

Cyber-Risk Oversight 2020

Key Principles and Practical Guidance
for Corporate Boards



© 2020 by the National Association of Corporate Directors and the Internet Security Alliance. All rights reserved.

Except as permitted under the US Copyright Act of 1976, no part of this publication may be reproduced, modified, or distributed in any form or by any means, including, but not limited to, scanning and digitization, without prior written permission from the National Association of Corporate Directors or the Internet Security Alliance.

This publication is designed to provide authoritative commentary in regard to the subject matter covered. It is provided with the understanding that neither the authors nor the publishers, the National Association of Corporate Directors and the Internet Security Alliance, is engaged in rendering legal, accounting, or other professional services through this publication. If legal advice or expert assistance is required, the services of a qualified and competent professional should be sought.



Cyber-Risk Oversight 2020

Key Principles and Practical Guidance
for Corporate Boards

Prepared by Larry Clinton

President and CEO,
Internet Security Alliance

WITH SUPPORT FROM

Josh Higgins

Senior Director of Policy and Communications
Internet Security Alliance

Friso van der Oord

Senior Director of Research and Editorial
National Association of Corporate Directors

Acknowledgements

NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Peter R. Gleason, Chief Executive Officer

Erin Essenmacher, President and Chief Strategy Officer

Friso van der Oord, Senior Director, Research and Editorial

Christopher Hetner, NACD Cybersecurity Advisor

Leah Rozin, Senior Research Manager

Barton Edgerton, Associate Director, Governance Analytics

Ted Sikora, Manager Of Benchmarking and Data Insights

Reaa Chadha, Senior Research Analyst

Andrew Lepczyk, Research Analyst

Margaret Suslick, Manager, Copy Editing & Print Production

Patricia W. Smith, Art Director

Alex Nguyen, Senior Graphic Designer

Prepared by **Larry Clinton**, President and CEO, Internet Security Alliance, with support from **Josh Higgins**, Senior Director of Policy and Communications, Internet Security Alliance, and **Friso van der Oord**, Senior Director of Research and Editorial, National Association of Corporate Directors.

We wish to thank the following individuals for their contributions to this Handbook (in alphabetical order by organization):

Tracie Grella, Garin Pace, Anthony Shapella, AIG

Lisa Humbert, Bank of Tokyo Mitsubishi, MUFG

Adrian Peters, BNY Mellon

Bob Zandoli, Bunge

Nick Corzine, Lou DeSorbo, Ben Havelka, Geoji Paul, Centene

Catherine Ide, Center for Audit Quality

Robert Kolasky, Daniel Kroese, Ashley Montgomery, Department of Homeland Security

Joe Buonomo, Robert Gardner, Direct Computer Resources

Jim Halpert, Andy Serwin, DLA Piper

Robyn Bew, Andrew Cotton, EY

Jillian Stickels, FBI

Greg Montana, FIS

Nasrin Rezai, General Electric

Melissa Hathaway, Hathaway Global Strategies

Dan Lips, Celeste Lowery, Internet Security Alliance

J. R. Williamson, Leidos

Scott Rush, Lockheed Martin

Robyn Boerstling, National Association of Manufacturers

Ben Abrams, Mike Papay, Northrop Grumman

Jeff Brown, Raytheon

Tim McKnight, Richard Puckett, SAP

John Frazzini, Robert Vescio, SSIC

Gary McAlum, USAA

Richard Spearman, Vodafone

Table of Contents

Acknowledgements	2
Foreword	4
Introduction	6
PRINCIPLE 1	12
Cybersecurity as a Strategic Risk	
Directors need to understand and approach cybersecurity as a strategic, enterprise risk—not just as an IT risk.	
PRINCIPLE 2	16
Legal and Disclosure Implications	
Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances.	
PRINCIPLE 3	20
Board Oversight Structure and Access to Expertise	
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.	
PRINCIPLE 4	
An Enterprise Framework for Managing Cyber Risk	25
Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.	
PRINCIPLE 5	
Cybersecurity Measurement and Reporting 30	
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.	
Conclusion	34

TOOLKIT

Road Map for the Cyber-Risk Oversight Toolkit	36
Tool A – 10 Questions for a Board Member to Ask About Cybersecurity	37
Tool B – Assessing the Board’s Cyber-Risk Oversight Effectiveness	41
Tool C – The Cyber-Insider Threat—a Real and Ever-Present Danger	43
Tool D – Supply-Chain and Third-Party Risks	45
Tool E – Incident Response	49
Tool F – Board-Level Cybersecurity Metrics	53
Tool G – Cybersecurity Considerations During M&A Phases — Mergers and Acquisitions	56
Tool H – Sample Dashboards	60
Tool I – Building a Relationship With the CISO	63
Tool J – Enhancing Cybersecurity Oversight Disclosures—10 Questions for Boards	66
Tool K – Personal Cybersecurity for Board Members	69
Tool L – Department of Homeland Security Cybersecurity Resources	70
Tool M – Department of Justice and Federal Bureau of Investigation—Responding to a Cyber Incident	72

Foreword

By Robert Kolasky, Director, National Risk Management Center, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security

Ensuring the cybersecurity resilience of the United States is truly a whole-of-society effort. We have seen cyber adversaries target electric utilities and financial institutions, cripple rural hospitals with ransomware attacks, attempt to undermine our democratic processes, and find points of technological leverage to steal massive amounts of intellectual property. The importance of cybersecurity for our nation's national security, economic security and competitiveness, and public health and safety is fortunately well understood and documented at this juncture.

In response to the dramatic changes in the threat landscape, a welcomed and necessary shift has been the increased emphasis on cybersecurity as a strategic, enterprise-wide risk by senior leaders at organization, going beyond the realm of IT functions. No longer can cybersecurity conversations be purely focused on IT controls, such as network defense. These technical capabilities must be coupled with robust risk-management practices—knowing your major risks, understanding the size of your attack surface, assessing the criticality of your digital infrastructure based on the type of business processes they support, conducting inventories of connected users and devices, and then using this awareness to harden systems and add resilience in a targeted and prioritized manner.

With this in mind, this Handbook rightfully states that a cybersecurity incident at an organization can no longer be looked at as a mere IT problem. Rather, these incidents represent potential business losses (either realized or unrealized) that must be treated with the same vigilance as more traditional vectors of business disruption and loss of profit. Additionally, in a connected digital world, an incident or breach at one organization may ripple across supply chains and even industry sectors—and in some cases result in major structural damage to the nation.

The Cybersecurity and Infrastructure Security Agency (CISA) believes that understanding the key principles of cybersecurity risk management shouldn't require a technical background or decades of experience in network protection roles. Leaders in organizations as well as their overseers need to be able to contextualize and discuss cyber-risk management decisions in plain English.

CISA sees ourselves as the nation's cybersecurity risk advisor. We work with partners—at different levels of government and within industry—to better understand, analyze, prioritize, and manage risk to the nation's critical infrastructure and the federal government. While we don't directly manage your cyber risks

or sit on top of your networks, we can provide your organization with our situational awareness, aggregated across 16 critical infrastructure sectors; scalable tools and services to better identify and mitigate vulnerabilities; and incident-response capabilities to help minimize downtime following an incident.

Listening to our private-sector partners, we've learned some important lessons. Chief among them has been better operationalizing the

partnership by engaging not just with the right organizations but with the right people at these organizations. The lens through which a chief information security officer (CISO) looks at cybersecurity is different than that of a chief risk officer (CRO), chief information officer (CIO), chief technology officer (CTO), chief counsel, chief executive officer (CEO), or board member. All are key stakeholders, but all will bring slightly different perspectives to addressing the cyber-risk challenge.

While the touchpoints between cybersecurity hubs within the federal government and technically focused network defenders in the private sector have been historically strong, the connections with the enterprise-risk management portions of organizations are admittedly less mature.

While the touchpoints between cybersecurity hubs within the federal government and technically focused network defenders in the private sector have been historically strong, the connections with the enterprise-risk management portions of organizations are admittedly less mature.

This reality presents a prime opportunity to use the guidance contained in this Handbook for deeper risk management integration between government and industry. CISA has recently launched what we are calling the National Risk Management Dialogue—a series of high-level conversations with chief risk officers and enterprise-risk management executives at critical infrastructure organizations. We'll be doing more of these around the country and look forward to continued engagement.

Another lesson we've learned from our conversations with partners is that, despite the emphasis on systemic risk and advanced persistent threats, cybersecurity basics still matter—a lot. Basic hygiene is lacking, including simple controls such as backing up systems, patch management, and network segmentation. In ensuring the adoption of these cyber essentials, all organizations—regardless of size or maturity of cyber-risk management practices—have some role to play. With the distributed and interconnected nature of the global information and communications technology supply chain, helping organizations around us to raise their cybersecurity baselines can actually make us safer, too.

A third lesson is based on a truism that good risk analysis and management depends on good risk metrics. Too often, cybersecurity has been treated as a “too-hard-to-measure” problem, but we are now making progress in quantifying cyber risk. Frameworks are in place to evaluate what needs to be measured, and they have been broadly adopted in a manner that supports aggregation of data. While not an easy endeavor by any means, efforts need to be made to evaluate the cyber impact against traditional business metrics and then push the analysis further upstream to evaluate incidents and controls in terms of their impact on business outcomes. This new thinking will help us to better evaluate the merit of additional investments in cyber controls and other forms of risk management.

CISA commends NACD for producing this Handbook. It offers foundational and practical guidance that can have lasting impact on the good governance of cybersecurity. In a world where your risk is my risk, and vice versa, collective defense that leverages the principles set forth in this report will help us to keep the American economy strong and our national critical functions resilient.

Introduction

As corporate fiduciaries, boards of directors are responsible for overseeing management strategy, as well as for their identification and planned response to enterprise-wide risks impacting the company and its value to stakeholders and shareholders. In the past 25 years, the nature of corporate asset value has changed significantly, shifting away from the physical and toward the virtual. This rapid “digitization” of corporate assets has resulted in a corresponding transformation of strategies and business models—as well as the digitization of corporate risk.

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. They are also subject to increasing risk from the loss of IP and trad-

ing algorithms, destroyed or altered data, declining public confidence, attacks against critical infrastructure and corresponding systemic risks, and evolving global regulatory sanctions. According to the *Global Risks Report 2019*, business leaders in advanced economies rank cyberattacks among their top concerns.¹ A serious attack can destroy not only a company’s financial health but also have systemic effects causing harm to the economy as a whole and even national security.

Leading companies view cyber risks in the same way they do other critical risks—in terms of a risk-reward trade-off. This approach is challenging for two reasons. First, 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, to include not only cybercriminals but also ideologically motivated “hacktivists” and nation-states. As a result, the effects of cyberattacks are expanding well beyond information loss or business disruption. They can have a severe

impact on an organization’s reputation and brand through loss of consumer confidence. Companies and directors may also incur legal risk resulting from cyberattacks. At the same time, the competitive need to deploy new and emerging technologies in order to lower costs, improve customer service, and drive innovation is stronger than ever. Adopting these technological innovations and capabilities may offer strong returns but can also increase cyber risk. These competing pressures mean that conscientious and

comprehensive oversight at the board level is essential, requiring more strategic dialogue with management than in the past.

Starting in 2014, NACD, in conjunction with AIG and the Internet Security Alliance, published the first edition of the handbook. Since then, we’ve made enhancements

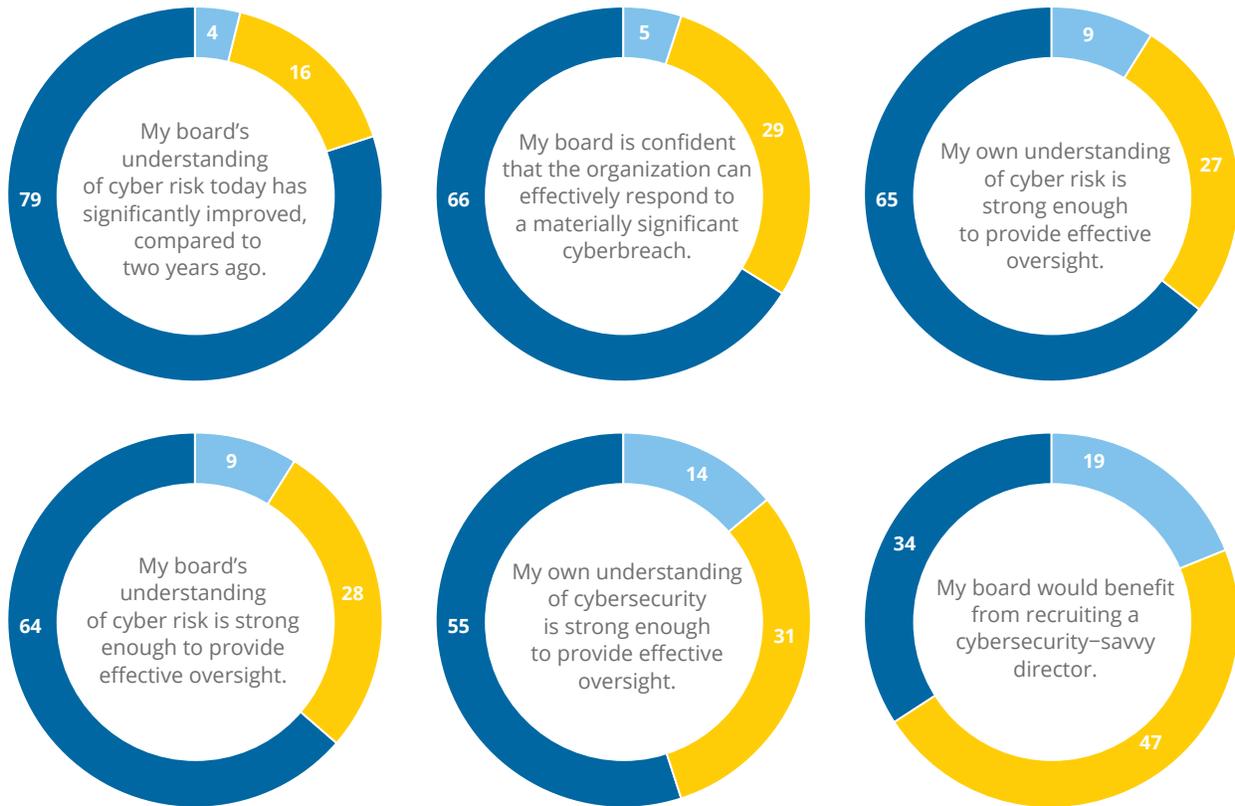
to address a shifting cyber-risk environment and reflect increased governance expectations from key stakeholders, including investors and regulators. This third edition is centered on the same five key principles to enhance cyber-risk oversight:

1. Directors need to understand and approach cyber-security 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 with adequate staffing and budget.
5. Board-management discussions about cyber risk should include identification and quantification of

A serious attack can destroy not only a company’s financial health but also have systemic effects causing harm to the economy as a whole and even national security.

¹ The World Economic Forum, *Global Risks Report 2019* (Geneva, Switzerland: World Economic Forum, 2019), p. 6.

Board Perspective on Cyber-Risk Oversight (percentage of directors)



Source: 2019–2020 NACD Public Company Governance Survey

■ Agree ■ Neither agree nor disagree ■ Disagree n=344–347
Due to rounding, numbers may not add up to 100.

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.

This edition of the Handbook offers new guidance for each of the five key principles and includes an extensive toolkit to help boards adopt the principles. The tools address insider threats, oversight of incident response, and third-party risk management and offers guidance for understanding new management methods to measure cyber risk in empirical and economic terms. In recent years, boards have raised their understanding of cybersecurity matters. According to the *2019–2020 NACD Public Company Governance Survey*, 66 percent of boards agree that they are confident their organization can effectively respond to a materially

significant cybersecurity breach. Moreover, 79 percent of directors report that their boards have significantly improved their understanding of cyber risk compared to two years ago.

While some language in the Handbook refers to public companies, these principles are applicable to—and important for—all directors, 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. In fact, a 2019 NACD survey suggests that the cybersecurity challenge may be especially acute for private companies that are not immune from threats but lack resources to create a robust cybersecurity program. This level of vulnerability demands more proactive and deeper board engagement.²

² NACD, *2018–2019 NACD Private Company Governance Survey* (Arlington, VA: NACD, 2019), p. 15.

A Rapidly Evolving Cyber-Threat Landscape

The 2018 CSIS/McAfee report on cybercrime concluded that “cybercrime is relentless, undiminished, and unlikely to stop. It is just too easy and too rewarding, and the chances of being caught and punished are perceived as being too low. Cybercriminals at the high end are as technologically sophisticated as the most advanced IT companies and, like them, have moved quickly to adopt cloud computing, artificial intelligence, . . . and encryption.”³ In a 2019 survey, CEOs of the largest 200 global companies rated “national and corporate cybersecurity” as the number one threat to business growth and the international economy in the next 5 to 10 years.⁴

Who Gets Attacked, What Gets Attacked, and How

One of the defining characteristics of these attacks 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 until they achieve their goals. The reality is that if a sophisticated attacker targets a company’s systems, they will almost certainly breach them.

In addition, attackers hacking into a system, insider threats including contract workers and employees—whether disgruntled or merely poorly trained—present at least as big an exposure for companies as attacks from the outside. According to McKinsey, insider threats are present in half of all cyberbreaches.⁵ This highlights the need for a strong and adaptable security program, equally balanced between external and internal cyber threats. Organizations can’t deal with advanced threats if they are unable to stop low-end attacks. More recently, cyber extortion through ransomware attacks has significantly increased as a key risk for organizations of all sizes. (See [Tool E – Incident Response](#).)

The vast majority of cyber incidents are economically motivated.⁶ Cyberattackers routinely attempt to



QUESTIONS BOARDS SHOULD ASK SENIOR MANAGEMENT ON INSIDER THREATS

Boards can ask the following questions to better understand what controls are in place to mitigate insider threat risk:

- What systems are in place to vet employees and identify malicious behavior?
- Do employees only gain access to data and systems necessary to do their jobs (no more, no less)?
- Does the security team know exactly which employees have elevated privileges, and are they monitored to ensure they are not abusing their access?

See Tool C: The Cyber Insider Threat—A Real and Ever-Present Danger.

steal, corrupt, or encrypt 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 attack.

Moreover, although many smaller and medium-sized companies have historically believed that they were too insignificant to be targets, that perception is wrong. In fact, the majority of small and medium-sized businesses have been victims of cyberattacks.⁷ In addition to being targets in their own right, 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.

³ CSIS and McAfee, *Economic Impact of Cybercrime—No Slowing Down* (2018), p. 4.

⁴ Source: EY, *CEO Imperative Study* (2019), p. 2

⁵ Tucker Bailey, Brian Kolo, Karthik Rajagopalan, and David Ware, “Insider threat: the human element of cyber risk,” McKinsey & Company, September 2018.

⁶ Louis Columbus, “76% Of IT Security Breaches Are Motivated By Money First,” *Forbes.com*, May 15, 2018.

⁷ Jonathan Crowe, “7 Eye-Opening Cybersecurity Statistics Every Small Business Needs to Know in 2019,” *NinjaRMM Blog*, March 1, 2019.



NO ONE IS IMMUNE TO CYBER RISKS

Some organizations believe that they are unlikely to be the victims of a cyberattack because they are relatively small in size, are not a well-known brand name, and/or don't hold substantial amounts of sensitive consumer data, such as credit card numbers or medical information.

In fact, adversaries target organizations of all sizes and from every industry, seeking anything that might be of value, including the following assets:

- Business plans, including merger or acquisition strategies, bids, etc.
- Trading algorithms
- Contracts or proposed agreements with customers, suppliers, distributors, joint venture partners, etc.
- Employee log-in credentials
- Facility information, including plant and equipment designs, building maps, and future plans
- R&D information, including new products or services in development
- Information about key business processes
- Source code
- Lists of employees, customers, contractors, and suppliers
- Client, donor, or trustee data

Source: Internet Security Alliance

Cyber Threats by the Numbers

A quick review of key statistics makes the point that not only is the cybersecurity challenge stunningly large, but also that it is growing massively on a global scale.⁸

- Annual losses from cybercrime range from \$500 billion to \$1 trillion and are projected to rise to \$5 trillion by 2024.
- One ISP reports 80 billion malicious scans a day.⁹
- There are 300 million new malicious viruses or malware created every day.¹⁰
- There are 4,000 ransomware attacks every day.¹¹
- Just 10 percent of cybercrimes in the United States are reported.¹²
- Sixty-four percent of Americans have lost personal data or had fraudulent charges due to cybercrime.¹³
- On average, breaches are not detected until 146 days after the breach has occurred.¹⁴

The Economics of Cybersecurity Are Upside Down

There is general consensus in the cybersecurity field that cyberattackers are well ahead of the corporations that must defend against them. To begin, the Internet is designed as an “open system” with little thought to security. The tools used to conduct cyberattacks are relatively inexpensive to acquire, and highly profitable when executed. For example, a denial of service attack can be “outsourced” from a criminal provider on the Dark Web for about \$500. Access to corporate mailboxes can be purchased for about \$300 and fake social media account access can be purchased for \$100.¹⁵ The “business model” for cyberattackers is attractive—they can use the same attacks over and over across a world-wide list of targets. Cyberattackers generally have “first mover” advantage, meaning that cyber-risk defenses tend to lag a generation behind the attackers. It is also traditionally difficult for defenders to demonstrate return on investment (ROI) for cyberattack prevention, and successful law enforcement response to such attacks is virtually nonexistent. According to some estimates, less than 1 percent of cyberattackers are successfully prosecuted.¹⁶

This does not mean that defense is impossible. Indeed, the sections covering Principles 4 and 5 as well

⁸ McAfee, “There’s Nowhere to Hide from the Economics of Cybercrime,” on McAfee.com.

⁹ Jack Foster, “21 Terrifying Cyber Crime Statistics,” on dataconnectors.com.

¹⁰ Virginia Harrison and Jose Pagliery, “Nearly 1 million new malware threats released every day,” CNN Business, April 14, 2015.

¹¹ Federal Bureau of Investigation, *How to Protect Your Networks From Ransomware*, p. 2.

¹² Matt Powell, “11 Eye Opening Cyber Security Statistics for 2019,” *CPO Magazine*, June 25, 2019.

¹³ CSIS and McAfee, *Economic Impact of Cybercrime—No Slowing Down* (2018), p. 4.

¹⁴ Jamie Manuel, “I Got Breached—Now What? (Part nine in our series of Canada’s Digital Privacy Act),” *Symantec Official Blog*, February 28, 2017.

¹⁵ CSIS and McAfee, *Economic Impact of Cybercrime—No Slowing Down* (2018).

¹⁶ Roger A. Grimes, “Why it’s so hard to prosecute cyber criminals,” *CSO*, December 6, 2016.

as Tool F describe how organizations can now perform more robust, empirical, and economics-based cyber-risk assessments. By understanding cyber risk in this way, organizations can better measure the impact of various attacks on their business. As a result, the organization can more clearly calculate its cyber-risk appetite, which in turn supports development of a more informed corporate strategy and enhances the ability of the board to oversee management's efforts to address their particular cyber risks. Board members need to ensure that management is fully engaged in making the organization's systems as resilient as economically feasible. This includes developing defense and response plans that are capable of addressing sophisticated attack methods.

Balancing Cybersecurity With Growth and Profitability

Like other critical risks 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 technology, cloud computing, and "smart" devices, can yield significant cost savings and business efficiencies, but they can also create major security concerns if implemented haphazardly.

Similarly, trends such as BYOD (bring your own device), 24/7 access to information, the growth of sophisticated "big data" analytics, 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 also dramatically weaken the security of the organization. It is possible for organizations to defend themselves while staying competitive and maintaining profitability. However, successful cybersecurity cannot simply be "bolted on" at the end of business processes. It needs to be woven into an organization's key systems, processes and culture from end to end—and when done successfully, it can help build competitive advantage.

But to be effective, cyberstrategy must be more than simply reactive. Leading organizations 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.

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

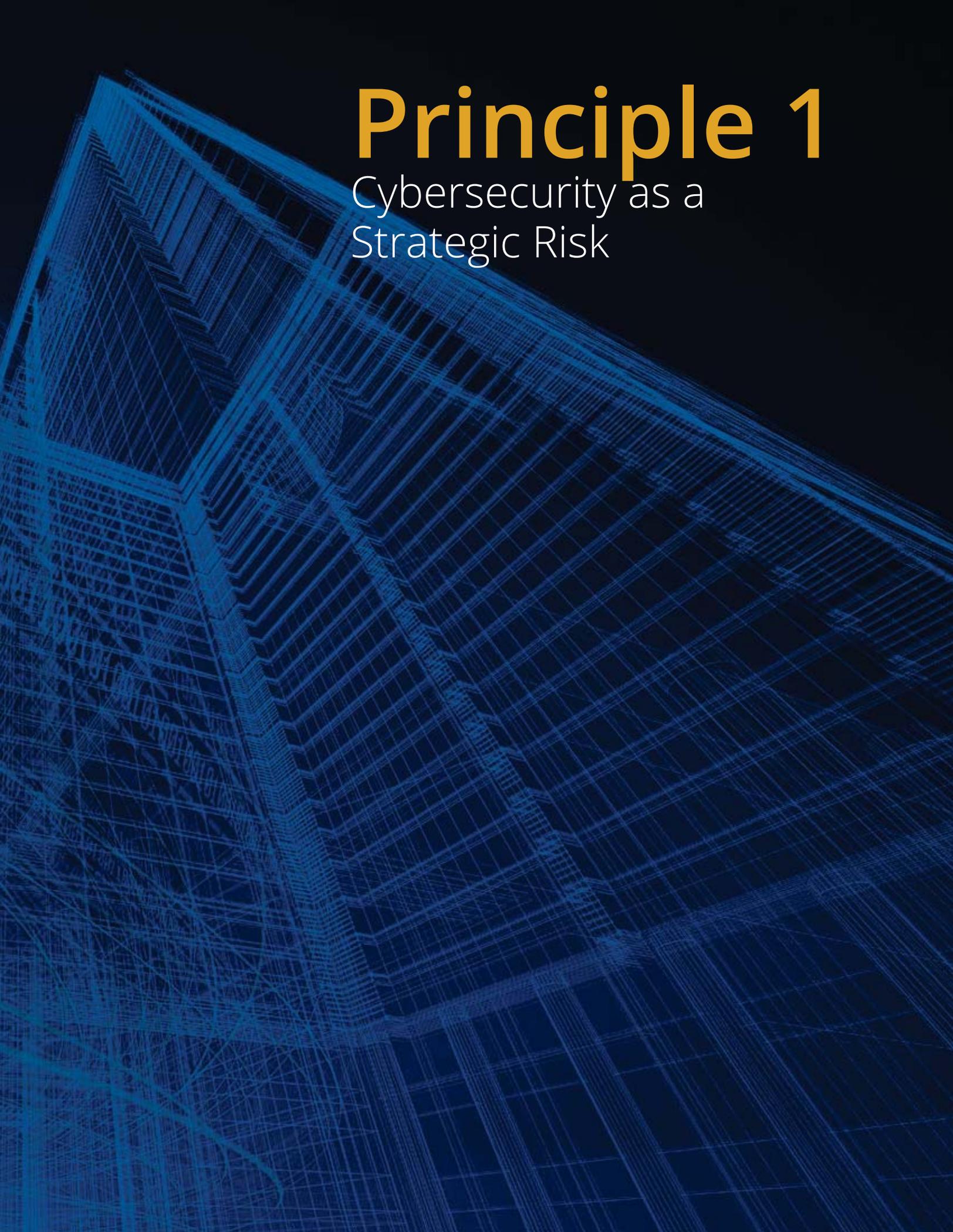


TOOL PREVIEW: BOARD OVERSIGHT OF INCIDENT RESPONSE

Incident response is a critical component of a cybersecurity 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 protection.
- **Protective Capabilities** – policies, education, access controls, protection procedures.
- **Detection** – capabilities to detect anomalies and events.
- **Response** – playbook, regular cyber exercises, coordinated efforts across business units.
- **Recovery** – remediation and after-action improvement.

See Tool E – Incident Response for more information.



Principle 1

Cybersecurity as a
Strategic Risk

Cybersecurity as a Strategic Risk

Directors need to understand and approach cybersecurity as a strategic, enterprise risk—not just as an IT risk.

Historically, many companies and organizations categorized information security as a technical or operational issue to be handled by the information technology (IT) department. This misunderstanding was fed by siloed operating structures that left functions and business units within the organization feeling disconnected from responsibility for the security of their own data. Instead, this critical responsibility was handed off to IT, a department that in most organizations is strapped for resources and budget authority. Furthermore, 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 last several years, technology and data have moved out of their supporting roles and taken center stage as critical drivers of strategy. Executives and board members in organizations of every size and sector now recognize that they need to respond to transformational forces that are “global and highly

complex, encompassing new business models, new entrants and new markets—and always with the looming prospect of next-wave technology disruptors.”¹⁷ The business community’s level of awareness of the importance of information security in general, and the cross-functional nature of cybersecurity in particular, has taken a similar path—fueled in part by the constant stream of headlines about cyber incidents.

While progress has been made, many management teams and boards still hold dated views about cybersecurity. The 2019–2020 NACD Public Company Governance Survey noted that a majority of board members continue to regard cybersecurity as an area for improvement¹⁸ and expect changing cybersecurity threats to have a major impact on their business in the next 12 months.¹⁹ A global information security survey conducted by EY reached similar conclusions, finding that “77% of organizations are still operating with only limited cybersecurity and resilience [against cyber threats], while 87% of organizations warn they

Over the last several years, technology and data have moved out of their supporting roles and taken center stage as critical drivers of strategy.



TOOL PREVIEW: BASELINE QUESTIONS BOARDS CAN ASK ABOUT CYBERSECURITY

- Are we considering the cybersecurity aspects of our major business decisions—such as M&A, partnerships, new product launches, etc.—in a timely fashion?
- What do we consider our most valuable assets? How does our IT system interact with those assets? What would it take to feel confident that those assets were protected?

See Tool B – Assessing the Board’s Cyber-Risk Oversight Effectiveness.

¹⁷ EY, *Navigating the Four Themes of Technology Disruption* (London, United Kingdom: EY, 2015), p. 2.

¹⁸ NACD, *2019–2020 NACD Public Company Governance Survey* (Arlington, VA: NACD, 2019), p. 13.

¹⁹ *Ibid.*, p. 12.

do not yet have sufficient budget to provide the levels of cybersecurity and resilience they want.”²⁰

Executives and board members now recognize that cybersecurity is an integral element in the critical and often very challenging transformations that their companies are undertaking 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 their own major digital transformations with effective management of inherent cyber risk that can compromise the enterprise’s long-term strategic interests. Proper oversight of this difficult balance (and often friction) 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, 83 percent of directors said they would support management undertaking potentially disruptive innovation projects that have the potential to increase long-term value, even if they create additional risks.²¹ Boards and management teams need to acknowledge the potential tension between the need for strategic innovation—increasingly fueled by digital transformation—and the imperatives of preserving security and trust.²² Recognizing the high stakes of successful digital transformation in today’s competitive landscape, we believe that cybersecurity should now be viewed as a means for a company to execute its (digital) strategy as securely as possible. At its best, cybersecurity allows companies to create long-term value and sustain trust with its customers and other key stakeholders.

Greater specifics, including what management needs to present to the board in order to appreciate cyber risk in economic terms, are outlined in Principle 5 and Tool F.

Boards members should also understand what “crown jewels” the company most needs to protect, and ensure that management has a protection, detection, and response strategy. While protection typically starts with the crown jewels, boards can ask management about the process for inventorying cyber risks across

the organization, including how they work across business verticals, to help identify potential vulnerabilities. The board should instruct management to consider not only the highest-probability attacks and defenses, but also low-probability, high-impact attacks that would be catastrophic attacks. These could include separate but interconnected risks that, when combined, create even greater damage.²³ With emerging disruptive technologies on the horizon, it is becoming even more critical for boards and management to continually evaluate whether their current definition of crown jewels is still valid. This can help ensure that the organization is targeting its cybersecurity resources most effectively.

In leading organizations, management teams and boards are starting to integrate the adoption of emerging technologies and data capabilities into discussions about key strategy and plans that cut across the entire organization. Ideally, cybersecurity should be part of the same dialogue. In other words, cybersecurity should be seen as an enterprise-wide strategy and risk-management issue that should be addressed holistically and proactively considered when making major strategic decisions.



IDENTIFYING THE COMPANY'S "CROWN JEWELS"

Directors should engage management in a discussion of the following questions on a regular basis:

- What are our company's most critical data assets?
- Where do they reside? Are they located on one or multiple systems?
- How are they accessed? Who has permission to access them?
- How often have we tested our systems to make sure that they are adequately protecting our data?

²⁰ EY, “Global Information Security Survey,” on EY.com.

²¹ EY and Corporate Board Member, *How Boards Are Governing Disruptive Technology* (2019), p. 3.

²² Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs* (2010), p. 8.

²³ See NACD, *The Report of the NACD Blue Ribbon Commission on Adaptive Governance: Board Oversight of Disruptive Risks* (Arlington, VA: NACD, 2018), pp. 11–12, and the KPMG Audit Committee Institute, *Global Boardroom Insights: The Cyber Security Challenge* (2014), p. 7.



GUIDING PRINCIPLES FOR BOARD-LEVEL METRICS

While the kind of metrics used by an organization will be determined by the organization's unique environment and needs, there are a series of core principles to guide what metrics management should be providing to the board. These metrics should follow these guiding principles:

- Be relevant to the audience (full-board; key committee).
- Be reader-friendly: use summaries, callouts, graphics, and other visuals and avoid technical jargon.
- Convey meaning: communicate insights, not just information.
 - Highlight changes, trends, and patterns over time.
 - Show relative performance against peers, against industry averages, against other relevant external indicators, etc. (e.g., maturity assessments).
 - Indicate impacts on business operations, costs, market share, etc.
- Concise: Avoid information overload
- Above all, enable discussion and dialogue

See Tool F: Board-Level Cybersecurity Metrics.

Source: NACD

Cyber Risk and the Business Ecosystem

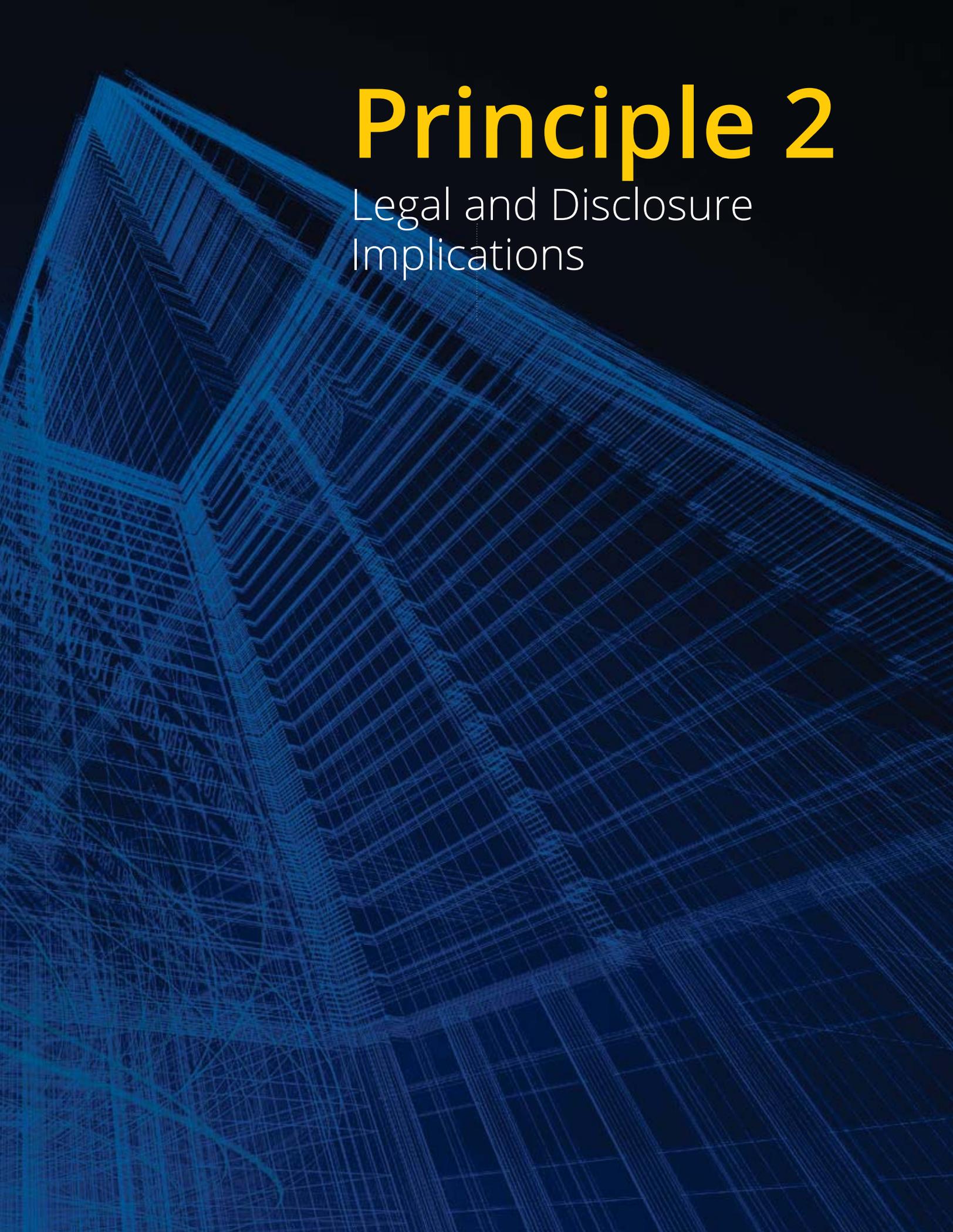
Cyberattacks can take on many different forms and have evolved far beyond traditional hacking. For example, spear phishing—a common email attack strategy that targets specific individuals—is a leading cause of system penetration. Activities such as product launches or production strategies that use complex supply chains that span multiple countries and regions can magnify cyber risk. Similarly, mergers and acquisitions, which have increased in frequency over the past few years and require the integration of complicated systems, often on accelerated time lines and without sufficient time allocated to perform comprehensive due diligence, can increase cyber risk.

Another obstacle companies face in creating a secure system is the degree of interconnection that the organization's network has with its partners, suppliers, affiliates, and customers. Several significant and well-known cyberattacks did not actually start within the target's IT systems, but instead resulted from vulnerabilities in one of their vendors or suppliers.

In addition, organizations are adopting new ways to manage data, (e.g., having some data residing on external networks or in public "clouds"), which can improve cost-effectiveness and efficiency, but also introduce new risks. For example, by outsourcing their data storage, companies have limited direct ability to secure the data, but must make sure that adequate risk-management steps are taken, such as understanding the security tools and monitoring provided by the cloud provider.

As a result, directors should ensure that management is assessing cybersecurity not only as it relates to the organization's own networks, but also with regard to the larger business ecosystem in which it operates. Effective boards will engage management in a discussion of the varying levels of risk that exist across the company's value chain and understand how these less-controllable risks are taken into consideration in the decision making about the company's appropriate cyber-risk posture and tolerance.²⁴

²⁴ See NACD, et al., *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014) (an NACD white paper).



Principle 2

Legal and Disclosure
Implications

Legal and Disclosure Implications

Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.

The legal and regulatory landscape with respect to cybersecurity, including public disclosure, privacy and data protection, information-sharing, and infrastructure protection requirements, is complex and constantly evolving. Boards should stay informed about the current compliance and liability issues faced by their organizations—and, potentially, by board members on an individual or collective basis. Cyber requirements at the US state level vary widely, and each industry faces increasing requirements from US federal regulators. Outside of the US, jurisdictions are increasingly adopting their own cyber regulations, such as the European Union's Network and Information Security Directive and data security and breach requirements such as the General Data Protection Regulation. Some of these requirements now include governance structures, rapid notification of incidents, oversight of third-party vendors, and (in California) statutory damages class-action risk for many notifiable data breaches. Boards should understand whether management has an effective compliance program to meet changing requirements, reporting responsibilities, and related obligations. While some of these regulations are highlighted in this principle and throughout the Handbook, they are examples and far from all-inclusive.

High-profile attacks may spawn lawsuits, including (for public companies) 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 data, sector, and operating locations.

High-profile attacks may spawn lawsuits, including (for public companies) shareholder derivative suits accusing the organization of mismanagement, waste of corporate assets, and abuse of control.

The US business judgment rule may protect directors, so long as the board has taken reasonable oversight before and investigation steps following a cybersecurity incident. Other considerations include maintaining records of boardroom discussions about cybersecurity and cyber risks; staying informed about industry-, region-, or sector-specific requirements that apply to the organization; and determining what to disclose in the wake of a cyberattack. 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.

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 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.

Public Disclosures and Reporting Requirements

Companies and organizations may be subject to a range of disclosure obligations related to cybersecurity risks and cyber incidents, including the following:

- [Interpretive guidance for public companies updated by the US Securities and Exchange Commission \(SEC\) in 2018.](#)
- Industry-specific regulations from the SEC, Federal Trade Commission, and other agencies that affect sectors such as retail, health care, bank-

ing and insurance, chemicals, telecommunications, broker-dealers and registered investment firms, utilities, and critical infrastructure, as well as requirements for government contractors or organizations who hold government data.

- State-level information-security and data-breach notification laws.
- Global regulations, including regional (e.g., European Union), international, and country-specific laws and standards.

Challenges 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 definition of privacy or the “right to be forgotten.” While directors do not need to have deep knowledge about this increasingly complex area of law, they should be briefed by inside or outside counsel on a regular basis about requirements that apply to the company. Reports from management should enable the board to assess whether or not the organization is adequately addressing these potential legal risks.

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, “Investors will have greater confidence that [a] company is not withholding information if it proac-

tively 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.”²⁵ In response, some public companies are increasing their voluntary disclosures, in the proxy statement and elsewhere, about how the board is approaching cyber-risk oversight. (See [Tool J – Enhancing Cybersecurity Disclosures—10 Questions for Boards.](#))

SEC Disclosure Guidance

Cybersecurity has, for several years, been high on the agenda of the US Securities and Exchange Commission (SEC), and in 2011, the Commission’s Division of Corporate Finance issued guidance, calling on companies to assess their disclosure obligations with regard to their cybersecurity risks and cyber incidents.

In 2018, the SEC unanimously approved new [interpretative guidance](#), which outlines requirements for publicly traded companies to disclose cybersecurity risks and material incidents. It underscores that cyber risk poses “grave threats to investors,” the markets, and the country.

In a [statement](#), SEC chairman Jay Clayton urged public companies, “to examine their controls and procedures,” not solely to conform with securities law disclosure obligations, but also keeping in mind financial and reputational considerations. The guidance focuses on the following core areas:



TOOL PREVIEW: QUESTIONS TO ENHANCE COMMUNICATIONS WITH SHAREHOLDERS

1. 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?
2. How do our cybersecurity-related disclosures compare to those of our competitors and industry peers?
3. Is cybersecurity included in the company’s list of risk factors?
4. How do we describe cybersecurity risk management activities?
5. Is cybersecurity included in the areas of expertise that we consider important on the board, and/or does it appear in one or more directors’ biographies?

See [Tool J – Enhancing Cybersecurity Disclosures—10 Questions for Boards.](#)

²⁵ Council of Institutional Investors, *Prioritizing Cybersecurity: Five Investor Questions for Portfolio Company Boards* (April, 2016), p. 5.

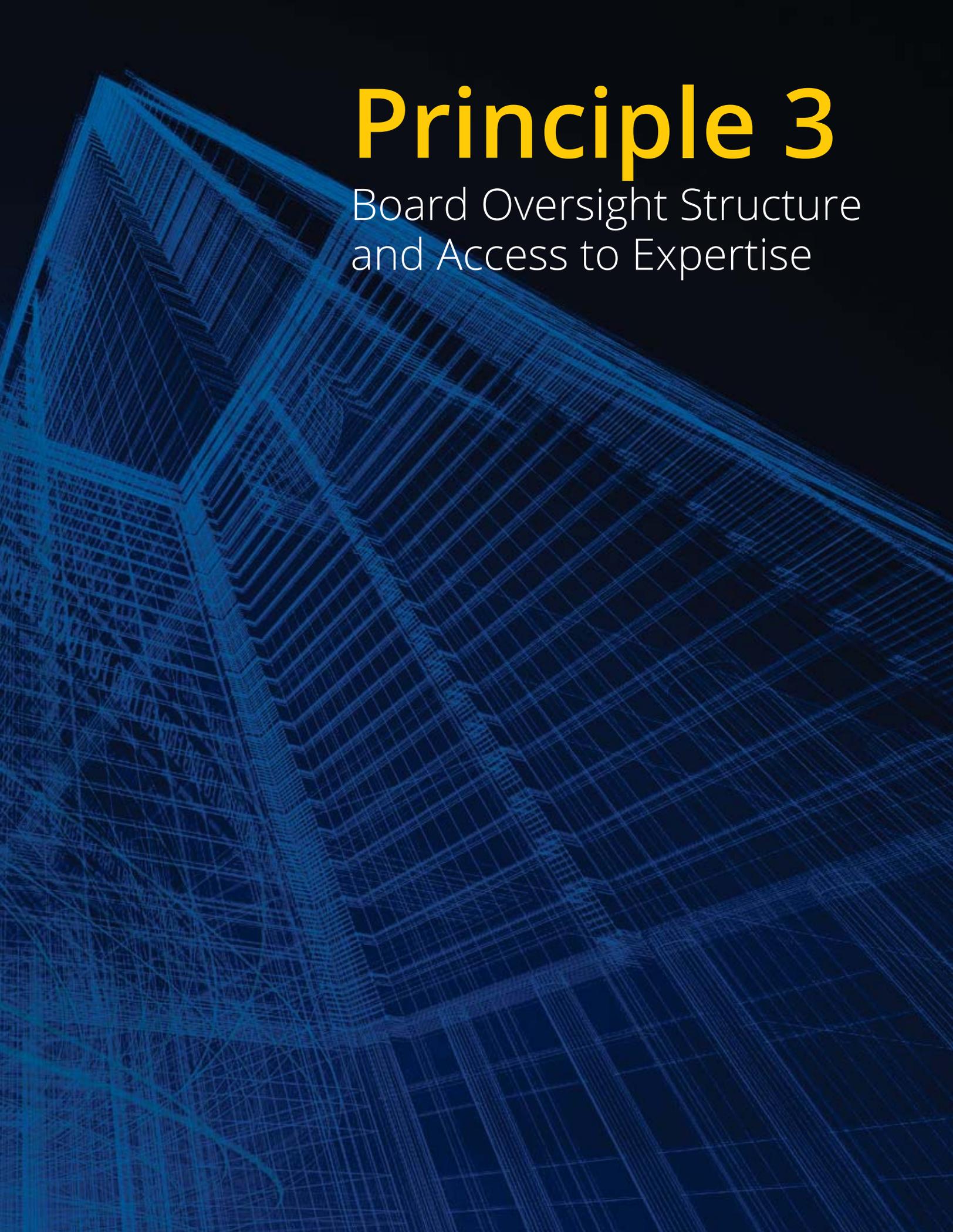
- **Pre-incident disclosure:** The SEC calls for transparency around the identification, quantification, and management of cyber risk across an organization.²⁶ As technology evolves, an organization's attack surface expands, especially as more connected devices are added to networks and reliance on an expansive supply chain evolves. Companies are required to set the stage for the quick identification and management of cyber incidents that have a material impact on their business.
- **Board oversight:** The board's responsibility is to understand cyber risk, quantify it, and oversee it. The SEC advises companies to disclose, as part of their proxy statement, the board's role and engagement in cyber-risk oversight, and notes that the discussion "should include the nature of the board's role in overseeing the management of [cyber] risk."²⁷ In order to respond to the SEC guidance, board members have to be privy to the company's overall cyber exposures, integrating this insight as part of their 360-degree view of the company's risks.
- **Incident disclosure:** The SEC requires companies to "inform investors about material cybersecurity risks and incidents in a timely fashion."²⁸ This requires having structures in place to identify and quantify cyber-risk exposure, allowing the organization to rapidly determine whether a cyberbreach was in fact material, thus requiring transparency to investors and shareholders. One preliminary step is to establish which technology assets and suppliers hold proprietary and confidential data, such as customers' personal details or strategic business information. This insight can also inform decisions on the organization's cyber-risk management strategy, including whether to manage or transfer a specific risk.
- **Controls and procedures:** Companies are expected to assess whether their enterprise-wide risk management processes are sufficient to safeguard the organization from cyber disasters. With a constantly evolving attack surface, there needs to be ongoing due diligence to identify and manage new risks, especially during a merger or acquisition. Most companies have long been doing this when it comes to other perils—for example, natural disasters—and it is imperative to extend the same process to cyber risk.
- **Insider trading:** In a provision that is new to the 2018 guidance, the SEC reminds companies, directors, officers, and other insiders of insider trading prohibitions.²⁹ In practice, this means that directors, officers, and other executives who are aware of a company's cyber vulnerabilities or a breach could be liable if they sell company stock, or instruct anyone else to do so, before such a breach or vulnerability is divulged.

²⁶ See the SEC's *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*.

²⁷ See the SEC's *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, p. 18.

²⁸ *Ibid.*, p. 4.

²⁹ *Ibid.*, p.21.



Principle 3

Board Oversight Structure
and Access to Expertise

Board Oversight Structure and Access to Expertise

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.

Board Responsibility in Cyber-Risk Oversight Is Growing

As the cyber threat has grown, the responsibility (and expectations) of board members also has grown. Directors need to do more than simply understand that threats exist and receive reports from management. They need to employ the same principles of inquiry and constructive challenge that are standard features of board-management discussions about strategy and company performance. As a director at an NACD forum 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.”³⁰

As discussed in Principle 1, leading boards now understand that cybersecurity is not simply a separate discussion item to be addressed for a few minutes at the end of a board meeting. Rather, cybersecurity is an essential element of many board-level business decisions and needs to be integrated into discussions about issues like mergers, acquisitions, new product development, strategic partnerships, and the like at an early stage. As a result, boards need to be accessing information not simply 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 4.

Over the past decade, boards have become more active in overseeing cybersecurity and requiring information from management. A 2012 survey found that fewer than 40 percent of boards regularly received reports on privacy and security risks, and 26 percent rarely or never received such information.³¹

Since then, boardroom practices have changed dramatically. In an NACD

survey of public-company directors, 79 percent now believe their “board’s understanding of cyber risk today has significantly improved, compared to two years ago.”³² In fact, most public-company directors say their boards discuss cybersecurity issues on a regular basis and receive information from a range of management team members. A majority of 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. In fact, more than 75 percent of boards reviewed their company’s current approach to securing its most critical assets against cyberattacks within the past year.³³ (See the chart, [Cyber-Risk Oversight Practices Performed Over the Past 12 Months](#), on page 22.)

Over the past decade, boards have become more active in overseeing cybersecurity and requiring information from management.

³⁰ NACD, et al., *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014) (an NACD white paper), p. 3.

³¹ Jody R. Westby, Carnegie Mellon University, *Governance of Enterprise Security: CyLab 2012 Report*, (Pittsburgh, PA: Carnegie Mellon University, 2012), p. 16.

³² NACD, *2019–2020 NACD Public Company Governance Survey* (Arlington, VA: NACD, 2019), p. 20.

³³ *Ibid.*, p. 10.

Despite these signs of progress, a majority of directors “are looking to improve cybersecurity oversight across the coming year.”³⁴ Only a small percentage of directors believe their board has a “high” level of knowledge of cyber risks, and few organizations say their information security reporting currently fully meets their expectations.³⁵ A study from EY reported that less than half of organizations believed their board and executive management have a sufficient understanding of cybersecurity to fully evaluate preventative measures and cyber risks.³⁶ When asked to assess the quality of information provided by the board to senior management, information about cybersecurity was rated lowest, with nearly a quarter of public-company directors reporting that they were dissatisfied or very dissatisfied with the quality of information provided by management about cybersecurity. Only 15 percent said that they were very satisfied with the quality of the information they received.³⁷

Finally, even in organizations that have implemented good board education programs on cybersecurity, leading directors recognize that this education needs to be regularly refreshed. A recent NACD survey found that a majority of boards see cybersecurity as “an area where board knowledge can grow quickly stale. Since threats are nearly limitless and constantly mutate, directors must assume their current understanding of cyber risks has an expiration date.”³⁸

How Can Boards Access the Cybersecurity Information They Need?

There is no single approach that will fit every board: some 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.

Board members should set clear expectations with management about the format, frequency, and level of detail of the cybersecurity-related information they wish to receive. In reviewing reports from management. This should begin with using the cybersecurity expertise within the company to enhance their knowledge. For example, the organization’s Chief Information Security Officer, or other senior management official responsible for overseeing security, can help the boards better understand cybersecurity.

However, directors should be mindful that there might be an inherent bias on the part of management to downplay the true state of the risk environment. Many boards find the scope of cybersecurity reporting insufficient. One study found that 60 percent of IT staff do not report cybersecurity risks until they are urgent—and more difficult to mitigate—and acknowledged that they try to filter out negative results.³⁹ This potential bias can be mitigated if boards ask management to adopt a more comprehensive and enterprise-wide risk framework and reporting structure discussed in Principle 4.



TOOL PREVIEW: WAYS TO BUILD BETTER RELATIONSHIPS WITH THE SECURITY TEAM AND THE CISO

- Understand the CISO’s role and mandate.
- Spend time with the security team outside the boardroom.
- Assess how the CISO and security team collaborate with other departments within the organization and with stakeholders outside the organization.

See Tool I: Building a Relationship With the CISO.

³⁴ NACD, *Current and Emerging Practices in Cyber Risk Oversight* (Arlington, VA: NACD, 2019), p. 1.

³⁵ “Is cybersecurity about more than protection?” EY Global Information Security Survey, at: https://www.ey.com/en_gl/advisory/global-information-security-survey-2018-2019 (August 16, 2019).

³⁶ *Ibid.*, p. 24.

³⁷ NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p. 28.

³⁸ NACD, *2018–2019 NACD Public Company Governance Survey* (Arlington, VA: NACD, 2018), p. 17.

³⁹ Sean Martin, “Cyber Security: 60% of Techies Don’t Tell Bosses About Breaches Unless It’s ‘Serious,’” *International Business Times*, April 16, 2014.

The nominating and governance committee should ensure the board’s chosen approach is clearly defined in committee charters to avoid confusion or duplication of effort. The full board should be briefed on cybersecurity matters at least quarterly and as specific incidents or situations warrant. Committees with designated responsibility for risk oversight—and for oversight of cyber-related risks in particular—should receive briefings on at least a quarterly basis.

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 meet together once a year for a discussion that includes a “deep dive” on cybersecurity.⁴⁰

Management reporting to the board on relevant cybersecurity matters should also be flexible enough to reflect the changing threat environment, as well as

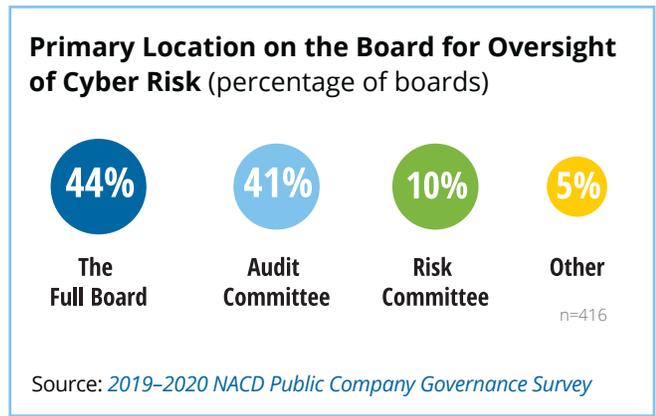
evolving company circumstances and board needs. In a recent brief, NACD highlights a number of factors that may determine how management engages the board, including

- the maturity of the information security program,
- “steady” state vs. after an incident,
- shifting regulatory requirements, and
- director tenure and expertise.⁴¹

While including cybersecurity as a stand-alone item on board and/or committee meeting agendas is now a widespread practice, the issue should also be integrated into a wide range of issues to be presented to the board including discussions on 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. In many ways cybersecurity is now a cross-cutting issue similar to legal and finance. Effective boards approach cybersecurity as an enterprise-wide risk-management issue.

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 can, and ought to, consider augmenting their in-house expertise by using a variety of methods to integrate independent expert assessments. Those



⁴⁰ Adapted from Robyn Bew, “Cyber-Risk Oversight: 3 Questions for Directors,” *Ethical Boardroom*, Spring 2015

⁴¹ NACD, *Current and Emerging Practices in Cyber Risk Oversight*, (Arlington, VA: NACD 2019), pp. 3–4.

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 multiclient 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 to organize the board to manage the oversight of cyber risk—and, more broadly, enterprise-level risk oversight—is a matter of considerable debate. 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.”⁴² Indeed, in 2018, 100 percent of large US public companies included cybersecurity on their list of disclosed risks, and 84 percent included disclosures that at least one board-level committee was charged with oversight of cybersecurity matters.⁴³ Yet just 41 percent of boards assign the majority of cybersecurity-related risk-oversight responsibilities to the audit committee, which also assumes significant responsibility for oversight of financial reporting and compliance risks.

Some companies are considering whether to add cybersecurity and/or IT security expertise directly to the board via the recruitment of new directors. While this may be appropriate for some companies or orga-



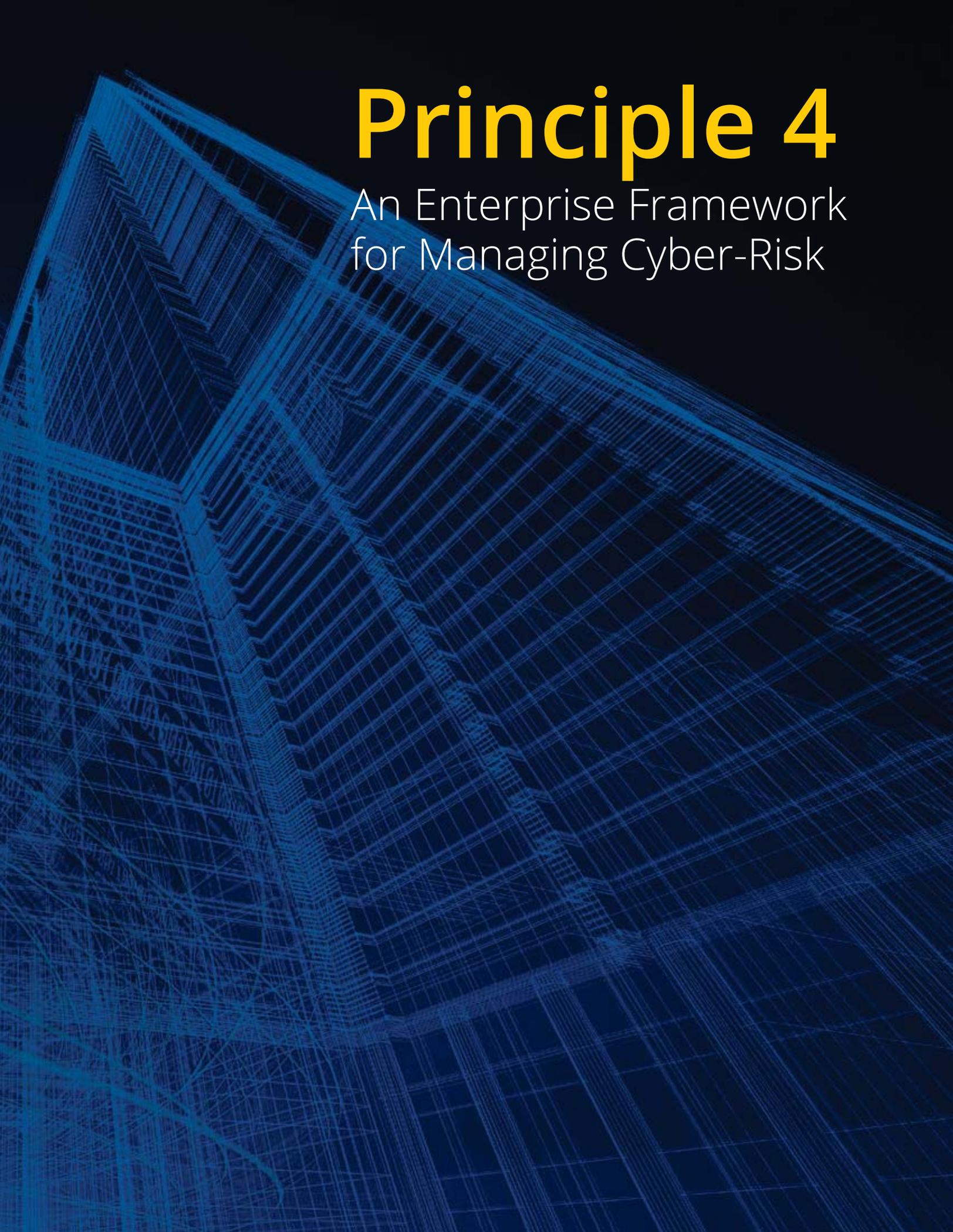
A CYBER EXPERT ON EVERY BOARD?

- How are we defining a “cyber expert”? The very 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 security issues?
- 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 non-financial experts have with these respective issues?
- How does having a single cyber expert on the board mesh with the cross-functional cyber-management structures that are becoming increasingly common (such as the “Three Lines of Defense” model discussed on [page 27](#))?
- Does placing a cyber expert on the board set a precedent for assigning seats to other specialized areas such as diversity or environmental, social, and governance (ESG) matters?

nizations, there is no one-size-fits-all approach that will apply everywhere. 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 (see the sidebar above for questions) a board should consider before opting for this strategy.

⁴² NACD, *The Report of the NACD Blue Ribbon Commission on Adaptive Governance: Board Oversight of Disruptive Risks* (Arlington, VA: NACD, 2018), p. 13.

⁴³ EY Center for Board Matters, *Cybersecurity disclosure benchmarking* (EY, 2018), p. 5.



Principle 4

An Enterprise Framework
for Managing Cyber-Risk

An Enterprise Framework for Managing Cyber Risk

Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.

Principles 4 and 5 of the *Cyber-Risk Oversight Handbook* differ in some respects from the first three principles in that the first three principles focused specifically on what the board should be doing itself and Principles 4 and 5 focus more on what the board should be expecting from management. In order for boards to engage in effective oversight, it is important to fully understand the responsibilities that management has in addressing the organization's cybersecurity. As technology has become more integral to business strategy, management has taken on the role of deploying, managing, and protecting new technology capabilities across the organization. Technology now integrates modern organizations, whether workers are across the hall or halfway around the world. But the existing reporting structures and decision-making processes at many companies are often legacies of a siloed operating model, where each department and business unit makes decisions and manages risks relatively independently, without fully taking into account the digital interdependency that is a fact of modern business.

Directors should seek assurances that management is taking an appropriate enterprise-wide approach to cybersecurity. Specifically, boards should assess whether management has established both an enterprise-wide technical framework as well as a management framework that will facilitate effective governance of cyber risk. An integrated risk model should consider cyber risk not as unique or separate from other business risks, but rather as part of a comprehensive risk-management plan. Having an integrated approach to risk allows businesses to more

effectively address cybersecurity risk across the entire enterprise.

The Technical Framework

Modern digital technology systems are immensely complicated. Moreover, business and competitive pressures demand that organizations continually adapt and update these systems. This could mean adopting artificial intelligence (AI), cloud configurations, blockchain, the Internet of Things, or quantum computing to change business practices and unleash innovation. Clearly, directors cannot be expected to fully track and understand all these changes and their implications for cybersecurity. However, boards should understand from management that they use the appropriate cybersecurity framework to defend the digital technology systems that the enterprise relies on.

Although some organizations choose to adopt a single cybersecurity framework, it is more likely that organizations will select specific aspects of various frameworks and adapt them to their unique business needs. To date, no one framework has been empirically demonstrated as superior from a security perspective (possibly due to the vast variance in cyberattack methods), but increasingly tools are being developed that map to various frameworks and will enable management to determine and in some cases quantify security management of the systems they choose to use. Greater detail on this process is discussed in Principle 5.

Among the most commonly used technical frameworks management can select and adapt are these:

Having an integrated approach to risk allows businesses to more effectively address cybersecurity risk across the entire enterprise

- The National Institute of Standards and Technology (NIST) cybersecurity framework, which consists of “standards, guidelines, and best practices to manage cybersecurity-related risk.”⁴⁴ The NIST cybersecurity framework’s “core” includes five key functions: identify, protect, detect, respond, and recover.⁴⁵ The framework is presented in both a 55-page PDF document⁴⁶ and an Excel table that lists more than one hundred security recommendations.⁴⁷
- The International Organization for Standardization (ISO) created the ISO/IEC 27000 standards for information security.⁴⁸ ISO explains that “using this family of standards will help your organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties.”
- SANS. The Center for Internet Security’s “CIS Controls” include a list of 20 different security controls for organizations, categorized as “basic,” “foundational,” or “organizational.”⁴⁹ These controls range from establishing an inventory of hardware and software assets to penetration testing and red team exercises.⁵⁰
- The Payment Card Industry (PCI) Data Security Standards set “operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.”⁵¹

Establishing A Management Framework for Cybersecurity

Consistent with the understanding outlined in Principle 1 that cybersecurity is broader than simply an “IT” issue is the realization that cyber risk management should not be thought of as the responsibility of just the IT experts. Even with good technical controls, personnel need to be trained in proper use of digital assets, hence a secure culture is a critical aspect of

cybersecurity. Obviously, compliance and legal issues are critical elements of the overall cyber strategy. With the need for increased and better calibrated cybersecurity budgets, finance is a critical function, as is R&D and marketing. For boards, one of the areas of concern regarding cyberattacks is reputational risk, making it important for the public relations and communications departments to contribute to cyber-risk management. Cybersecurity needs to be managed across the enterprise, and many different parts of the organization need to take responsibility for specific activities and be held accountable for their contribution to an effective enterprise-wide program.

There is no one model that will apply perfectly to all organizations, but a cross-functional, multistakeholder approach is almost certainly something boards should consider having management implement. 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 multistakeholder 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*. This basic model stresses not only that multistakeholders ought to be involved 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 a cross-departmental basis. A senior manager with cross-departmental authority, such as the chief financial officer, chief risk officer, or chief operating officer (not the chief information officer), should lead the team.

⁴⁴ National Institute of Standards and Technology, “Cybersecurity Framework.”

⁴⁵ National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, April 16, 2018.

⁴⁶ Ibid.

⁴⁷ National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (Excel download).

⁴⁸ International Organization for Standardization, “ISO/IEC 27001 Information Security Management.”

⁴⁹ Center for Internet Security, “The 20 CIS Controls & Resources.”

⁵⁰ Ibid.

⁵¹ PCI Security Standards Council, “Maintaining Payment Security.”

2. Appoint a cross-organization 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.
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 to 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 "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 take into account 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 more than IT security, the budget for cybersecurity should not be exclusively tied to one department: examples include allocations in areas such as employee training, tracking legal

regulations, public relations, product development, and vendor management.⁵²

Three Lines of Defense Model

A second conceptual model has emerged over the past few years, originating in the financial services sector but increasingly being adopted by leading organizations in various sectors. This "Three Lines of Defense" model stresses multiple independent owners within the organization having varied and increasing roles in assessing and checking cyber-risk management. The model may be summarized this way:

- **Line 1** – operates the business, owns the risk designs, and implements risk management.
 - Line 1 executes risk and control procedures. Each business line defines the cyber risk they face and weaves cyber risk and self-assessment into risk, fraud, crisis management, and resiliency processes.
 - Business lines need to actively monitor existing and future exposures and vulnerability threats and assess what impact cyber risk has on new tech deployment, client relationships, and business strategies.
- **Line 2** – defines policy statements and defines the Risk Management framework. It provides a credible challenge to the first line and is responsible for evaluating risk exposure so that the board can determine risk appetite.
 - Line 2 should be established as a separate independent function. Line 2 manages enterprise cyber-risk appetite and the risk-management framework within overall enterprise risk. Line 2 challenges the first line, determines how to appropriately measure cyber risk, and integrates results into a risk-tolerance statement for the company.
 - The focus of the first and second lines needs to be on effectively managing risk, not on regulatory compliance, although compliance can be integrated into these lines.
- **Line 3** – commonly, internal audit is responsible for independent evaluation of the first and second lines.
 - Line 3 provides an independent, objective assessment of company processes and controls

⁵² Source: Internet Security Alliance. Adapted from Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs* (Washington, DC: ANSI, 2010). See also Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: ISA, 2013).

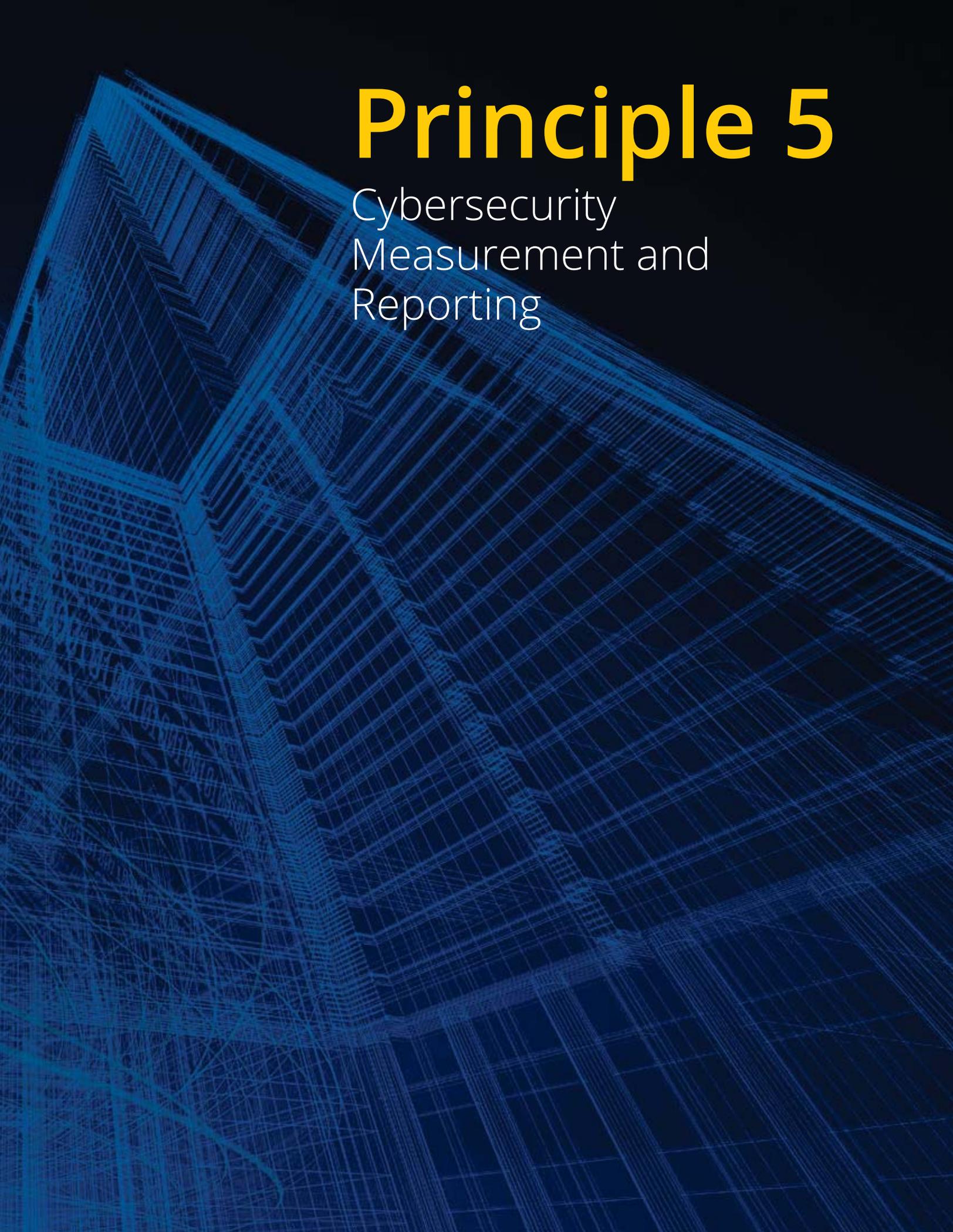
across lines one and two with a focus on operational effectiveness and efficiency. Traditionally, internal audit has focused its testing work on technical IT controls but will need to expand its scope to assess whether cybersecurity is effectively managed as an enterprise risk.

- Internal audit performs process and control assessments, validates technology infrastructure, reviews controls to mitigate third-party risks, conducts independent penetration testing, and stays abreast of new threats.



TOOL PREVIEW: FEDERAL GOVERNMENT CYBERSECURITY RESOURCES

Tool L and *Tool M* present US federal government cybersecurity resources available to the private sector to help inform directors' discussions with management about how the organization is utilizing such resources. *Tool I* contains considerations for building a relationship with the cybersecurity team.



Principle 5

Cybersecurity
Measurement and
Reporting

Cybersecurity Measurement and Reporting

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.

Perfect cybersecurity is an unrealistic goal. Nevertheless, understanding and managing financial exposure to cyber risk is a critical component to board risk oversight. Managing cyber risk—as with all risks in general—is a continuum, not an end state. Beyond existing security initiatives and compliance discussions, understanding cyber risk in economic terms is increasingly important because of the growing, strategic nature of the risk.

Boards need to understand how management has determined the effectiveness of the firm’s controls and processes in reducing the exposure to cyber risk to an acceptable level. This level of quantification of effective cyber-risk management allows the company to make better risk-informed decisions about its strategy and, in turn, its resource-allocation choices. (See “[Defining Risk Appetite](#),” p. 31.)

Traditional risk assessment approaches have had difficulty fulfilling these requirements. Historically, cyber-risk assessments tended to follow long check lists of highly technical information or control requirements—often 500 or more.

These methods have been mostly qualitative and have not assessed cyber risk through economic terms.⁵³ In recent years, quantitative economic assessments of cyber risk have matured to the point where cyber risks can now be quantitatively assessed. Accordingly, similar to the modelling of credit, insurance, and strategic

risks, cyber risks can now be modeled quantitatively to improve risk-management performance.

It is rather common to see cyber-risk assessment outcomes expressed as “critical,” “high,” “medium,” etc. While this kind of rating does provide a measure of order of magnitude (ordinal measurement), it does not help decision makers to effectively compare different kinds of cyber risk or to compare cyber

risks with other kinds of risks faced by the organization. After all, how can you compare a “high” cyber risk to a “high” financial risk? Which risks warrant greater investment and which risks should we accept? Quantitative assessments allow organizations to drill down and consider the likelihood, impact, velocity, duration

and interdependency for these risks, which helps management and boards to make informed decisions about the relative criticality of these risks and funding strategies for their mitigation.

Boards are expected to establish transparent and quantitative means for evaluating and understanding an organization’s cyber-risk exposure. The US Securities and Exchange Commission released guidance in 2018 to assist public companies in preparing disclosures about cybersecurity risks and incidents.⁵⁴ To address these increased expectations, companies need to understand the financial impact associated with cyber-event risk. Boards of directors and management

Quantitative assessments allow organizations to drill down and consider the likelihood, impact, velocity, duration and interdependency for these risks, which helps management and boards to make informed decisions.

⁵³ Jack Jones, *Understanding Cyber Risk Quantification: A Buyer’s Guide* (2019).

⁵⁴ See <https://www.sec.gov/rules/interp/2018/33-10459.pdf>, Section 2. Risk Factors.

are also expected to demonstrate to investors due care in the governance and oversight of cyber risk. Moreover, credit rating agencies such as Moody's are beginning to incorporate a financial quantitative measurement related to cyber-risk exposure, signaling that cyber risk will necessarily become a core component to overall corporate financial management. Leveraging these mathematical and scientific methods for improved analyses can allow for more effective decision making compared to qualitative types of risk scoring and heat map risk reporting.⁵⁵

Increased Understanding of Cybersecurity Economics

As companies recognize the value of quantification of cyber risk, much work is being done to enable more advanced quantitative analysis. Several methods have emerged in recent years for expressing cyber risks in economic terms in place of subjective ordinal scales. These more contemporary methodologies, such as X-Analytics, Factor Analysis of Information Risk, and various cyber Value at Risk (VaR) models tend to view cyber risk not as categories (e.g., supply chain or insiders) but through potential financial loss.

In summary, by calculating the degree of their financial exposure to cyber risk, organizations can better determine where to place and prioritize their cybersecurity investments to address the greatest, most impactful risks.

Tool F on Board-Level Cybersecurity Metrics provides greater detail as to how this is done. However, there are questions that boards can ask to ensure management is using these types of cyber-risk assessment.

At a conceptual level, boards should consider asking questions such as the following:

- **What data, and how much data, are we willing to hold, lose, share, or have compromised as a practical business matter?** In this context, distinguishing between mission-critical assets and other data that is important, but less essential, is a key first step. Besides data loss, business disruption must also be considered. How long can we afford to be down? If our data was inaccessible due to ransomware, would we pay the ransom?

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 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 proper monitoring, trending and communication is 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*

⁵⁵ Hubbard, Douglas W., and Richard Seiersen, *How to Measure Anything in Cybersecurity Risk* (Hoboken, NJ: John Wiley & Sons Inc., 2016).

- **How should cyber-risk mitigation investments be allocated among basic and advanced defenses?** Most organizations typically apply security measures equally to all data and functions. However, protecting low-impact systems data from sophisticated threats could require greater investment than the benefits warrant. For those lower-priority assets, organizations should consider accepting a greater level of security risk than higher-priority assets, as the costs of defense will likely exceed the benefits. Boards should encourage management to frame the company's cybersecurity spending in terms of Return on Investment (ROI), and probability of occurrence associated with exploitation. They should also reassess probability of occurrence and reassess ROI regularly, as the costs of protection, the company's asset priorities, and the magnitude of the threat will change over time.
- **What options are available to assist us in mitigating certain cyber risks?** Organizations of all industries and sizes have access to end-to-end solutions that can assist in lessening some portion of cyber risk by directly reducing the probability of exploitation. Beyond coverage for financial loss, they include a battery of preventative measures, such as reviews of cybersecurity frameworks and governance practices, employee training, IT security, expert response services, and consultative security services. The inclusion of these value-added services proves even further the importance of moving cybersecurity outside of the IT department into enterprise-wide risk and strategy discussions at both the management and board levels.
- **What options are available to assist us in transferring certain cyber risks?** Cyber insurance is a control and exists to provide financial reimbursement for unexpected losses related to cybersecurity incidents. This may include accidental disclosure of data, such as losing an unencrypted laptop, or malicious external attacks, such as phishing schemes, malware infections, or denial-of-service attacks. Determining when this option makes economic sense requires the ability to quantify the return it provides versus other controls. Cyber insurance would not be the first option chosen but it is practical when the risk reduction it achieves versus cost is a better value than the risk reduction other measures would provide. When choosing a cyber-insur-

ance partner, it is important for an organization to choose a carrier with the breadth of global capabilities, expertise, market experience, and capacity for innovation that best fits the organization's needs. Insurers frequently conduct in-depth reviews of company cybersecurity frameworks during the underwriting process, and policy pricing can be a strong signal that helps companies understand their cybersecurity strengths and weaknesses, providing a potential path to improve their cybersecurity maturation. Many insurers, in partnership with technology companies, law firms, public relations companies and others, also offer access to the preventative measures discussed above.

- **How should the impact of cybersecurity incidents be assessed?** Conducting a proper impact assessment can be challenging given the number of factors involved. To take just one example, publicity about data breaches can substantially complicate the risk-evaluation process. Stakeholders—including employees, customers, suppliers, investors, the press, the public, and government agencies—may see little difference between a comparatively small breach and a large and dangerous one. As a result, reputational damage and associated impact (including reactions from the media, investors, and other key stakeholders) may not correspond directly to the size or severity of the event. The board should seek assurances that management has carefully thought through these implications in devising organizational priorities for cyber-risk management.

Early Methods for Economically Assessing Cyber Risk

Management can use systematic methods to determine their exposure to cyber risk. Effective assessments include technical analysis but go beyond that to fold in other aspects of the business. Sophisticated assessments can be presented to the board, enabling directors to help management determine the organization's risk appetite and appropriate allocation of resources.

Key steps toward more advanced cyber-risk assessment and management may include these:

- Management should seek out the best data available to make assessments of possible attack scenarios.

- Management should focus on scenarios that are probable and would yield an expected loss significant enough to matter to the business.
- Calculate the best case, worst case, and most likely case of attack and identify what degree of loss is acceptable (risk appetite).
- Determine the investment required to mitigate, or transfer, risk to an acceptable level.
- Run multiple scenarios using methods such as Monte Carlo simulations to more accurately define risk and mitigation costs to various scenarios.



ASSESSING THE ECONOMICS OF CYBER-SECURITY

Below are a few sample questions boards can consider asking management that will help to assess the current economics of a company's cyber risks and its cybersecurity efforts:

- What are our quarterly expected loss ratio metrics related to our cyber-risk condition across our various business units and operating environments?
- What is the financial impact related to our cyber-risk worst-case scenario?
- What processes have we established related to making cyber-risk acceptance, cyber-risk remediation, and cyber-risk transfer decisions? How do we measure how these decisions reduce our financial exposure to cyber risk?
- How are we measuring and prioritizing our control-implementation activities and cybersecurity budgets against our financial exposure to cyber risk? Have we connected our control implementation strategy and cybersecurity programs, including budgets, with our cyber-risk transfer strategy?
- Based on our financial performance targets, how can cyber risk impact our financial performance? What is our annual cyber-risk expected loss value?

See Tool F - Board-Level Cybersecurity Metrics.

Conclusion

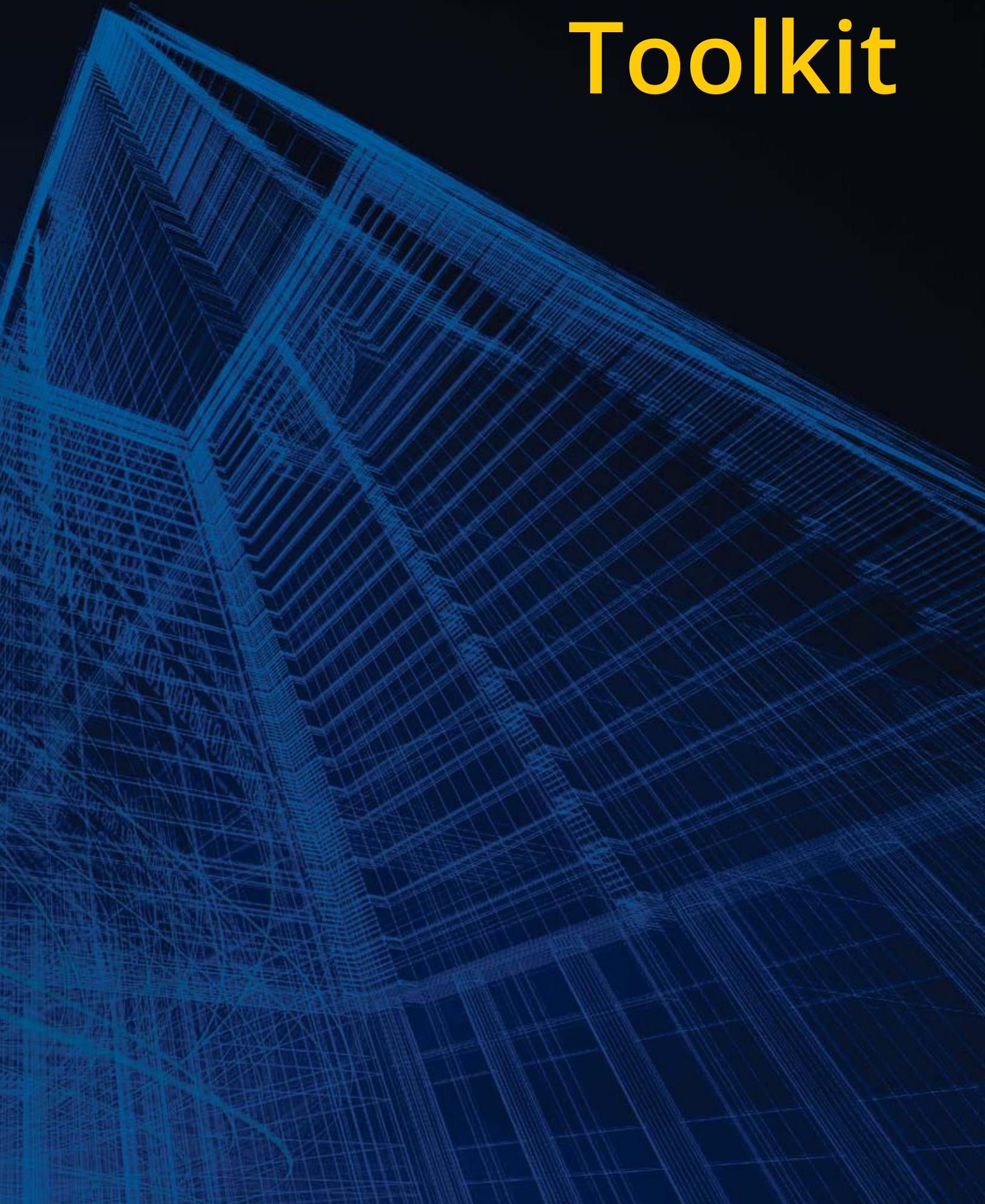
Cybersecurity is now a serious, enterprise-level risk and strategy challenge. Several characteristics make the nature of the threat especially formidable: its complexity and speed of change; the potential for significant financial, competitive, and reputational damage; and the fact that complete protection is an unrealistic objective. Despite dramatic increases in private-sector cybersecurity spending, the economics of cybersecurity still favor the attackers. Moreover, many technological innovations can increase vulnerability to cyber threats.

Boards need to continuously assess their effectiveness in addressing cybersecurity, both in terms

of their own fiduciary responsibility as well as their oversight of management's activities. While the approaches taken by individual boards will vary, the principles in this Handbook offer a helpful blueprint and timely guidance.

Ultimately, as one director put it, "Cybersecurity is a human issue." The board's role is to bring its judgment to bear and provide effective guidance to management, in order to ensure the cybersecurity program is appropriately designed and sufficiently resilient given their company's strategic imperatives and the realities of the business ecosystem in which it operates.

Toolkit



Road Map for the Cyber-Risk Oversight Toolkit

While the five core principles offer an overall governance approach that boards can adopt to oversee cybersecurity, the following tools provide practical guidance to implementing these principles. Below is a road map that links the five cyber-risk oversight principles with the corresponding tools:

Principle 1

Directors need to understand and approach cybersecurity as a strategic, enterprise risk—not just as an IT risk.

- **Tool A** – 10 Questions for a Board Member to Ask About Cybersecurity
- **Tool B** – Assessing the Board’s Cyber-Risk Oversight Effectiveness
- **Tool G** – Cybersecurity Considerations During M&A Phases—Mergers and Acquisitions

Principle 2

Directors should understand the legal implications of cyber risks as they relate to their company’s specific circumstances.

- **Tool B** – Assessing the Board’s Cyber-Risk Oversight Effectiveness
- **Tool D** – Supply Chain and Third-Party Risks
- **Tool E** – Incident Response
- **Tool J** – Enhancing Cybersecurity Oversight Disclosures—10 Questions for Boards
- **Tool L** – Department of Homeland Security Cybersecurity Resources
- **Tool M** – Department of Justice and Federal Bureau of Investigation—Responding to a Cyber Incident

Principle 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.

- **Tool A** – 10 Questions for a Board Member to Ask About Cybersecurity
- **Tool B** – Assessing the Board’s Cyber-Risk Oversight Effectiveness
- **Tool C** – The Cyber-Insider Threat—a Real and Ever-Present Danger
- **Tool I** – Building a Relationship With the CISO
- **Tool K** – Personal Cybersecurity for Board Members

Principle 4

Directors should set the expectation that management will establish an enterprise-wide, cyber-risk management framework with adequate staffing and budget.

- **Tool C** – The Cyber-Insider Threat—a Real and Ever-Present Danger
- **Tool D** – Supply Chain and Third-Party Risks
- **Tool E** – Incident Response
- **Tool G** – Cybersecurity Considerations During M&A Phases—Mergers and Acquisitions
- **Tool I** – Building a Relationship With the CISO

Principle 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.

- **Tool B** – Assessing the Board’s Cyber-Risk Oversight Effectiveness
- **Tool F** – Board-Level Cybersecurity Metrics
- **Tool H** – Sample Dashboards

Tool A – 10 Questions for a Board Member to Ask About Cybersecurity

By Jeff Brown, Chief Information Security Officer, Raytheon



OBJECTIVE OF THE TOOL:

This tool offers suggested questions that board members can ask management to conduct oversight of their cyber-risk management, and explains what answers to those questions might look like.

The questions that follow do not encompass everything a company must do to protect itself. However, these questions should be a good start to give a board some confidence that the company understands what it needs to do and is structurally set up to succeed.

Tier 1. Policy and Governance

This covers a set of prerequisite control issues that every organization must address. If these questions are not satisfactorily answered, continuing on to Tier 2 and Tier 3 questions will offer little useful insight.

1. How is personally identifiable information (PII) treated domestically and internationally? What are the safeguards of stolen equipment?

Why it's important: The legal and branding penalties for PII violations are severe and very public. Requirements vary greatly between states, and especially between countries. With the preponderance of employee computing assets being laptops or tablets, it is a safe bet that some will be lost or stolen.

Helpful answer: "We know where all of our PII is stored. We have it encrypted at rest and in transit. All of our employees who routinely handle PII are trained in safeguarding procedures. We have periodic (usually annual) training on PII for our employees. We are aware of the differences in PII requirements, especially in Europe, and have taken the necessary additional steps to comply."

Answers that demand additional prodding:

- "Our employees won't accept disk encryption of their laptops."
- "We don't have that much PII."
- "Our non-HR employees don't handle PII, so we don't need to train them."

2. How many third parties have access to your systems, and what controls are placed on them?

Why it's important: This would include outsourced cloud applications (such as those commonly used for customer-relationship management or payroll, for example), applications or systems that are located on your premises but managed by a third party from off-site (such as facility monitoring), or outsourced infrastructure. Employees of third parties seldom screen their employees as well as you would yourself. Their controls tend to be generic. In addition, advanced threats are increasingly targeting suppliers, so a compromised supplier-employee account could be a back door into your systems. It is much harder to "know when you fail" when your data and systems are outsourced.

Helpful answer: "We have a formal process for reviewing third-party contracts and connectivity. Third-party personnel screening requirements and system security requirements are included in contracts. Access by individuals is strictly controlled to limit them to necessary data only."

Answers that demand additional prodding:

- "We rely on our suppliers to be secure."
- "Each line of business manages their own suppliers' access."
- "We don't really have a good listing of the data that third parties have access to."

3. **Do you have an incident response plan for addressing the loss of your own or a customer's intellectual property?**

Why it's important: When a customer's program data is stolen through a sophisticated attack, when there is a PII breach that must be disclosed, or when an employee leaks information about a compromise that would not have otherwise been made public, the company's leadership team must be engaged. It is no longer an IT security activity. Legal must address the regulatory implications. Communications must deal with the press. A product group must talk to the customers. For a PII breach, Human Resources must inform employees. And in some sectors, companies are responsible for reporting supplier breaches, so Supply Chain and Contracts/Procurement must be involved. A plan needs to be in place and exercised.

Helpful answer: "Our company-level incident response plan includes provisions for cyber events, especially those that would require notification to customers or regulators. The entire senior leadership team is involved. We exercise or table top the plan periodically."

Answers that demand additional prodding:

- "The lines of business are responsible for this."
- "Every event is so different that planning for it is futile."
- "We are not a target, so we don't need to be this sophisticated in our approach."

Tier 2. Core Security Infrastructure and Processes

These are some of the best practices for enterprises who wish to be effective, particularly against sophisticated attackers and any other cyber threat. The items listed below are essential to successfully managing these attacks. In the end, if a company doesn't get these three practices right, most of their other cyber-protection efforts risk being overwhelmed.

4. **Do you allow anything in your network to talk directly to the Internet?**

Why it's important: When an individual employee's computers (desktops or servers) can talk directly to the Internet it bypasses all points at which the traffic can be monitored or screened. That leaves the company with some liability for failing to screen out harassing traffic or prevent inappropriate surfing. More important, attackers love this configuration. They have direct access to their targets without annoying defenses in the way.

Helpful answer: "No user or server can talk directly to the Internet. Everything we have goes through a proxy of some sort to mask our internal structure and provide a governance and monitoring point."

Answers that demand additional prodding:

- "Our engineers insist on direct Internet access to do research."
- "Web proxies are too expensive."
- "Some of our applications need direct access." (Yes, the poorly designed applications!)

5. **Do you allow single-factor authentication for remote access?**

Why it's important: When an attacker gets into your network, the first thing they will do is try to capture passwords via any number of relatively easy methods. They almost always succeed. If a company's virtual private network (VPN) access or email access uses only UserID and passwords (single factor) the attacker no longer has to attack your company. They simply log on as one of your employees with all of his or her accesses and privileges. They become an insider.

Helpful answer: "All remote-access VPN requires two-factor authentication. Specific Internet-facing websites may have single factor or no authentication after a governance process validates that the website contents are releasable to the public."

Answers that demand additional prodding:

- "We have single-factor VPN."
- "We use single-factor Outlook Web Access."

6. **How do you manage your Internet gateways?**

Why it's important: Internet gateways are the first line of a layered defense. If they are managed or designed poorly it puts too much stress on all your other defenses. More so than anywhere else in the network, consistency here will make or break your security. That usually implies central management, as local IT personnel are too susceptible to training gaps and pressures from local leadership to bypass key, but inconvenient, controls. Central management is also almost always cheaper.

Helpful answer: “All gateways [it doesn’t matter how many] are managed by a single group using common tools and processes. This ensures our configurations of routers, firewalls, proxies, etc., are all consistent. All the logs from the gateways are pulled back for central review and archiving.”

Answers that demand additional prodding:

- “Each of our geographic regions or businesses run their own.”
- “Internet access is a site responsibility.”
- “We have standards; we expect our businesses/sites to adhere to them.”

Tier 3. Advanced Defenses

If the answers to all of the above questions are satisfactory, then a director can probe a bit deeper into some of the less common, but highly effective, practices indicative of the top cyber-defense organizations.

7. How do you use and store netflow data?

Why it’s important: Netflow data is the single most important set of data you have to investigate incidents. It is simply a record of the traffic metadata in your network: what addresses talked to each other and when, what protocol was used (mail, web, control, etc.) and how much data was transferred. The data allows you to track the movements of an attacker throughout the network. Without it, the chances of finding all the computers the attacker accessed is slim. You miss one compromised computer and you will be doing the investigation again in six months.

Helpful answer: “We collect netflow data from almost every router in the network [not just at the Internet gateways]. We store at least three months’ worth of data [preferably much longer] and have the people on staff who know how to analyze the data.”

Answers that demand additional prodding:

- “What’s netflow?”
- “We only keep X days, because storage costs are high.”
- “It’s on our road map.” (Turning it on and storing it is not a technical challenge.)

8. Is there a central authority governing all of your active directory domains?

Why it’s important: Active directory is the enforcement mechanism for all desktop security policies. A single domain, or a small set of centrally managed domains, allows you to consistently enforce desktop policies. It also allows for rapid mitigations for many zero-day attacks. Finally, you can run various tools on active directory databases to eliminate inactive objects (people or machines). Having multiple, diverse databases reduces the efficiency.

Helpful answer: “We have a single domain throughout the company [or very few]. They all have the same design and are managed by a single group of domain administrators.”

Answers that demand additional prodding:

- “Each business or region runs its own.”
- “Our administrators [or outsourcers] need to be able to remotely manage servers easily.”

9. How do you get your actionable, unclassified cyber intelligence?

Why it’s important: Nobody can be successful on their own in IT security. You need teammates. Having and acting on intelligence quickly will cost very little but can go a long way toward protecting a company which is in the second wave of the attack.

Helpful answer: “We are members of our industry Information Sharing and Analysis Center [ISAC/ISAO]. We also have purchased several commercial threat feeds. We have processes for moving the intelligence into our network sensors and processes.” Alternatively, a good answer would be this one: “Our managed security provider has access to numerous intelligence feeds.”

Answers that demand additional prodding:

- “We just don’t have the time or expertise.” (This answer will be more common among smaller companies.)
- “We’re good enough that we don’t need to collaborate.”
- “We do, but we don’t get much out of it.” (You get out what you put in.)

10. Do you employ a data-leak prevention product as part of an insider threat program?

Why it's important: Insider threats are often cited as the most serious cyber threat, because an insider has already had access for a prolonged period. That is even more true when you consider that once a sophisticated attacker is in a network they are essentially an insider. So being able to detect abnormal activity or activity that violates policy is becoming increasingly critical. In some industries, such as finance or pharmaceuticals, it is essential to their survival.

Helpful answer: "As part of a larger program, we employ desktop or perimeter data-leak prevention systems. We have a group of people [either in IT security or industrial security] who monitor and act on the alerts."

Answers that demand additional prodding:

- "There are too many false positives." (This is often true, but good tuning can make the number tolerable.)
- "We tried it, but we acquired too much private employee information."
- "We don't want to look like Big Brother."

Tool B – Assessing the Board’s Cyber-Risk Oversight Effectiveness

By Richard Puckett, Vice President of Security, Operations, and Strategy, Thomson Reuters



OBJECTIVE OF THE TOOL:

This tool helps directors identify which questions to ask senior management 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 the Board’s Cyberliteracy

1. 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?
2. Are we able to effectively interpret/assess management’s presentations and their answers to our questions?
3. 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?
4. Is the organization adequately monitoring current and potential cybersecurity-related legislation and regulation?
5. Does the company have 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?

USE THE NUMERICAL SCALE TO INDICATE WHERE THE BOARD’S CULTURE GENERALLY FALLS ON THE SPECTRUM SHOWN BELOW.		ACTION ITEM
We classify cyber risk as an IT or technology risk.	<div style="display: flex; justify-content: space-around; align-items: center;"> ← 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 → </div>	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).	<div style="display: flex; justify-content: space-around; align-items: center;"> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 </div>	Cybersecurity is incorporated into forward-looking discussions with management (e.g., new product/service development, M&A/joint ventures, market entry).
The board receives information about cybersecurity exclusively from management.	<div style="display: flex; justify-content: space-around; align-items: center;"> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 </div>	The board receives firsthand information about cybersecurity from non-management sources.
Information about emerging cyber threats or potential issues is filtered through the CEO.	<div style="display: flex; justify-content: space-around; align-items: center;"> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 </div>	The CEO encourages open access and communications between and among the board, external sources, and management about emerging cyber threats.

6. Does our organization participate in any of the public- or private-sector ecosystem-wide cybersecurity and information-sharing organizations?
7. Is the organization adequately monitoring current and potential cybersecurity-related legislation and regulation?
8. Does the company have 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?

CASE IN POINT



Lax Security Culture Allowed North Korean Hackers to Penetrate a Multinational Corporation and Entertainment Industry Leader

In 2014, a multinational entertainment industry corporation reported a “brazen attack” on the company. Hackers penetrated the company’s information systems, stole data, and leaked sensitive information online, including copies of unreleased films and embarrassing emails. The attackers also used malware to erase assets within the company’s information systems. The US government blamed North Korea’s government for the attack.

At the time, former employees stated that the company’s lax security practices contributed to the attack. One employee noted that they would report security violations to the security team and repeated reports would be ignored. Another former employee explained that the company had no real understanding of information security and no real investment in it.

This incident could have been avoided or more effectively managed if the company had had more robust oversight of cybersecurity to ensure a strong security culture was present at all levels of the organization.

Source: Hilary Lewis, “Sony Hack: Former Employees Claim Security Issues Were Ignored,” *The Hollywood Reporter*, December 5, 2014.



International Banking System Exhibits Strong Leadership in Response to Breach

In 2016, a bank in Asia experienced a major cyberattack, resulting in millions of dollars being transferred through the international SWIFT banking network. Although the SWIFT network was not compromised through this breach, SWIFT leadership proactively took action to preserve its reputation and delivered a message to all its clients that weaknesses in their systems would no longer be tolerated. SWIFT also created the Customer Security Program following this incident. This program led to the establishment of a customer security control framework providing a variety of mandatory and suggested criteria for SWIFT clients. This framework established a security baseline for all of the 11,000 banking institutions that use SWIFT. As a result of this program, by 2018, 94 percent of SWIFT clients had attested to their compliance with the framework.

Source: Rachael King, “Central Banking FinTech RegTech Global Awards 2019,” *Central Banking*, September 4, 2019.

Tool C – The Cyber-Insider Threat— a Real and Ever-Present Danger

By Gary McAlum, Chief Security Officer, USAA; Adrian Peters, Chief Technology Risk Officer, BNY Mellon; and J. R. Williamson, Chief Information Security Officer, Leidos



OBJECTIVE OF THE TOOL:

Of all the issues around cyber risk, perhaps the greatest challenge is mitigating the insider threat. The cyber-insider threat encompasses employees, contractors, vendors, and others who have legitimate access to the network, systems, and/or data of the organization to some degree. This Tool outlines the types of insider threats businesses face and questions boards should be asking to ensure management is adequately addressing insider threats.

Verizon's *Data Breach Report* identified five types of cyber-insider threats:¹

- **Careless Workers:** Employees or partners who non-maliciously misappropriate resources, break acceptable use policies, mishandle data, install unauthorized applications, or use unapproved workarounds
- **Inside Agents:** Insiders recruited, solicited, or bribed by external parties to exfiltrate data
- **Disgruntled Employees:** Insiders recruited, solicited, or bribed by external parties to exfiltrate data
- **Malicious Insiders:** Actors with access to corporate assets who use existing privileges to access information for personal gain
- **Feckless Third Parties:** Business partners who compromise security through negligence, misuse, or malicious access to, or use of, an asset

This Tool will help boards of directors ask senior management the right questions to ensure that these wide-ranging cyber-insider threats are being properly mitigated.

Questions Boards Should Ask Senior Management About Insider Threats

- What systems are in place (background checks, channels that allow employees to report concerns, etc.) to vet employees and identify malicious behavior? Is there a strong collaboration between information security, physical security, general counsel, human resources, corporate investigations, and other key partners in managing these systems?
- Do employees only gain access to the data and systems necessary to their jobs (no more, no less)? How is access managed when an employee leaves the company or accepts a new position within the company?

COMMON INDICATORS OF INSIDER THREATS

There are certain warning signs companies can watch for to identify an insider threat:

- Poor performance appraisals
- Voicing disagreement with policies
- Disagreements with coworkers
- Financial distress
- Unexplained financial gain
- Odd working hours
- Unusual overseas travel
- Leaving the company

Source: Ellen Zhang, "The Early Indicators of an Insider Threat," *Data Insider* (blog), January 14, 2019.

¹ Verizon, *Verizon Insider Threat Report: Out of sight should never be out of mind* (2019), p. 5.

- Does the security team know exactly which employees have elevated privileges, and are they monitored to ensure that they are not abusing their access?
- Are processes and technologies in place to detect and prevent information from leaving the network? Are these enforced to control use of removable media (like USB drives)?
- Is a data classification policy in place and enforced to ensure proper labeling and handling?
- How do we know our detective controls are working, and how can we measure their effectiveness? Do we periodically test them with internal assets and external parties to validate their effectiveness?
- Do we have a comprehensive incident response plan involving all stakeholders (human resources, the general counsel, compliance, security, others)? Is there a strong relationship with law enforcement partners for incident response? Are there in-house forensic capabilities, or is an outside firm on retainer?
- Do we have a backup and recovery program? Could we recover our systems and critical data if access was prevented or data corrupted in the main system? Do we have strong controls around our critical vendor relationships?

CASE IN POINT



Insider Threat Steals Personal Data from 1.5 Million Customers of Major Regional Bank

A US regional banking giant announced in early 2018 that personal data of 1.5 million customers may have been stolen by a malicious insider. The company stated that it had become aware of a theft of data by a former employee from some of its contact lists. The insider had been working with a third party to steal company contact lists. The incident resulted in the bank notifying the 1.5 million clients that some information—such as name, address, phone number, and certain account balances—may have been exposed. Personally identifiable information—such as social security numbers, account numbers, PIN, user IDs, passwords, and driver license numbers—were not exposed as a result of the theft. In response to the incident, the bank offered ongoing identity protection free of charge to all current and new customers following the discovery.

Source: Doug Olenick, “Ex-Sun Trust employee helps compromise 1.5 million bank clients,” *SC Magazine*, April 20, 2018.

Tool D – Supply-Chain and Third-Party Risks

By Lisa Humbert, Operational Risk Officer of the Americas, Bank of Tokyo Mitsubishi, MUFG; and Tim McKnight, Chief Security Officer, SAP



OBJECTIVE OF THE TOOL:

Some of the biggest cybersecurity risks that enterprises must manage are their supply chain and third-party relationships. Many data breach incidents are caused by third-party vulnerabilities. As a result, the strength of an organization's cybersecurity often depends on the weakest link in its supply chain, which can directly affect the company's profitability and reputation. This Tool details questions that directors should be asking management to ensure adequate security measures are in place to address supply-chain and other third-party risks.

Below we have provided definitions for both Cyber Supply-Chain Risk Management and Third-Party Risk Management, and considerations for both disciplines. In some industries these functions overlap; however, the activities for each are distinct.

This Tool details questions, with considerations, that directors should be asking management to ensure that adequate security measures are in place to address Cyber Supply-Chain Risk Management and Third-Party Risk Management.

NIST defines cyber supply-chain risk management (C-SCRM) as “the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of [IT] product and service supply chains.”¹

Third-Party Risk Management (TPRM) is the standardized process companies use to monitor and manage risk associated with key partners and vendors.

Questions Directors Can Ask to Assess the Company's Approach to Cyber Supply-Chain Risk Management

1. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks? Here are some items to consider:
 - a. Risk and reward analysis, and accounting for cybersecurity management and Information Technology governance in the Total Cost of Ownership calculation
 - b. Negotiation strategies inclusive of cybersecurity insurance provisions
 - c. Implementation of service-level agreements inclusive of reporting, metrics, and ongoing monitoring requirements

CYBERSECURITY RISK IN THE SUPPLY CHAIN

- Each new supplier adds security vulnerability
- Cyber attackers often target third-parties
- Understanding what suppliers have data, where it is stored, and who has access to it
- Data quality checks and data flow mapping
- Supplier maturity within the FinTech community
- Contract negotiations and terminations
- Employee skill level
- Subcontractors
- Age of contracts
- Internal cybersecurity maturity
- End-to-end process management and oversight

¹ NIST, “Cyber Supply Chain Risk Management” on csrc.nist.gov.

2. What do we need to do to fully include cybersecurity in current supply-chain risk management? Here are some items to consider:
 - a. Training supply-chain personnel to recognize cybersecurity risk and enabling mitigation activities
 - b. Third-party due diligence throughout the proposal, selection, and onboarding processes
 - c. Cybersecurity expertise leveraged during the negotiating and contracting process
3. How are cybersecurity requirements built into contracts and service-level agreements? How are they enforced? Contracts and service-level agreements can be written to include requirements for the following:
 - a. Cybersecurity insurance provisions
 - b. Personnel policies, such as background checks, training, etc.
 - c. Access controls
 - d. Encryption, backup, and recovery policies
 - e. Secondary access to data
 - f. Requirements around the use of subcontractors
 - g. Countries where data will be stored
 - h. Data-security standards and notification requirements for data breaches or other cyber incidents
 - i. Incident-response plans
 - j. Audits of cybersecurity practices and/or regular certifications of compliance
 - k. Participation in testing and contingency activities
 - l. Requirements for timely return/destruction of data at termination

CASE IN POINT



An Impact on the Consumer Experience

A US-based consumer reporting agency suffered a data breach that affected the personally identifiable information of more than 100 million Americans. Hackers penetrated the company's information system using known vulnerabilities in software, which was developed by a third-party software vendor and widely used. An external third party notified the public about vulnerabilities before the breach. The data breach was preventable had the company patched the vulnerability in the third-party software. The company was required to pay a multimillion-dollar data breach settlement.

Source: Lily Hay Newman, "All the Ways Equifax Epicly Bungled Its Breach Response," *Wired*, September 24, 2017.



Major US Retailer Breached by Vulnerability in Third-Party Vendor's Security

A major US retailer suffered a data breach after hackers penetrated a third-party vendor's information systems to steal network credentials. Hackers then stole 70 million shoppers' information. The incident revealed that an organization's cybersecurity is as strong as the weakest link in its supply chain: in this case, a third-party refrigeration and HVAC services vendor.

At the time, the major retailer had passed Payment Card Industry (PCI) standard compliance audits, which highlighted the limits of the compliance approach to cybersecurity. "Just because you pass a PCI audit does not mean that you're secure," warned a security researcher at the time. A chief technology officer commented: "Compliance can give you a false sense of security."

Source: "Target Hackers Broke in Via HVAC Company," *Krebs on Security* (blog), February 14, 2014; John P. Mello Jr., "Target Breach Lesson: PCI Compliance Isn't Enough," *Tech News World*, March 18, 2014.

4. Do our vendor agreements provide adequate controls for legal risks and compliance requirements (e.g., FTC, HIPAA, GDPR, etc.)? Here are some items to consider:
 - a. Access to confidential or proprietary data, personally identifiable information (PII), sensitive personal information (SPI), or handling of personal health information
 - b. Data, used for regulatory, financial, or other internal reporting, provided by a third party
 - c. Third-party compliance with laws, regulations, policies, and regulatory guidance
5. Are we indemnified against security incidents on the part of our suppliers/vendors? Here are some items to consider:
 - a. Breach, incidents, and vulnerabilities
 - b. Limitation of liability
 - c. Intellectual property violations

Questions Directors Can Ask to Assess the Company's Approach to Third-Party Risk Management

1. What will need to be done to fully include cybersecurity in current third-party risk management? Here are some items to consider:
 - a. Initial and ongoing monitoring of third-party compliance and the control environment
 - b. Assessment process and cadence, designed to identify and remediate weaknesses and threats
 - c. Skilled personnel assigned to monitoring and oversight of the third party

CASE IN POINT



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. 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. 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.

Source: Anna Convery-Pelletier, "The Delta Airlines Security Breach: A Case Study in How to Respond to a Data Breach," *Radware* (blog), October 24, 2018.

2. How are we monitoring compliance of operational and legal requirements? Here are some items to consider:
 - a. Reporting and testing
 - b. On-site and remote assessments
 - c. Periodic business reviews with the third party
3. Do we have the right skill set to conduct assessments, testing, and ongoing monitoring of our third-party population? Here are some items to consider:
 - a. Creating a risk-management framework, including defined roles and responsibilities
 - b. Adequate understanding of the products and services provided by the third party
 - c. Understanding of external regulatory guidance and impacts on the third-party products and services
4. How difficult/costly will it be to enhance monitoring of access points in the supplier network? Here are some items to consider:
 - a. Data protection need and availability
 - b. Multilayered assessment of data quality, and inflow/outflow
 - c. Access to supplier network
5. How difficult/costly will it be to establish and maintain a viable cybersecurity program for our third-party risk? Here are some items to consider:
 - a. Technology and infrastructure
 - b. Organizational staffing
 - c. Regular cross-functional stakeholder collaboration to ensure effective access controls

Tool E – Incident Response

By Nasrin Rezai, Global Chief Information and Product Cybersecurity Officer, General Electric; and Greg Montana, Chief Risk Officer, FIS



OBJECTIVE OF THE TOOL:

Since not all incidents can be prevented, response is a critical component of a cybersecurity program. Incident response capability is necessary for rapidly detecting events and incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring business services. This Tool outlines steps boards should take to ensure that their organizations have an effective incident response program.

These are the business capabilities and functions required to support incident response:

- **Governance:** Knowledge of assets and where they reside with appropriate controls, data protection, and regular risk assessment and management
- **Protective Capabilities:** Policies, employee awareness and education, control procedures to validate access, information protection procedures, and continual validation
- **Detection:** 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
- **Recover:** Speedy remediation and after-action improvement

INCIDENT RESPONSE – THE “HOW” MATTERS!

The experiences of some organizations in responding to large-scale breaches have demonstrated that how a company responds to an incident has direct correlation with impacts to its brand reputation and stock valuation.

Major Credit Reporting Agency:

US website vulnerability was exploited by an unattributed threat actor to gain access to files containing approximately 143 million US customers' data.

Financial Impact: \$1.4 Billion USD

Company Response: Came forward four months after the breach occurred. Website for victim communication was nonfunctional in the initial days. Some company management sold stock worth millions of dollars during the time between the company's internal discovery and the public announcement.

Result: Stock price dropped as much as 35 percent in the days, and years, following the incident announcement. Response measures led to supplemental negative press reporting regarding stock sales and victim communication. The company is likely ordered to pay \$650 million USD for the settlement alone, the largest dollar amount known for a data breach settlement.

International Aluminum and Energy Company:

Ransomware targeted an industrial company. Files were encrypted across multiple systems and locations, thus halting some of the company's production.

Financial Impact: ~\$75 million USD

Company Response: Came forward publicly quickly after the breach occurred. Very quickly put incident response plans into action, had good backup and didn't have to pay ransom. It segregated networks to prevent the spread of the infection.

Result: Stock price went up 1.5 percent despite loss of productivity.

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 a speedy path to business service recovery and a timely response to customers and the market.

Questions Boards Should Ask Senior Management on Incident Response

1. Is there an incident playbook with clear definitions of incidents, roles and responsibilities, and escalation processes? Are core business functions such as IT, business, legal, and communication integrated into the response plan? How does it fit into the company's overall crisis and business recovery plan?
2. What are the escalation criteria for notifying senior leadership and the board if necessary? Who has final decision-making authority?
3. Is the organizational resiliency tested around large risk scenarios and exercised through tabletops and common threat simulation?
4. Are there established relationships with the intel community and key regulators? Have information-sharing relationships been established through Information Sharing and Analysis Centers and consortiums and with other companies?

CONTACTING EXTERNAL PARTIES

In addition to external counsel, boards and management teams should consider whether to notify the following:

- Independent forensic investigators
- The company's insurance provider
- The company's external audit firm
- Crisis communications advisors
- Law enforcement agencies (e.g., the Federal Bureau of Investigation, Department of Homeland Security, US Secret Service).
- Regulatory agencies.
- US Computer Emergency Response Team (US-CERT).

Adapted from Jody Westby's post on Forbes.com, "Don't Be a Cyber Target: A Primer for Boards and Senior Management," Jan. 20, 2014.

CASE IN POINT



US-Based Consumer Reporting Agency Loses 145 Million Americans' Records

A US-based consumer reporting agency suffered a data breach that affected the personally identifiable information of 145 million Americans in 2017. Hackers penetrated the company's information system using known vulnerabilities in Apache Struts software, which was developed by a third-party software vendor and widely used. The Department of Homeland Security's US Computer Emergency Readiness Team (US-CERT) notified the public about vulnerabilities before the breach. The data breach was preventable had the company patched the vulnerability in the third-party software. The company was required to pay a \$650 million data breach settlement.

Source: Brian Fung, "Every type of personal data Equifax lost to hackers: 145 million Social Security numbers, 99 million addresses and more," the *Washington Post*, May 8, 2018.

5. Does the organization have notification and mandatory reporting obligations (e.g., in regard to 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)? What are they?
6. What are the criteria and what is the process for disclosing incidents to investors?
7. What can we do to mitigate the losses from an incident?
8. What are the critical, key performance indicators used to measure incident response effectiveness (e.g., time to detect, and time to respond)?
9. What key steps do you follow after a critical incident? What steps do you follow to ensure this type of incident doesn't occur again?

CASE IN POINT



International Aluminum and Renewable Energy Company Responds to a Disaster

On March 18, 2019, an international aluminum and renewable energy company's operations were disrupted by a cyberattack. The company was forced to suspend production at some of its plants due to ransomware.

The company moved quickly to isolate its operations to halt the spread of the ransomware and worked to implement manual operations. The company resisted paying the ransomware and quickly detected the source of the malware. The company focused on transparency, providing regular updates and daily press conferences.

As of July 2019, the attack was expected to cost the company at least \$75 million. However, security experts praised the company for its management of its incident response. A US-based security expert commented, "Transparency and engagement are always appreciated because, fundamentally, we see a lot of the same threats and activity. Sharing and engaging the public can help prevent activity like this from having a similar large-scale impact in the future."

Source: Richard Chirgwin, "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation blitz," *The Register*, January 25, 2018.

RANSOMWARE INCIDENTS AND EXECUTIVE-LEVEL BEST PRACTICES

By Andrew Cotton, Partner and Americas Assurance Cybersecurity Leader, EY

Introduction

Ransomware attacks are an increasingly common type of cyberattack affecting organizations around the world. In the United States, hospitals, school districts, city governments, and companies have been victimized by ransomware, which involves a hacker penetrating and locking the organization's information systems. When this happens, the hacker often demands a virtual currency payment to unlock the system and restore operations. Such an attack can disrupt organizations' operations—often for a period of days.

For Boards exercising cyber-risk oversight, it is important to ensure that executive management has plans and procedures for potential ransomware incidents. This part of Tool E provides best practices to guide executive management on the issue of ransomware.

Executive-Level Best Practices for Ransomware Incidents

According to EY's best practices, an organization's executive should designate an incident commander and command staff to direct and coordinate teams, make decisions, and allocate resources. The following are key responsibilities of the Information Technology, Information Security, and Legal & Communications teams. In addition, the executive should require teams to share information in a centrally managed location and collaborate on tasks.

Information Technology (IT)

- Disconnect Infected machines, power down noninfected machines.
- Identify and evaluate available backups.
- Determine last "clean" images for reimaging:
 - Work with InfoSec to identify period prior to attacker accessing the network.
- Prioritize restoration:
 - Servers (active directory, production systems, email)
 - Business-critical workstations (e.g., payroll, profit centers)
 - General user workstations

- Work with InfoSec to remediate misconfigurations or vulnerabilities that enabled attacker access to the network.

Information Security (InfoSec)

- Identify ransomware variant to
 - determine if the decryption key is publicly available, and
 - collect intelligence on similar ransomware attacks to inform the investigation.
- Conduct forensic investigation to determine
 - the initial infection vector / how the attackers gained access to the network;
 - attacker-accessed systems and activities on the systems; and
 - if data was exfiltrated.
- Scan noninfected machines for evidence of actor activity.
- Work with IT to remediate the misconfigurations or vulnerabilities that enabled attacker access to the network.

Legal & Communications

- Notify company officers and employees of the disruption.
 - Provide guidance on handling infected computers, turning off noninfected computers.
 - Work with IT and InfoSec to communicate alternative methods for business-critical functions (e.g., email, payroll, production).
- Notify business partners / key external parties.
- Prepare a public statement on the disruption.
- Keep company officers, employees, business partners, and the public informed as incident investigation progresses.
- Prepare for regulatory or compliance requirements.

Tool F – Board-Level Cybersecurity Metrics

By John Frazzini, President and CEO, Secure Systems Innovation Corp.; Robert Gardner, Direct Computer Resources; Lou DeSorbo, Chief Security and Risk Officer, Centene Corp.; Geoji Paul, Director Security Risk Management, Centene Corp.; and Nick Corzine, Manager Cyber Risk Computation, Centene Corp.



OBJECTIVE OF THE TOOL:

Modern businesses are increasingly data driven. Boards now routinely use metrics to help inform their strategic and oversight functions on finance, market competition, marketing sales, etc. This Tool describes how metrics can be used to measure the effectiveness of cybersecurity programs and offers advice on how boards can leverage those metrics to conduct oversight of their organization's cybersecurity programs.

Typically, directors rely on management to develop these metrics and present them in a fashion useful to the board's oversight mandate. Cybersecurity is not substantially different in this respect. (See [Guiding Principles for Board-Level Metrics](#) on page 14.)

However, the development of useful cybersecurity metrics has been an evolutionary process. Moreover, with digital technology and underlying systems constantly changing and affecting a growing number of enterprise activities, the type of cybersecurity metrics at both the management and board level need to evolve, as well.

Traditionally, cybersecurity briefings have been relegated to segregated reviews given during a designated portion of a board meeting. However, as discussed in Principle 1 of this Handbook, cybersecurity issues are best addressed when considered as an inherent part of business decisions, such as decisions on strategic partnerships, new products, M&A, etc., and ought to be addressed in the formative stages of these discussions. As a result, different types of metrics may be

QUESTIONS ABOUT STRATEGIC METRICS

Directors should also ask management about strategic metrics related to the company's approach to security and risk. The following are examples of questions to consider:

- What, in quantitative terms, is our risk appetite and how is it measured? (See [Principle 5](#).)
- How do we measure the effectiveness of our cybersecurity program?
- How do we measure our cybersecurity maturity?
- How do we measure the contribution of cyber risk to related enterprise business risks?
- What metrics do we use to measure the security of our third-party suppliers and providers (vendors, partners, clients, etc.)?
- What metrics do we use to track employee awareness and compliance with cybersecurity policy?
- What is internal audit's review plan related to cybersecurity?
- What are the results of the most recent reviews?
- What progress has been made on addressing any findings?
- Is there a plan to engage an external auditor to do an independent assessment of the company's cyber-risk management program?
- How do we track management or other exceptions to organizational cybersecurity requirements?

more appropriate for specific business topics than more generalized cybersecurity metrics, which may be more appropriate for a comprehensive, system-wide review given in the traditional separate board discussion. Relying on these generalized metrics—other than for compliance purposes—can actually create a false sense of security. A 2019 study by Forrester on the issue concluded, “Traditional metrics paint an incomplete picture and can leave companies blind to potential risk.”¹

Ultimately, directors will need to work with members of management to define the cybersecurity information, metrics, and other data that is most relevant to them given the organization’s operating environment—including industry or sector, regulatory requirements, geographic footprint, and so on. Board-level metrics should highlight changes, trends, and patterns over time, show relative performance, and indicate impact. External penetration test companies and third-party experts may be able to provide effective benchmarks within industry sectors. This Tool will outline questions board members should be asking management to ensure proper metrics are being collected on the enterprise’s cyber risk.

Organizations may now measure enterprise cyber-risk contribution (positive and negative) based on the maturity of their overall cybersecurity program. This approach greatly exceeds compliance-related audits (generally more of a Yes/No type of response) by asking “to what extent” has a control been implemented and how effective is it in reducing an organization’s overall cyber-risk posture. An axiom in the cybersecurity industry is that compliance does not equal security, and the simple premise here is that those companies with a higher level of cybersecurity maturity, versus just compliance, will contribute significantly less enterprise cyber risk to the corporation than those that have less maturity.

Two key cyber-risk maturity programs include the existing [Aerospace Industry Association \(AIA\) National Aerospace Standard \(NAS\) 9933 tool](#) and the emerging [USA Department of Defense \(DoD\) Cybersecurity Maturity Model Certification \(CMMC\) program](#). The NAS 9933 tool builds on top of the Center for Internet Security Top 20 Controls families by adding a maturity rating for each control that ranges from level 1 to level 5, as well as by adding two additional control families. The DoD is developing a CMMC program with the intent of assessing DoD supply chain participating companies’ cybersecurity maturity in order to determine if they qualify to work on DoD sensitive but unclassified programs. The CMMC will use a very similar approach to the NAS 9933 model for assessing and rating cybersecurity maturity.

To help strengthen management reporting on cyber security, we have included a select set of board-level metrics in four categories: (1) [strategic metrics](#), (2) operational metrics (below), (3) [economic metrics](#), and (4) [business program/project metrics](#).

OPERATIONAL METRICS

Traditional operational metrics provide relatively little strategic context or information about performance and risk position. However, they can still be helpful in assisting the board in understanding critical compliance issues and stimulating useful discussions about trends, patterns, and root causes, and benchmarking with others in the industry. The following are examples of questions that board members can ask management about operational metrics:

- What operational metrics are we tracking and why?
- How many unpatched vulnerabilities do we have on critical systems and why?
- How many blocked attacks have we addressed in the last quarter?
- How many data incidents (e.g., exposed sensitive data) has the organization experienced in the last reporting period?
- How does our cybersecurity budget compare with others in our industry?
- What security initiatives were proposed and not funded? What were the trade-offs?
- What are the metrics that management uses to compute cyber risk?
- How long does it take for us to discover and address a significant cyber risk?
- What percent of our supply chain failed our cybersecurity assessment?

¹ Forrester Consulting, *Better Security and Business Outcomes With Security Performance Management: Mitigating Risk And Generating Revenue With Metrics That Matter* (September 2019), p. 5.

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. To get started, there are several questions boards should consider asking management:

- What are our quarterly expected loss ratio metrics related to our cyber-risk condition across our various business units and operating environments?
- What is the financial impact related to our cyber-risk worst-case scenario?
- What processes have we established related to making cyber-risk acceptance, cyber-risk remediation, and cyber-risk transfer decisions? How do we measure how these decisions reduce our financial exposure to cyber risk?
- How are we measuring and prioritizing our control-implementation activities and cybersecurity budgets against our financial exposure to cyber risk? Have we connected our control-implementation strategy and cybersecurity programs, including budgets, with our cyber-risk transfer strategy?
- Based on our financial performance targets, how can cyber risk impact our financial performance? What is our annual cyber risk expected loss value?
- What is our cyber-risk remediation plan to achieve our target expected loss tolerance level? Is our plan producing a net-positive financial return?
- How does our cybersecurity program align cyber-risk-based, expected loss ratio analysis and expected loss tolerance targets? How are we measuring, tracking, and demonstrating how our cybersecurity investments are reducing our financial exposure to cyber incidents and delivering cybersecurity return on investment?
- How are we measuring and aligning our cyber-risk-based, expected loss ratio analysis and cybersecurity planning with our cyber insurance risk-transfer plan?
- How do we measure the effectiveness of our organization's cybersecurity program and how it compares to those of other companies?

QUESTIONS ABOUT METRICS RELEVANT TO SPECIFIC BUSINESS PROGRAMS

- Based on the best available data, how likely is it that there will be a cybersecurity incident on this project that would be significant enough to require board involvement?
- Given the most likely, least likely, and average chances of a cybersecurity incident on this project, what would be the anticipated cost in dollars and cents? (Monte Carlo simulations may be helpful in making this determination.)
- What would be the cost of mitigating or transferring this cyber risk down to a level consistent with our risk appetite?
- What are the key factors that are contributing the most to the probability of the risk occurring and the impact of realizing the cyber risk, and what are our strategies to mitigate those factors?

Tool G – Cybersecurity Considerations During M&A Phases—Mergers and Acquisitions

By Jeff Brown, Chief Information Security Officer, Raytheon, and Andrew Cotton, Partner and Americas Assurance Cybersecurity Leader, EY

Introduction

In recent years, new rules and regulations such as the European Union's General Data Protection Regulation and China's Cybersecurity Law, among other data protection regulations and laws globally, are beginning to shine a light on cybersecurity due diligence during mergers and acquisitions. Additionally, recent high-profile breaches have occurred during M&A phases, resulting in massive drops in purchase price and organizations becoming saddled with the selling company's vulnerabilities and breaches. As a result, cybersecurity needs to be a major consideration as companies go through the M&A process. This Tool describes the role cybersecurity plays throughout each phase of the merger and acquisition process.

Risks that organizations should be aware of include these:

- 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 parent company to investigation costs, financial liability, regulatory penalties, or reputational damage.
- Attackers might still be in the acquired company's network, creating a risk of the attacker migrating into the parent company's network.
- The acquired company may be targeted immediately after the announcement, because the presumably less cybersecurity-mature, smaller acquisition target could become a back door into the larger company when their networks are connected.

The consequences of any of these risks being realized can be severe. When discovered prior to the acquisition closing, it could potentially reverse the business case for the deal. When discovered afterward it can saddle the parent company with unexpected costs and liability.

Accordingly, directors should ask management to conduct a cyber-risk assessment for each phase of the transaction's life cycle to confirm systems and processes are secure, and to quantify the risks that may impact the company after the deal closes, including revenues, profits, market value, market share, and brand reputation.

Strategy and Target Identification Phase

The risk of attack starts 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 gossip, a slowdown in a company's release cycle, staff reductions, or data leakage through social media channels. According to published reports, hackers have already targeted law firms, signaling that thieves are scouring the digital landscape for more sophisticated types of information than credit card accounts.¹ Law firms, financial advisers, and other associated firms are attractive to hackers not only because they hold trade secrets and other sensitive information about corporate clients but also because they are privy to details about early-stage deal exploration that could be stolen to inform insider trading or to gain a competitive advantage in deal negotiations.

¹ Dan Packel, "US Law Firm Falls Victim to Alleged Chinese Hacking as Clients Face Threats," *The American Lawyer*, February 20, 2019.

During this phase, management should gain an understanding of cyber risks associated with the target company and model the impact of those risks to compliance posture, financial forecasts, and potential valuations. Management can perform the following analysis even before direct engagement with the target company:

- **Modeling the financial impact of identified cyber risks:** These risks may not only impact a company's return on invested capital, but also result in loss of competitive advantages, costly remediation, fines, and possibly years of litigation, depending on what was stolen. An initial estimate of the impact may be material enough to encourage strategy teams to alter a deal trajectory. The estimate can be refined as the transaction process continues and as risks are mitigated.
- **Understanding 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. Outside the United States, other countries are increasingly implementing their own cybersecurity laws and regulations, which at times can be at odds with the regulations with which the acquiring company has experience. Of particular note, the implementation of the European Union's Global Data Protection Rule (GDPR) with its potentially large penalties represents a new acquisition risk that boards should understand before moving forward with an acquisition involving the data of European individuals.

Due Diligence and Deal Execution Phases

During these phases, cybersecurity due diligence is critical. Significant 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 want to manage 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/assume. Due Diligence teams can identify cyber risks by conducting a tailored cybersecurity assessment:

- Identify insufficient investments in cybersecurity infrastructure, as well as deficiencies in staff resources, policies, etc.
- Identify lax cultural attitudes toward cyber risk.
- Determine cybersecurity-related terms and conditions (or the lack thereof) in customer and supplier contracts that have a potential financial impact or result in litigation for noncompliance.
- Discover noncompliance with cybersecurity-related data privacy laws or other applicable regulations and requirements.
- Identify recent data breaches or other cybersecurity incidents.

Ideally, the acquiring company would assess these risks through an on-site assessment, especially when the target is a small company where underspending on IT and cybersecurity is more likely. Such an 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.

The output of the assessment would be a very rough estimate of the cost of bringing the target up to standards (which might affect the business case) and an assessment of whether or not the target's intellectual property is already publicly available or in the hands of competitors. Where there has been a recent breach, the assessment should also reveal if the target has made sufficient improvement to prevent 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 able to interview key security personnel who are not aware of the potential acquisition.

Acquirers should fully understand the target company's requirement for domestic and global compliance and reporting. Depending on the industry and the target company locations, the regulatory environment of the target company could be very different than that of the acquirer. 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 conduct "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' radar, 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 which 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.

Effective due diligence on cybersecurity issues demonstrates to investors, regulators, and other stakeholders that management is actively seeking to protect the value and strategic drivers of the transaction, and that they are aiming to lower the risk of a cyberattack before integration. These risks can then be factored into the initial price paid and into performance improvement investments, enabling a robust transaction proposal to be presented to shareholders for approval.

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.² Moreover, global requirements should also be considered during the acquisition process. Requirements in the European Union's General Data Protection Regulation might affect what sensitive information can be shared between potential buyers and the seller company.³

Integration Phase

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 1, they become a target for social engineering attacks by those seeking to use the small company 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. Thus, the sooner the parent company can integrate the target company into their security environment, the better.

Many of these integration activities are complex and could take a year or more to complete. Integration teams need to have the cyber expertise to address the smallest of details to identify and mitigate cyber risks, including these:

- 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, boards should pay particular attention to integration projects slipping to the right 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 1 integration plan to extend as much of the parent company's cyber protections as possible to the target company immediately. At a minimum, the plan should include these steps:

- An exchange of threat information to include Internet domains to be blocked
- Employee awareness training emphasizing the risk of phishing attacks mimicking emails from the new parent company
- 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

Boards should also note the special case where only a portion of a company is being acquired. In this case, the target's parent company will certainly be less willing to accept what they see as intrusive assessments, either pre- or post-closing. Furthermore, the need to decouple the target from the parent company's infrastructure could delay the target's integration into your security infrastructure by a year or more. Together, these two factors mean that the acquiring company's ability to detect and mitigate cyber risk is greatly reduced.

² "Key Takeaways from the SEC's 2018 Cybersecurity Guidance," *Kirkland Alert*, Kirkland & Ellis, February 28, 2018.

³ "Due Diligence and GDPR: How to stay compliant during a transaction," *Visma Admin Control*, February 9, 2018.

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 itself, and should vigilantly maintain their cybersecurity efforts. Applying this two-pronged approach during M&A will serve to ultimately protect stakeholder value.

CASE IN POINT



Global Web-Services Provider Breach Lowers Offering Price by \$350 Million

In December 2014, a global web-services provider learned that Russian hackers had breached the company's information systems and gained access to 500 million users' account information. While the company's senior management learned of the breach and was briefed on internal investigations, the company did not disclose the breach until September 2016 when it was in negotiations to sell its business to a telecommunications company. The web-services provider later disclosed a 2013 breach affecting 1 billion users' accounts. The company faced large fines and a class-action settlement. The purchasing company lowered its offering price by \$350 million after the breach was announced.

An internal review submitted to the company's board found that "the 2014 Security Incident was not properly investigated and analyzed at the time, and the Company was not adequately advised with respect to the legal and business risks associated with the 2014 Security Incident." A *National Law Review* analysis concluded: "The failures of [the company's] senior executives illustrate precisely why the board of directors now must play a critical role not just in proactive cybersecurity, but in overseeing the response to any major cyber incident."

Source: Edward J. McAndrew, "The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far)," *National Law Review*, May 11, 2018; Anjali Athavaley and David Shepardson, "Verizon, Yahoo agree to lowered \$4.48 billion deal following cyber attacks," Reuters, February 21, 2017.



Health-Care Companies Implement System to Secure Acquired Company Assets

During an acquisition in 2018, a major health-care provider was concerned about the risk of a cybersecurity breach via the acquired practice's computer systems. During the acquisition process, the company searched for a way to securely connect the networks of newly acquired doctors' practices to their own networks. To accomplish this, the company created an appliance between their networks and those of the practices being acquired. This tool allowed the company to detect threats and suspicious behavior and protect their network from any vulnerabilities stemming from the acquired company's systems.

Source: Bricata, "Cybersecurity Case Study: Securely Integrating a Business Network After a Merger and Acquisition," Security Boulevard, September 3, 2019.

Tool H – Sample Dashboards

By J. R. Williamson, Chief Information Security Officer, Leidos

Cybersecurity Performance Dashboard

This dashboard demonstrates maturity of an organization’s cyber-risk management across different domains throughout the organization. Boards can use dashboards like these to better understand where the organization’s cyber-risk management is more mature and where it is less mature. It can also visualize goals for where the organization wants to make improvements.

DOMAIN	PERFORMANCE	HIGHLIGHTS
Leadership and Governance	 0 1 2 3 4	<ul style="list-style-type: none"> • Continuous monitoring by PMO • Initial policies ready for review by policy review committee • Information Security Steering Committee meeting monthly
Human Factors	 0 1 2 3 4	<ul style="list-style-type: none"> • Kick off video filmed with CEO in support of cyber awareness and training • Scheduled air date end of July, followed by planned activities for cyber awareness and training, globally • Initial phishing campaign completed for baseline; global phishing campaign underway
Information Risk Management	 0 1 2 3 4	<ul style="list-style-type: none"> • SAP Governance, Risk, and Compliance (GRC) project has redesigned and deployed new roles and processes for Information Technology (IT); business roles and processes currently in design • Proof of concept for vendor risk assessment process successful; process automation in early stages • Application security assessment program started
Business Continuity and Crisis Management	 0 1 2 3 4	<ul style="list-style-type: none"> • Multiday/cross-functional mock incident exercise completed with Incident Response, executive management and operational teams • Information Security response plans completed • Additional Information Security playbooks being completed
Operations and Technology	 0 1 2 3 4	<ul style="list-style-type: none"> • Redesign of identity access management platform completed with project plan revised • Q1 2017 Financially Significant Application (FSA) access certification completed successfully
Legal and Compliance	 0 1 2 3 4	<ul style="list-style-type: none"> • Legal is working on compliance with new European Global Data Privacy Regulations (GDPR) • PCI Self Assessment Questionnaire (SAQ) filings on track for July 31 due date • Sarbanes-Oxley (SOX) Q2 '17 management testing is 100% complete

Key Risk Indicator Scorecard

A key risk indicator (KRI) scorecard can be used to succinctly display major risks to the organization across domains, what the status is in managing that risk, and what is being done to correct any gaps that exists across key risks. Boards can use these tools to understand where management needs to be focusing its efforts on cybersecurity improvements.

Illustrative Example

Cybersecurity Scorecard/Sample KRI Scorecard				
RISK DOMAIN	KEY RISK INDICATOR	STATUS	CHANGE	NOTES
Crown Jewels	Confidence in critical asset inventories	!	↑	Asset management system being built
Program Maturity	NIST maturity vs. target milestones	✘	▬	NIST assessment is complete
Risk Management	Volume, rate & severity of risk escalations	!	▬	ERM structures are not in place
People & Culture	% of key positions filled with successor identified	!	↓	New positions created but still unfilled
Resources	Changes in risk assessment tied to risk & security investments	✓	↑	Significant spending on cyber continues
Incident Readiness	Frequency & outcome of response exercises	!	▬	No exercises in this period
Legal & Regulatory Compliance	Quality & quantity of interaction with regulators	✓	↑	Significant spending on compliance
Third Party & Cloud	Proportion of third parties with access to critical assets	✘	↓	New policies implemented but not yet applied to vendors
External Landscape	Frequency and impact of attacks on industry peers	!	▬	No observed change
Industry Collaboration	Changes in frequency and quality of collaboration with peers	✓	↑	Intimate collaboration with third-party experts

 Acceptable
  Near tolerance
  Outside of tolerance
  Favorable
  Neutral/No change
  Unfavorable

Key Information Security Metrics Dashboard

Key information security metrics dashboards may be used to evaluate the organization’s performance in responding to and remediating cybersecurity incidents. These metrics can be used to understand how long it takes the organization to discover and remediate risks, and what progress is being made through organizational initiatives such as awareness trainings and hardware and software upgrades.

Illustrative Example

Key Information Security Metrics					
		STATUS	TARGET	TREND	NOTES
Key Incident Dwell Time	Average time to discover key security incidents. Time from exploit to discovery.	X Days	Y Days		Does not include daily virus detection and remediation Mandiant 2017 report 35 days for internal in Americas
Extreme Risk Device Remediation	Extreme risk devices remediated to plan (7 days) for urgent and high vulnerabilities	XX%	XX%		ERD are highest value servers based on use and data - 17% of population
Obsolete Operating Systems	Percent servers with obsolete OS in the environment	X%	X%		Replacement of legacy applications will allow for elimination of supporting servers
Phishing Click Rate	Percentage of users that click on phishing campaign emails sent by the security operations team	XX.X%	XX.X%		Industry average 19-20%
Security Awareness Training	Percentage of workforce that completed annual security training	XX%	XX%		First year including non-company workers Employee-only 98%.
Ticket Closure Time	Average time per month taken to close tickets from Security Operations Center	X Days	Y Days		Identified by 24/7 operations center to be investigated by internal team

All targets are for FYxx, and consider changes in scope, volume, and complexity of each area.

 Up  Flat  New  Down

Tool I – Building a Relationship With the CISO

By Jeff Brown, Chief Information Security Officer, Raytheon

Introduction

As corporate information-security functions mature, corporate directors must ask themselves how they can effectively communicate with the security executive. The individual occupying the position manages vast numbers of operational, reputational, and monetary risks. The development of a close and candid relationship between the board and the CISO is increasingly important for effective cyber-risk oversight. Accordingly, many board members now seek to establish an ongoing relationship with the CISO through full-board and committee meetings, but also outside the board room. This Tool offers guidance on how boards can more effectively establish a relationship with their organization's CISO and security team.

At NACD's inaugural global Cyber Summit in 2015, more than 200 directors from Fortune Global 500 companies and cybersecurity experts discussed the evolving role of the CISO, including the potential for this individual to serve as a critical source of information and insight for the board. As one director observed, "A strong cybersecurity program allows our business to compete and flourish. A CISO with the right skills can be a tremendous asset, including as an informed set of eyes and ears for directors, but at too many companies they are still viewed as tactical support for the CIO."¹

This Tool will provide a guide for directors to establish or enhance relationships with the CISO and security team. The questions and guidelines below can assist directors in establishing or enhancing a relationship with the CISO and, consequently, assist them in gaining a better understanding of the company's overall approach to cybersecurity. Because not every question will have relevance for every company, directors should select those most appropriate to the issues and circumstances at hand.

Understand the CISO's Role and Mandate

- What is the CISO's 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?²
- To whom does the CISO report? There is no clear industry consensus on this topic. By far, the largest percentage report to the CIO although there is a growing feeling (echoed earlier in this publication) 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 and security. That is weighed against the value of having the CISO's supervisor able to understand the technology and risks and capable of arbitrating trade-offs without escalating the issue to the CEO. Regardless of which option carries the day in the long term, the deciding factor is not to whom the CISO reports, but whether or not that person has a strong voice on the executive team to advocate 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? Comparing this figure with industry spending trends is probably the best way to gain context over the adequacy of funding. What is its size (e.g., percentage of total IT spending), and how does this figure compare with leading practice in a company's particular industry and generally?
- How much of the security infrastructure is outside of the budget or directive authority of the 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 these budget trade-offs internally in real time, the more rapid the response and the lower the risk.
- 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 (i.e., what difficult budget decisions they had to make that resulted in risk acceptance). A conversation about what fell below the cut line and what decision process was used to evaluate trade-offs will always be illuminating.

¹ Quotation is from a participant in the Global Cyber Summit, held April 15–16, 2015, in Washington, DC. Discussions were conducted under the Chatham House Rule.

² See, for example, Marc van Zadelhoff, Kristin Lovejoy, and David Jarvis, *Fortifying for the Future: Insights from the 2014 IBM Chief Information Security Officer Assessment* (Armonk, NY: IBM Center for Applied Insights, 2014).

- What role does the CISO play in the organization’s enterprise risk management (ERM) structure and in the implementation of ERM processes?
- What role, if any, does the CISO play beyond setting and enforcing cybersecurity policies on the enterprise network and related control systems?
- Does the CISO provide input on the development process for new products, services, and systems or on the design of partnership and alliance agreements, etc., such that cybersecurity is “built in” rather than “added on” after the fact?
- Does the CISO have a role in evaluating the cyber risk of acquisitions during due diligence?

Spend Time With the Cybersecurity Team Outside of the Board Room

With packed board meeting agendas, it is probably 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.

- Directors can also ask the security executive for an assessment of their personal cybersecurity posture, including the security of their devices, home networks, etc. These discussions are not only informative for individual directors, but also will help safeguard the volumes of confidential information board members receive in the course of their service.
- Many security teams routinely produce internal reports for management and senior leadership on cyberattack trends and incidents. Directors can discuss with the CISO, corporate secretary, and board leaders whether this information might be relevant and useful to include in board materials.
- Gain insight into the CISO’s relationship network.

Inside the Organization

- How does the CISO or the information-security team collaborate with other departments and corporate functions on cybersecurity-related matters? For example, does the CISO coordinate with
 - business development regarding due diligence on acquisition targets and partnership agreements;
 - internal audit regarding the evaluation and testing of control systems and policies;
 - human resources on employee training and access protocols;
 - 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?

The CISO should be able to articulate how cybersecurity isn’t just a technology problem; it’s about paving the way for the company to implement its strategy as securely as possible.

- What support does the CISO receive from the CEO, CIO, and senior management team?

EXECUTIVES REPORTING TO THE BOARD ON CYBERSECURITY (PERCENTAGE OF BOARDS)

In addition to external counsel, boards and management teams should consider whether to notify the following:

- | | |
|---|---|
| • Chief Executive Officer 56% | • Chief Technology Officer 29% |
| • Chief Information Officer 53% | • Business Unit Leaders 15% |
| • Chief Information Security Officer 45% | • Chief Human Resources Officer 4% |
| • General Counsel 39% | • Unsure 1% |
| • Chief Audit Executive 32% | • Other 13% |

Source: 2019–2020 NACD Public Company Governance Survey

Outside the Organization

- Does the CISO or the information security team participate in cybersecurity information-sharing initiatives (e.g., industry-focused, IT-community-focused, or public-private partnerships)? How is the information that is gathered from participation in such initiatives used and shared within the organization?
- Does the CISO (or the information security team) have relationships with public-sector stakeholders such as law enforcement agencies (e.g., FBI, INTERPOL, US Secret Service), regulatory agencies' cybersecurity divisions, the US Computer Emergency Response Team (US-CERT), etc.?

Inside and Outside the Organization

- How does the CISO or the information security team develop and maintain knowledge of the organization's strategic objectives, business model, and operating activities?
 - For example, in companies that are actively pursuing a "big-data" strategy to improve customer and product analytics, to what extent does the CISO understand the strategy and contribute to its secure execution?
 - What continuing education activities are undertaken by the CISO or the information security team in order to remain current in cybersecurity matters?

Assess Performance

- How is the CISO's performance evaluated? How is the information security team's performance evaluated? Who performs these evaluations, and what metrics are used?
- What cybersecurity performance measures and milestones have been established for the organization as a whole? Do we use a risk-based approach that ensures the highest level of protection for the organization's most valuable and critical assets?
- To what extent are cyber-risk assessment and management activities integrated into the organization's enterprise-wide risk-management processes? Are we using the frameworks from the National Institute of Standards and Technology (NIST), the International Organization for Standardization (ISO), or other similar frameworks to assess cybersecurity hygiene from an organization-wide perspective?

Engage the CISO in Discussion About the "State of the Organization"

- What was the organization's most significant cybersecurity incident during the past quarter? How was it discovered? What was our response? How did the speed of detection and recovery compare with that of previous incidents? What lessons did we learn, and how are these factored into the organization's continuous improvement efforts?
- Where have we made the most progress on cybersecurity in the past six 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?
- What organizations or locations have been exempted from one or more cybersecurity controls for business reasons? For example, critical applications only patching during quarterly maintenance windows, research organizations bypassing Internet filtering, or factories not being scanned. Such exceptions to policy and controls increase the overall risk to the company. Regardless of whether such exceptions are valid, management and the board need to be aware of the scope of the risk.

THE NEEDS OF CHIEF INFORMATION SECURITY OFFICERS

Chief information security officers (CISOs) need some attention and recognition, too. The CISO and the security team are among the most high-stress positions in the firm. They have a fairly constant expectation of being needed 24/7/365. Too often, they do not receive adequate internal support and are blamed when there are system failures that they did not

cause (sometimes being the victims of attacks from the Chinese military—literally). High turnover and low morale of the security team can lead to lower efficiency and increased risk. Personal wellness for the security team (adequate staffing, schedules, time off, and occasionally gratitude) is a pragmatic element of an overall management and security program.

Tool J – Enhancing Cybersecurity Oversight Disclosures—10 Questions for Boards¹

By Robyn Bew, Center for Board Matters, EY

Introduction

Cybersecurity attacks are among the gravest risks that businesses face today. EY's 2019 CEO Imperative Survey found that CEOs ranked national and corporate cybersecurity as the top global challenge to business growth and the global economy. As discussed in Principle 2, directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances, including potential requirements related to disclosures. This Tool offers 10 questions that boards can ask to enhance cybersecurity disclosures within their organization.

In this environment, stakeholders want to better understand how companies are preparing for and responding to cybersecurity incidents. They also want to understand how boards are overseeing these critical risk-management efforts. EY's annual Center for Board Matters investor outreach includes conversations with governance specialists from more than 60 institutional investors representing more than US \$32 trillion in assets under management. Sixty-one percent of respondents said cybersecurity, regardless of sector, was among those elevated risk issues, even though investors characterize cyber risk as a pervasive and standard risk impacting all companies. Some of the key themes arising from those conversations were these:

- an interest in understanding how boards are structuring oversight (i.e., is a committee or the full board charged with that responsibility)
- how directors are developing competence around and staying up-to-speed on cyber issues
- how often and who from management is reporting to the board
- key features of how management is addressing cyber risk
- many investors also expressed interest in data-privacy issues and compliance with new privacy laws and regulations

In response, many companies are enhancing their cybersecurity disclosures, with the most significant changes related to board oversight practices. (See [Figure 1](#).)

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 as they relate to cybersecurity, data privacy, and other key risk and strategy issues?
2. What feedback has the management team and/or Investor Relations received from our major investors? What questions are our investors 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? Specifically:
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?
6. Is cybersecurity included in the areas of expertise that we consider important on the board, and/or does it appear in one or more directors' biographies?

¹ Content adapted from *What Companies are sharing about cybersecurity risk and oversight* (EY, 2019).

7. Do we describe how the board and/or key committees receive information from management about cybersecurity matters?
8. Is cybersecurity included in the company's list of risk factors?
9. How do we describe cybersecurity-risk management activities, such as 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 cybersecurity-related disclosures compare to those of our competitors and industry peers?

The following data is from an analysis of cybersecurity-related disclosures in the proxy statements and annual reports on Form 10-K of the 82 companies on the 2019 Fortune 100 list that filed those documents in both 2018 and 2019 through September 5, 2019. The analysis was based on cybersecurity-related disclosures on the following topics:

- Board oversight, including risk-oversight approach, board-level committee oversight, and director skills and expertise
- Statements on cybersecurity risk
- Risk management, including cybersecurity-risk management efforts, education and training, engagement with outside security experts, and use of an external advisor

FIGURE 1. FORTUNE 100 COMPANY CYBERSECURITY DISCLOSURES, 2018-2019				
CATEGORY	TOPIC	DISCLOSURE	2018	2019
Board oversight	Risk-oversight approach	Disclosed a focus on cybersecurity in the risk-oversight section of the proxy statement	80%	89%
	Board-level committee oversight*	Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters	78%	84%
		Disclosed that the audit committee oversees cybersecurity matters	62%	65%
		Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	21%	28%
	Director skills and expertise	Cybersecurity included among areas of expertise sought on the board and/or cited in at least one director biography	40%	54%
		Cybersecurity included among the areas of expertise sought on the board	23%	32%
		Cybersecurity cited in at least one director biography	30%	40%
	Management reporting structure	Provided insights into management's reporting to the board and/or committee(s) overseeing cybersecurity matters	52%	54%
		Identified at least one "point person" (e.g., the Chief Information Security Officer or Chief Information Officer)	26%	33%
	Management reporting frequency	Included language on frequency of management reporting to the board or committee(s), but most of this language was vague	39%	43%
Disclosed reporting frequency of at least annually or quarterly; remaining companies used terms like "regularly" or "periodically"		12%	16%	
Statement on cybersecurity risk	Risk-factor disclosure	Included cybersecurity as a risk-factor consideration	100%	100%
Risk management	Cybersecurity-risk management efforts	Referenced efforts to mitigate cybersecurity risk, such as the establishment of processes, procedures, and systems	82%	89%
		Referenced response planning, disaster recovery, or business continuity considerations	49%	55%
		Stated that preparedness includes simulations, table-top exercises, response readiness tests, or independent assessments	9%	9%
	Education and training	Disclosed use of education and training efforts to mitigate cybersecurity risk	18%	26%
	Engagement with outside security community	Disclosed collaborating with peers, industry groups, or policymakers	6%	11%
	Use of external advisor	Disclosed use of an external independent advisor	13%	%

Percentages based on total disclosures for companies. Data based on the 82 companies on the 2019 Fortune 100 list that filed Form 10-K filings and proxy statements in both 2018 and 2019 through September 5, 2019.

*Some companies designate cybersecurity oversight to more than one board-level committee.

Source: EY, [Fortune 100 company cybersecurity disclosures 2018-19](#).

Tool K – Personal Cybersecurity for Board Members

By Melissa Hathaway, President, Hathaway Global Strategies

Introduction

While organizational cybersecurity is incredibly important, it is also critical that board members take precautions to ensure that they are engaging in proper cybersecurity practices and protecting their devices and their privacy. This Tool outlines 10 recommendations for board members to improve their own cybersecurity.

1. **Ensure all of your devices have up-to-date software.** It is essential to keep your devices and applications updated to the most current software available.
2. **Lock your WiFi, like you lock your house.** Establish a new password beyond the factory setting. Establish a guest account for houseguests, contractors, etc.
3. **Backup your data often—at least once per month.** Engage an encrypted backup service to protect yourself from ransomware.
4. **Think before you post; minimize your digital exposure.** Do not share anything that would give criminals information about your current or future whereabouts. Lock down your social media accounts by restricting your posts to friends. Regularly review and implement privacy and security settings.
5. **Switch on two-factor authentication for everything.** Use biometrics wherever possible.
6. **Use complex passwords for sensitive accounts.** Use (for example) your iPhone's keychain to secure your passwords. Use the recommended secure passwords.
7. **Dedicate a computer/device (that your children cannot use) to conduct any sensitive and financial transactions.**
8. **Conduct a regular, exhaustive search about what is out there concerning you and your family.**
9. **Dispose of electronic devices securely; wipe or safely destroy the device.**
10. **Freeze your credit.** A credit security freeze is an effective tool against financial identity theft, giving you maximum control over who has access to your credit.

Tool L – Department of Homeland Security Cybersecurity Resources

Cybersecurity and Infrastructure Security Agency – Cybersecurity Resources

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important mission for the US Department of Homeland Security and the nation. So much so that Congress established the Cybersecurity and Infrastructure Security Agency (CISA) in 2018 as part of the Cybersecurity and Infrastructure Security Agency Act.

As the nation's risk advisor, CISA works with partners at the federal, state, local, and private-sector level to defend against today's threats and build more secure and resilient infrastructure for the future. CISA's unique and comprehensive understanding of cyber threats and the risk environment as well as the needs identified by its stakeholders drives the programs and services it provides.

CISA offers a number of comprehensive resources to help organizations improve their cybersecurity resilience.

Cybersecurity Services

National Cybersecurity & Communications Integration Center (NCCIC). CISA coordinates and leads national cyber incident response and manages the response to federal cyber threats through a 24-hour cyber awareness, response, and management center. CISA works closely with public, private-sector, and international partners, offering technical assistance, information security, and education to defend federal networks, help the private sector to defend their networks, and raise awareness of current cyber and communications threats. Learn more at <https://www.cisa.gov/national-cybersecurity-communications-integration-center>.

National Cyber Awareness System (NCAS). CISA publishes information on cyber threats, tips, and advisories through the NCAS subscription service. Products through this system offer a variety of information for users with varied technical expertise. Learn more at <https://www.us-cert.gov/ncas>.

Hunt and Incident Response Teams (HIRT). CISA provides free, on-site assistance to organizations needing immediate investigation and resolution of cyberattacks. CISA members of HIRT can perform a preliminary diagnosis to determine the extent of compromise from a cyber incident. At the customer's request, a team will visit the organization to review networks, identify infected systems, and collect data for follow-on analysis. HIRT provides mitigation strategies, helps restore service, and provides recommendations to improve overall network and control-systems security. Learn more at <https://www.cisa.gov/national-cybersecurity-communications-integration-center>.

Industrial Control Systems (ICS) Support. CISA partners with and serves the industrial control systems community to reduce risk to these unique, potentially high-risk systems. Industrial control systems are defined as the devices, systems, networks, and controls used to operate and/or automate industrial processes. CISA plays a critical role by coordinating efforts among government and control-system owners, operators, and vendors on vulnerabilities, threats, and risks. CISA leads the ICS Joint Working Group (ICSJWG) to facilitate information sharing and reduce the risk to the nation's industrial control systems. Learn more at <https://www.us-cert.gov/ics/Industrial-Control-Systems-Joint-Working-Group-ICSJWG>.

Malware Analysis and Response. CISA collects, analyzes, and exchanges malware information 24 hours a day. Participants can submit malware artifacts (tools, malicious code, other attack technology, or indications like access statistics indicating a possible denial-of-service attack) electronically to CISA. Learn more at <https://www.cisa.gov/reporting-cyber-incidents>.

CISA's Enhanced Cybersecurity Services (ECS) program provides near real-time intrusion prevention and analysis to help US-based companies and state and local governments protect systems against unauthorized access, exploitation, and data theft. ECS shares sensitive and classified cyber threat information with accredited Commercial Internet Service Providers who then block malicious traffic from customer networks. ECS does not replace but augments an organization's existing cybersecurity resources by providing an additional layer of defense against known or suspected cyber threats, while also providing early detection of potential compromise. Learn more at <https://www.cisa.gov/enhanced-cybersecurity-services-ecs>.

Information Sharing

Sharing threat information is critical to prepare for and prevent both cyber and physical attacks. CISA consolidates and shares threat and compromise information; adversary tactics, techniques, and procedures; best practices and recommendations for cybersecurity improvements; and other critical information with stakeholders and partners.

Protected Critical Infrastructure Information (PCII) Program. The PCII Program protects private-sector information which is voluntarily shared with the government for homeland security purposes. The Department of Homeland Security has established processes for the secure receipt, validation, handling, storage, marking, and use of voluntarily submitted information. PCII is protected from disclosure under

- the Freedom of Information Act (FOIA);
- state local, tribal, and territorial disclosure laws;
- use in regulatory actions; and
- use in civil litigation.

The PCII program provides homeland security partners confidence that sharing their information with the government will not expose sensitive or proprietary data. Learn more at <https://www.cisa.gov/pcii-program>.

Automated Indicator Sharing (AIS). AIS enables instantaneous exchange of cyber threat indicators between the federal government and the private sector. AIS lets a company or federal agency share cyber-threat indicators in near real time in a confidential and secure format, helping protect others from the threat. Attackers are therefore able to use a particular attack only once, increasing their costs and reducing the prevalence of cyberattacks. Learn more at <https://www.cisa.gov/automated-indicator-sharing-ais>.

Information Sharing and Analysis Organizations (ISAOs). ISAOs provide information sharing activities among communities of interest, such as businesses across critical infrastructure sectors. Like Information Sharing and Analysis Centers (ISACS), ISAOs collect, analyze, and share cyber-threat information with their stakeholders. Learn more at <https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos>.

Information Sharing and Analysis Centers (ISACs). ISACs are formed by owners and operators in each critical infrastructure sector to help protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs collect, analyze, and disseminate threat information and provide members tools to mitigate risks and enhance resiliency. Learn more at <https://www.nationalisacs.org/>.

Cybersecurity Training

Industrial Control Systems (ICS) Training. CISA offers free ICS Training online through the ICS-CERT Virtual Learning Portal, and via Instructor-Led Training. Learn more at <https://www.us-cert.gov/training>.

Other Tools And Resources

Cyber Essentials. CISA has developed the Cyber Essentials campaign for small businesses and government agencies to understand and address their cybersecurity risk. Cyber Essentials aims to equip smaller organizations that historically have not been a part of the national dialogue on cybersecurity with basic steps and resources to improve their cybersecurity. Learn more at <https://www.cisa.gov/publication/cisa-cyber-essentials>.

CISA Insights. CISA Insights are informed by US cyber intelligence and real-world events. The publication provides background information on particular cyber threats and the vulnerabilities they exploit, as well as a ready-made set of mitigation activities that non-federal partners can implement. Learn more at <https://www.cisa.gov/insights>.

Regional Outreach. CISA has 10 regional offices across the country to improve the delivery of the agency's services to critical infrastructure owners and operators and state, local, tribal, and territorial partners. Each regional office includes experts in every CISA focus area, including in cybersecurity. CISA's regional structure ensures that all stakeholders have direct access to resources in their own backyard. Learn more at <https://www.cisa.gov/cisa-regional-offices>.

Reporting

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. To report, visit <https://www.us-cert.gov/report> or call (888)-282-0870 or email ncciccustomerservice@hq.dhs.gov.

Tool M – Department of Justice and Federal Bureau of Investigation— Responding to a Cyber Incident

What Are the Benefits of Reporting a Cyber Incident to the FBI?

The benefits of reporting a cyber incident to the FBI are more evident today than ever. 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 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 who 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 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 or take down botnets that have hijacked millions of innocent computers worldwide. These unique DOJ and FBI 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 intrusion to the FBI often enables investigators to make connections among related incidents.
 - This enables FBI to share valuable insights and information with companies 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 develop a relationship with their local FBI field office prior to an incident. Proactively building a relationship with the FBI provides companies with a dedicated FBI 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:

- Logs for the affected machines
- A timeline of events
- The identity of whoever reported the incident
- The identity of the victim of the incident
- The nature of the incident
- When the incident was initially detected
- How the incident was initially detected
- The actions that have already been taken
- Who has been notified

How Will the FBI Protect my Organization's Interests and Information?

Federal law enforcement agencies investigating cyber incidents seek first and foremost to 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
 - NCIJTF CyWatch 24/7 Cyber Center: 1-855-292-3937 or cywatch@ic.fbi.gov

Where Can I Find Out More?

- InfraGard: <https://www.infragard.org/>
 - InfraGard is an association of persons 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.

