelligence found that "AI applications are transforming existing threats, creating new classes of threats, and further emboldening state and non-state actors to exploit vulnerabilities in the US open society."[3]

Just as with the flip side of many other risks, certain applications of AI and ML tools can be used to enhance an organization's cybersecurity and lessen its risks. It is critical that the board work with management to understand the risk-reward balance of the specific uses of AI/ML their organization should embrace. This toolkit consists of two lists of questions to help guide the board's oversight of these advanced digital techniques. The first list is for the board's overall consideration of using various AI/ML techniques. The second list focuses on the specific issues in the use of AI for cybersecurity

DEFINING ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

"Artificial Intelligence (AI), a term coined by emeritus Stanford Professor John McCarthy in 1955, was defined by him as 'the science and engineering of making intelligent machines'. Much research has humans program machines to behave in a clever way, like playing chess, but, today, we emphasize machines that can learn, at least somewhat like human beings do."

"Machine Learning (ML) is the part of AI studying how computer agents can improve their perception, knowledge, thinking, or actions based on experience or data. For this, ML draws from computer science, statistics, psychology, neuroscience, economics and control theory."

Source: Professor Christopher Manning, Stanford University, 2020.[4]

GENERAL QUESTIONS FOR THE BOARD TO CONSIDER IN OVERALL USE OF AI/ML

1. **What is the goal for the company or organization to employ this system?**
2. **What is the plan to build or deploy this AI or ML application responsibly?**
3. **What type of system is the company using: process automation, cognitive insight, cognitive engagement, or some other type? Do our board and management understand how this system works?**
4. **What are the economic benefits of the chosen system?**
5. **What are the estimated costs of not implementing such a system?**
6. **Are there any potential alternatives to the AI or ML systems in question?**

7. How easy will it be for an adversary to execute an attack on the system based on the technical characteristics?
8. What is the organization's strategy to validate data set collection practices?
9. How will the company prevent inaccuracies that may exist in the data set?
10. What will be the damage incurred from an attack on the system in terms of the likelihood and the ramifications of the attack?
11. How frequently will the company review and update its data policies?
12. What is the organization's response plan for cyberattacks involving these systems?
13. What is the company's plan to audit the AI system?
14. Should the company create a new team to audit the AI or ML system?
15. Should the company build an educational program for its staff to learn about the use and risks of AI and ML in general?

QUESTIONS FOR THE BOARD OF DIRECTORS TO ASK WHEN DECIDING WHETHER TO USE AI FOR CYBERSECURITY PURPOSES[5]

1. What is the company's overall road map to implementing AI and/or ML in cybersecurity?
2. What are the cybersecurity goals that the organization is trying to achieve by implementing this AI or ML solution?
3. How will the system toughen the companies' security stance? How will success be measured?
4. What is the estimated harm that the company will face without the system?
5. What are the new cybersecurity vulnerabilities that the company will face in employing the system?
6. What type of cyberattack is the system designed to detect, predict, and respond to?
7. Is the system prepared to detect and weather a ransomware attack?
8. How would implementing such a system affect the organization's cybersecurity team? What are the benefits and risks associated with the tool's use by the team?
9. Should the company expand or update the current cybersecurity team?
10. How much would it cost for the company to create a new cybersecurity team?
11. Are there any positions that the company doesn't need any more due to employing the AI or ML cybersecurity system?
12. Should the company create a sub-team to monitor the outcomes and findings of the new system?
13. Will implementing such a system affect the company's cyber insurance enrollment?
14. Are there any potential legal consequences of not implementing AI/ML in a cybersecurity system?

ENDNOTES

[1] The following questions are designed primarily based on "A.I. and Risk Management: Innovating with confidence report" by Deloitte (https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/deloitte-gx-ai-and-risk-management.pdf) and "Attacking Artificial Intelligence: A.I.'s Security Vulnerability and What Policymakers Can Do About It" by Harvard Kennedy School Belfer Center for Science and International Affairs. (https://www.belfercenter.org/publication/AttackingAI).

[2] Daniel Zhang, Nestor Maslej, Erik Brynjolfsson, John Etchemendy, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Michael Sellitto, Ellie Sakhaee, Yoav Shoham, Jack Clark, and Raymond Perrault, *The AI Index 2022 Annual Report* (AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University, March 2022), p. 3. (https://aiindex.stanford.edu/wp-content/uploads/2022/03/2022-AI-Index-Report_Master.pdf)

[3] June 10, 2022, tweet of the DAIMLAS Artificial Intelligence Ecosystem Builders, "AI applications are transforming existing threats, creating new classes of threats, and further emboldening state and non-state adversaries to exploit vulnerabilities in the US open society," Twitter. (https://twitter.com/daimlas/status/1535389680195207168)

[4] Christopher Manning, Stanford University Human-Centered Artificial Intelligence, *Artificial Intelligence Definitions* (September 2020). (https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf)

[5] The previous tool questions should apply in this section as both are referring to the use of AI systems.

TOOL N

US Secret Service's Role in Stopping Financial Loss

By Global Investigative Operations Center Staff, US Secret Service

OUR HISTORY AND MISSION

Most identify the United States Secret Service (USSS) as the agency protecting the president, vice president, and domestic and foreign dignitaries. But the Secret Service was originally created in 1865 to protect the nation's financial infrastructure from counterfeiting. Today, the investigative mission of the Secret Service has evolved to coverage of crimes involving all forms of payment, to include digital assets. Regardless of the crime being investigated, the USSS's mission remains the same: mitigate the criminal activity, arrest those responsible, and return stolen assets to victims.

Through a network of field-based cyber-fraud task forces (CFTF) and strategically placed international offices, the US Secret Service takes a multifaceted approach to combatting cybercrimes by partnering with global, federal, and local law enforcement agencies to create a robust response to cyber fraud incidents. This includes business email compromises (BECs) and other social engineering schemes, ransomware, money laundering, and financially motivated crimes. The storied tradition of the Secret Service financial crimes investigations has resulted in the creation of a team dedicated exclusively to investigating crimes involving the illicit use of digital assets.

The Secret Service works closely with financial institutions, and more specifically with fraud prevention and recovery departments. This provides the Secret Service with a unique role in swiftly identifying and stopping fraudulent wire transfers. The Global Investigative Operations Center (GIOC), together with the field-based CFTFs, engage in rapid response to fraudulent wire transfers and other incidents.

Establishing proactive contact with the Secret Service and other law enforcement agencies is a key element in preventing, mitigating, and responding to cyber-enabled crimes, particularly when these crimes are financially motivated. Secret Service field offices have regional call centers, which operate 24 hours a day.[1]

Partnerships are key to both the protective and investigative mission of the USSS. The Secret Service emphasizes outreach and relationships with public and private sector partners, since it is critical to establish lines of communication before incidents occur. The Secret Service regularly contributes to virtual and in-person seminars, conferences, and tabletop exercises. Additionally, the Secret Service hosts cyber incident response simulations which focus on both law enforcement and private sector responses to criminal activity related to cybercrimes, including BECs. The Secret Service develops guides, alerts, and other materials for CFTF partners, public and private organizations, and individuals.

SPOTLIGHT: BUSINESS EMAIL COMPROMISES (BECS)

BECs target both businesses and individuals and result in the largest percentage of loss compared to other cyber-enabled financial crimes. Estimated losses exceed $43 billion in the past seven years, with $2.1 billion reported to the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3) in 2021.

BECs share similarities with other financially motivated social engineering schemes, such as phishing/smishing, romance, work-from-home, and elder fraud. BECs typically begin with the theft of contemporaneous and privileged information, which is then used to trick victims into transferring funds to fraudulent accounts via socially engineered emails. BEC criminals are indiscriminate and opportunistic, targeting all business sectors. Everyone is vulnerable: multinational corporations, small businesses, and individuals alike.

- Criminals use several means to compromise email accounts, including these:
  - Phishing attacks both broad and targeted to deploy malware and steal login credentials
  - Scraping the dark web to harvest login credentials from prior data breaches
  - Gaining access to email accounts through social engineering schemes
- Once email accounts are compromised, email rules and settings, such as auto-forwarding, are typically established to forward emails to other accounts.
- This allows criminals to surreptitiously monitor communications.
- A popular tactic is to create spoofed domains emulating a party in the transaction.
- The spoofed email accounts are often manipulated by changing an email's display name (i.e., send mail as) settings to mask a criminal's true email address.
- Stolen funds are laundered by several methods, including these:
  - Unwitting mules, typically romance scam victims
  - Witting mules and shell companies
  - Structured cash withdrawals
  - Luxury goods purchasing
  - Money transmitting services
  - Cashier checks
  - Digital asset transactions

Having a robust response is necessary to mitigate damages. The Secret Service recommends that directors ask if the following tactics have been developed for response within their organizations:

- Identify and establish an incident response team (IRT).
- Update and practice your incident response plan (IRP), including with law enforcement partners.
- *Immediate* reporting of the incident to law enforcement is critical.
- Practice good cyber hygiene (e.g., two-factor/multifactor authentication, update software patches, educate workforce on cyber-enabled fraud).
- Conduct BEC drills, similar to anti-phishing exercises.
- Review email systems for unauthorized access or rule creation.
- When aware of an incident, contact your bank to reverse transaction, for hold harmless and indemnification.
- As a reminder–Immediately report an incident to law enforcement, including your local US Secret Service Field Office (https://www.secretservice.gov/contact/field-offices).

For more information on BECs and how to prepare for other common cyber incidents, visit the USSS website.[2]

ENDNOTES

[1] For information about the US Secret Service's Field Offices, visit their "Field Offices" web page. (https://www.secretservice.gov/contact/field-offices)

[2] See the US Secret Service's web page, "Preparing for a Cyber Incident." (https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident)