Cyber-Risk Oversight

DIRECTOR'S HANDBOOK SERIES

NACD®
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Cyber-Risk Oversight

DIRECTOR'S HANDBOOK SERIES

Prepared by Larry Clinton
President & CEO, Internet Security Alliance

NACD®
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Acknowledgements

ISA thanks Robyn Bew of NACD for her role in stewarding the creation of this handbook. We also wish to thank the following individuals for their contributions (in alphabetical order by organization): Cherie Dawson, Tracie Grella, Chuck Jainchill, and Garin Pace, AIG; Daniel Crisp, BNYMellon; Dr. Robert Zandoli, Bunge Limited; Tim McNulty, Carnegie Mellon University; Dustin Wilcox, Centene; Cynthia Fornelli and Catherine Nance, Center for Audit Quality; Joe Buonomo and Bob Gardner, Direct Computer Resources Inc.; Jim Halpert, Nate McKitterick, and Tara Swaminatha, DLA Piper; Andrew Cotton and Sali Osman, Ernst & Young; Nasrin Rezai, General Electric; Eric Goldstein, Alexandra Mace, and Andy Ozment, Department of Homeland Security; David Perera, Internet Security Alliance; Leonard Bailey, Lionel Kennedy, and Christine Kringer, Department of Justice; Jim Connelly, Lockheed Martin; Brian Raymond, National Association of Manufacturers; J. R. Williamson, Northrop Grumman; Jeff Brown, Raytheon; Janet Bishop-Levesque and Mike Brown, RSA; David Estlick, Starbucks; Matt Fleming and Larry Trittschuh, Synchrony Financial; Tim McKnight, Thomson Reuters; Gary McAlum, USAA; Scott DePasquale, Utilidata; and Richard Spearman, Vodafone.

National Association of Corporate Directors

CHIEF EXECUTIVE OFFICER **Kenneth Daly**
PRESIDENT **Peter R. Gleason**
DIRECTOR OF RESEARCH **Friso van der Oord**
DIRECTOR OF STRATEGIC CONTENT DEVELOPMENT **Robyn Bew**
RESEARCH MANAGER **Ashley Marchand Orme**
SENIOR RESEARCH ANALYST **Ted Sikora**
RESEARCH ANALYST **Corey Albright**
RESEARCH ANALYST **Katherine W. Keally**
COPY EDITOR **Margaret Suslick**
ART DIRECTOR **Patricia W. Smith**
GRAPHIC DESIGNER **Alex Nguyen**
WEB CONTENT MANAGER **Cecelia Larsen**

Table of Contents

Introduction

In the past 25 years, the nature of corporate asset value has changed significantly, shifting away from the physical and toward the virtual. Close to 90 percent of the total value of the Fortune 500 now consists of intellectual property (IP) and other intangibles.[1] Along with the rapidly expanding "digitization" of corporate assets, there has been a corresponding digitization of corporate risk. Accordingly, policy makers, regulators, shareholders, and the public are more attuned to corporate cybersecurity risks than ever before. Organizations are at risk from the loss of IP and trading algorithms, destroyed or altered data, declining public confidence, disruption to critical infrastructure, and evolving regulatory sanctions. Each of these risks can adversely affect competitive positioning, stock price, and shareholder value.

Leading companies view cyber risks in the same way they do other critical risks—in terms of a risk-reward trade-off. This is especially challenging in the cyber arena for two reasons. First, the complexity of cyber threats has grown dramatically. Corporations now face increasingly sophisticated events that outstrip traditional defenses. As the complexity of these attacks increases, so does the risk they pose to corporations. The potential effects of a data breach are expanding well beyond information loss or disruption. Cyberattacks can have a severe impact on an organization's reputation and brand, which may be affected more by tangential factors like timing or publicity than the actual loss of data. Companies and directors may also incur legal risk resulting from cyberattacks. At the same time, the motivation to deploy new and emerging technologies in order to lower costs, improve customer service, and drive innovation is stronger than ever. These competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the board level is essential. As a result, managing and mitigating the impact of these aspects of cyber risk requires strategic thinking that goes beyond the IT department.

NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps boards should consider as they seek to enhance their oversight of cyber risks. This handbook is organized according to these five key principles:

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risk 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 of which risks to avoid, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

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.

A rapidly evolving cyber-threat landscape

As recently as a few years ago, cyberattacks were largely the province of hackers and a few highly sophisticated individuals. While problematic, many corporations could chalk up these events as simply a frustrating cost of doing business.

Today, corporations are subject to attackers who are part of ultra-sophisticated teams that deploy increasingly targeted malware against systems and individuals in multistaged, stealthy attacks. These attacks, sometimes referred to as APTs (for advanced persistent threats), were first deployed against government entities and defense contractors. More recently, they have migrated throughout the economy, meaning that virtually any organization is at risk.

[1] Ocean Tomo, "*Annual Study of Intangible Asset Market Value from Ocean Tomo, LLC*" (press release), Mar. 5, 2015.

RETURN TO TABLE OF CONTENTS

Cyber Threats by the Numbers

- Forty-eight percent of cyberbreaches result from criminal or malicious attacks.[i] Eighty percent of black-hat hackers are affiliated with organized crime.[ii]
- Top methods of access by cybercriminals include using stolen access credentials and malware.[iii] Attacks on mobile devices and cyberextortion attacks are both on the rise.[iv]
- The median number of days an organization is compromised before discovering a cyberbreach is 146.[v] Fifty-three percent of cyberattacks are first identified by law enforcement or third parties, compared with 47 percent that are discovered internally.[vi]
- Forty-eight percent of IT security professionals do not inspect the cloud for malware, despite the fact that 49 percent of all business applications are now stored in the cloud. Of those cloud-based applications, less than half are known, sanctioned, or approved by IT.[vii]
- Thirty-eight percent of IT organizations do not have a defined process for reviewing their cyberbreach response plans, and nearly a third have not reviewed or updated their plans since they were initially developed.[viii]

[i] Ponemon Institute and IBM, *2016 Cost of Data Breach Study: Global Analysis*, p. 2.
[ii] Limor Kessem, "2016 Cybercrime Reloaded: Our Predictions for the Year Ahead," Jan. 15, 2016.
[iii] Verizon, *2016 Data Breach Investigations Report,* p. 8–9.
[iv] Kessem, "2016 Cybercrime Reloaded."
[v] FireEye Inc, *Mandiant M-Trends 2016*, p. 4.
[vi] *Mandiant M-Trends*, p. 7, *2016 Data Breach Investigation Report*, p. 11.
[vii] Jeff Goldman, "48 Percent of Companies Don't Inspect the Cloud for Malware," *eSecurity Planet* (blog), Oct. 12, 2016.
[viii] Thor Olavsrud, "Companies complacent about data breach preparedness," *CIO*, Oct. 28, 2016.

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. 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, contract workers and employees—whether disgruntled or merely poorly trained—present at least as big an exposure for companies as attacks from the outside. 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.[2]

Greater connectivity, greater risk

Due to the immense amount of interconnection among data systems, it is no longer adequate that organizations secure only "their" network. Vendors, suppliers, partners, customers, or any entity connected with the company electronically can become a potential point of vulnerability. For example, a major oil company's systems were breached when a sophisticated attacker who was unable to penetrate the network instead inserted malware into the online menu of a Chinese restaurant popular with employees. Once inside the company's system, the intruders were able to attack its core business.[3]

Other high-profile breaches have not been the work of outside intruders, but rather were accomplished by employees or contractors who were given access to the company's network. In 2016, Harold Martin became the second contractor, after Edward Snowden, to gain notoriety for compromising one of the supposedly most secure organizations in the world—the U.S. National Security Agency—from the inside. Several years earlier, Pvt. Bradley (now Chelsea) Manning stole a massive amount of supposedly secure information from the U.S. military and handed it over to WikiLeaks for broadcast—again from the inside. In this case, poor human resource management was the culprit. More recently, the growing interconnection of traditional

[2] Verizon RISK Team, et al., *2013 Data Breach Investigations Report*, March 2013.
[3] Nicole Perlroth, "Hackers Lurking in Vents and Soda Machines," the *New York Times*, Apr. 7, 2014.

RETURN TO TABLE OF CONTENTS

information systems with nontraditional equipment such as security cameras, copiers, video-gaming platforms and cars—the so-called Internet of Things, or IoT—has resulted in an exponential increase in the number of potential points of entry for cyberattackers, and thus the need for organizations to expand their thinking about cyber-risk defense. A "distributed denial of service" attack in 2016 that severely restricted access to over 1,000 corporate websites, including those of Twitter, PayPal, and Netflix, was coordinated by hackers using hundreds of thousands of end-user devices, including home digital video recorders and webcams.[4]

Government agencies have focused primarily on defending the nation's critical infrastructure (including power and water supplies, communication and transportation networks, and the like) from cyberattack. While such attacks are technically possible and could have very serious consequences, the vast majority of incidents are economically motivated.[5] Cyberattackers routinely attempt to steal all manner of data, including personal information from customers and employees, financial data, business plans, trade secrets, and intellectual property. Increasingly, cyberattackers are employing tactics that encrypt an organization's data, effectively holding it hostage until they receive a payment—so-called "ransomware." Estimating the damage of cyberattacks is difficult, but some estimates put it at $400–500 billion or more annually, with a significant portion of costs going undetected.[6] Cybercrime costs quintupled between 2013 and 2015, and could top $2 trillion per year by 2019.[7]

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—a figure that is closer to 75 percent in the United Kingdom.[8, 9] Soberingly, according to the U.S. National Cyber Security Alliance, 60 percent of small companies that suffer a cyberattack are out of business within six months.[10] 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,

Why Would They Attack Us?

Some organizations believe 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

[4] Samuel Burke, "Massive cyberattack turned ordinary devices into weapons," CNNMoney.com, Oct. 22, 2016.
[5] Verizon, *2016 Data Breach Investigations Report*, p. 7.
[6] Steve Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019," *Forbes*, Jan. 17, 2016.
[7] Ibid.
[8] Patricia Harman, "50% of small businesses have been the target of a cyber attack," PropertyCasualty360.com, Oct. 7, 2015.
[9] Mark Smith, "Huge rise in hack attacks as cyber-criminals target small business," *The Guardian*, Feb. 8, 2016.
[10] Gary Miller, "60% of small companies that suffer a cyber attack are out of business within six months," the *Denver Post*, Oct. 24, 2016.

making vendor and partner management a critical function for all interconnected entities.

There is general consensus in the cybersecurity field that cyberattackers are well ahead of the corporations that must defend against them. Cyberattacks are relatively inexpensive yet highly profitable, and the resources and skills necessary to launch an attack are easy to acquire. It is no wonder that many observers believe cyber-risk defense tends to lag a generation behind the attackers. It is difficult 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.[11]

This does not mean that defense is impossible, but it does mean that 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 profitability

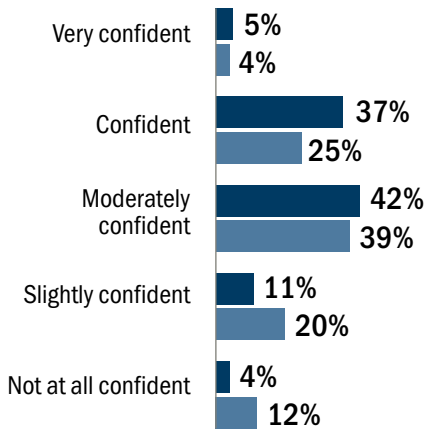
Like other critical risks organizations face, cybersecurity cannot be considered in a vacuum. Members of management and the board must strike the appropriate balance between protecting the security of the organization and mitigating downside losses, while continuing to ensure profitability and growth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

Many technical innovations and business practices that enhance profitability can also undermine security. For example, many 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. Properly deployed, they could increase security, but only at a cost.

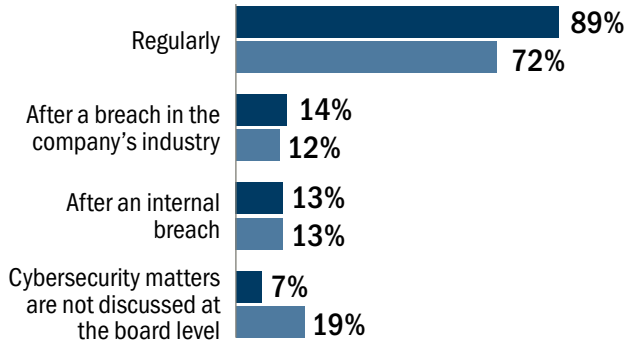
Similarly, trends such as BYOD (bring your own device), 24/7 access to information, the growth of sophisticated "big data" analytics, and the use of long, international supply chains may be so cost-effective that they are required in order for a business to remain competitive. However, these practices

FIGURE 1

How confident are you that your company is properly secured against a cyber attack?



How often is cybersecurity discussed at board meetings?



Public-company directors Private-company directors

Source: This data is compiled from the NACD 2016–2017 public- and private-company governance surveys.

[11] Robert M. Regoli, et al., *Exploring Criminal Justice: The Essentials* (Burlington, MA: Jones & Bartlett Learning, 2011), p. 378.

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 methods cannot simply be "bolted on" at the end of business processes. Cybersecurity needs to be woven into an organization's key systems and processes from end to end—and when done successfully, it can help build competitive advantage. One study found that four basic security controls were effective in preventing 85 percent of cyberintrusions:

- Restricting user installation of applications ("whitelisting").
- Ensuring that the operating system is "patched" with current updates.
- Ensuring that software applications are regularly updated.
- Restricting administrative privileges (i.e., the ability to install software or change a computer's configuration settings).[12]

The study showed that not only were these core security practices effective, they also improved business efficiency and created an immediate positive return on investment, even before considering the positive economic impact of reducing cyberbreaches.[13]

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.

[12] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, October 2013. See also: Internet Security Alliance, *Sophisticated Management of Cyber Risk* (Arlington, VA: Internet Security Alliance, 2013).
[13] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, October 2013.

PRINCIPLE 1

Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.

Historically, corporations have categorized information security as a technical or operational issue to be handled by the information technology (IT) department. This misunderstanding is fed by siloed corporate structures that may leave functions and business units within the organization feeling disconnected from responsibility for the security of their own data. Instead, this critical responsibility is handed off to IT, a department that in most organizations is strapped for resources and budget authority. Furthermore, deferring responsibility to IT inhibits critical analysis and communication about security issues, and hampers the implementation of effective security strategies.

Cyber risks should be evaluated in the same way an organization assesses the physical security of its human and physical assets and the risks associated with their potential compromise. In other words, cybersecurity is an enterprise-wide risk management issue that needs to be addressed from a strategic, cross-departmental, and economic perspective.[14]

Cyber risk and the business ecosystem

Some of the highest-profile data breaches to date have had little to do with traditional hacking. For example, spear phishing—a common e-mail attack strategy that targets specific individuals—is a leading cause of system penetration. Product launches or production strategies that use complex supply chains that span multiple countries and regions can magnify cyber risk. Similarly, mergers and acquisitions requiring the integration of complicated systems, often on accelerated timelines and without sufficient due diligence, can increase cyber risk.

Another obstacle companies face in creating a secure system is how to manage the degree of interconnection that the corporate network has with partners, suppliers, affiliates, and customers. Several significant and well-known cyberbreaches did not actually start within the target's IT systems, but instead resulted from vulnerabilities in one of their vendors or suppliers, as the examples in the section, "Greater connectivity, greater risk," on page 5 reflect. Furthermore, an increasing number of organizations have some amount of data residing on external networks or in public "clouds," which they neither own nor operate and have little inherent ability to secure. These interdependencies can undermine the security of the "home office." Many organizations also are interconnected with elements of the national critical infrastructure, raising the prospect of cyberinsecurity at one company or institution becoming a matter of public security, or even affecting national security.

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 ensure that they are adequately protecting our data?

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 ecosystem in which it operates. Progressive boards will engage management in a discussion of the varying levels of risk that exist in the company's ecosphere and take them into consideration as they calculate the appropriate cyber-risk posture and tolerance for their own corporation.[15] They should also understand what "crown jewels" the company most needs to protect, and ensure that management has a protection strategy that builds from those high-value targets outward. 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.[16]

[14] Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs*, 2010.

[15] NACD, et al., *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014) (an NACD white paper).

[16] Ibid. See also: KPMG Audit Committee Institute, *Global Boardroom Insights: The Cyber Security Challenge*, Mar. 26, 2014.

RETURN TO TABLE OF CONTENTS

See **Appendix A** for a list of cybersecurity questions that directors can ask management on issues such as situational awareness, strategy and operations, insider threats, supply-chain/third-party risks, incident response, and post-breach response. **Appendix B** outlines cybersecurity considerations related to mergers and acquisitions.

Cyber-risk oversight responsibility at the board level

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 Risk Governance recommended that risk oversight should be a function of the full board.[17] NACD research finds this to be true at most public-company boards with so-called "big-picture risks" (i.e., risks with broad implications for strategic direction, or discussions of the interplay among various risks). Yet just over half of boards assign the majority of cybersecurity-related risk-oversight responsibilities to the audit committee (Figure 2), which also assumes significant responsibility for oversight of financial reporting and compliance risks.

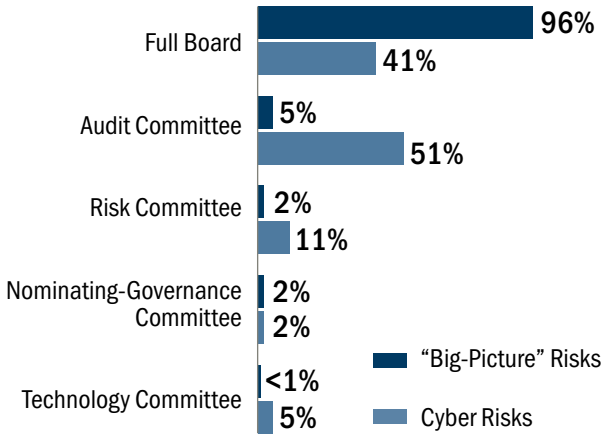
There is no single approach that will fit every board: some choose to conduct all cyber-risk-related discussions at the full-board level; others assign specific cybersecurity-related oversight responsibilities to one or more committees (audit, risk, technology, etc.); and still others use a combination of these methods. 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 semiannually 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.[18]

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 full-board discussions involving 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.

FIGURE 2

To which group has the board allocated the majority of tasks connected with the following areas of risk oversight? (Partial list of response choices; multiple selections permitted)



Source: *2016–2017 NACD Public Company Governance Survey*

See **Appendix C** for suggested questions to help directors assess their board's level of understanding of cybersecurity issues. **Appendix D** contains sample board evaluation questions related to cybersecurity oversight.

[17] NACD, *Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward* (Washington, DC: NACD, 2009).
[18] Adapted from Robyn Bew, "Cyber-Risk Oversight: 3 Questions for Directors," *Ethical Boardroom*, Spring 2015.

RETURN TO TABLE OF CONTENTS

PRINCPLE 2

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 required disclosures, privacy and data protection, information-sharing, infrastructure protection, and more, is complex and constantly evolving. Boards should stay aware of current liability issues faced by their organizations—and, potentially, by directors on an individual or collective basis. For example, 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 company's or organization's sector and operating locations.

The business judgment rule may protect directors, so long as the board takes reasonable 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 in one or more cyberbreach simulations, or "table-top exercises," to gain exposure to the company's response procedures 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 issued by the Securities and Exchange Commission (SEC) in 2011 (see page 12, "SEC disclosure guidance")
- Industry-specific regulations from the SEC, Federal Trade Commission, and other agencies that affect sectors such as retail, healthcare, banking 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), multilateral, 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 proactively communicates the process by which it assesses damage caused by a cyber incident and the methodology it uses to account for cyber incidents affecting data and assets. Communicating such a process will not reveal sensitive information about a company's cybersecurity efforts."[19]

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

RETURN TO TABLE OF CONTENTS

SEC disclosure guidance

In October 2011, the SEC's Division of Corporation Finance issued interpretive guidance as to how it views publicly held corporations' disclosure obligations under existing law with respect to cybersecurity risks and incidents. "CF Disclosure Guidance: Topic 2" noted that corporations had "migrated toward increasing dependence on digital technologies to conduct their operations," and described corresponding cybersecurity risks as a business risk that a "reasonable investor would consider important to an investment decision."[20]

Accordingly, the guidance stated that corporations should consider disclosing material information about cyber risks not only in general terms, but also on an incident-by-incident basis. The factors that the SEC suggested a corporation should weigh in determining the contours of its disclosure are

- frequency and severity of prior cyber incidents;
- probability of cyber incidents occurring;
- potential costs and consequences (e.g., assets or sensitive information misappropriation, corruption of data, disruption of operations);
- adequacy of preventative actions taken; and
- risk level of threatened attacks.[21]

The SEC further suggested that within their corporate filings, companies might want to disclose the following based on their circumstances and materiality, while avoiding "boilerplate" language.

- "[A]spects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences"
- A description of any outsourced functions that may have material cybersecurity risks and how the registrant addresses those risks
- A "[d]escription of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences"
- "Risks related to cyber incidents that may remain undetected for an extended period"
- A "[d]escription of relevant insurance coverage"[22]

While guidance from the Division of Corporation Finance does not constitute an SEC rule, regulation, or official statement, if companies choose not to follow these guidelines, pre-trial actions such as motions to dismiss could be made more difficult. Specifically, should a corporation be the victim of a cyberattack without having disclosed the information discussed above and suffer even a modest reduction in its share price, it risks a lengthy and costly process to resolve private lawsuits alleging inadequate public disclosure. Since 2011, the SEC's own enforcement priorities have included SEC-registered broker-dealers and investment advisers that violate rules regarding protecting customer data, and public companies that make materially false or misleading disclosures relating to cybersecurity.

Directors should ask management to solicit external counsel's point of view on potential disclosure considerations related to forward-looking risk factors in general, and also in terms of the company's game plan for response to a major breach or other cyber incident.

As disclosure standards, regulatory guidance, formal requirements, and company circumstances all continue to evolve, management and directors should expect to be updated on a regular basis by counsel.

[20] Securities and Exchange Commission, Division of Corporation Finance, "CF Disclosure Guidance," Oct. 13, 2011.
[21] Securities and Exchange Commission, Division of Corporation Finance, "CF Disclosure Guidance," Oct. 13, 2011.
[22] Ibid.

RETURN TO TABLE OF CONTENTS

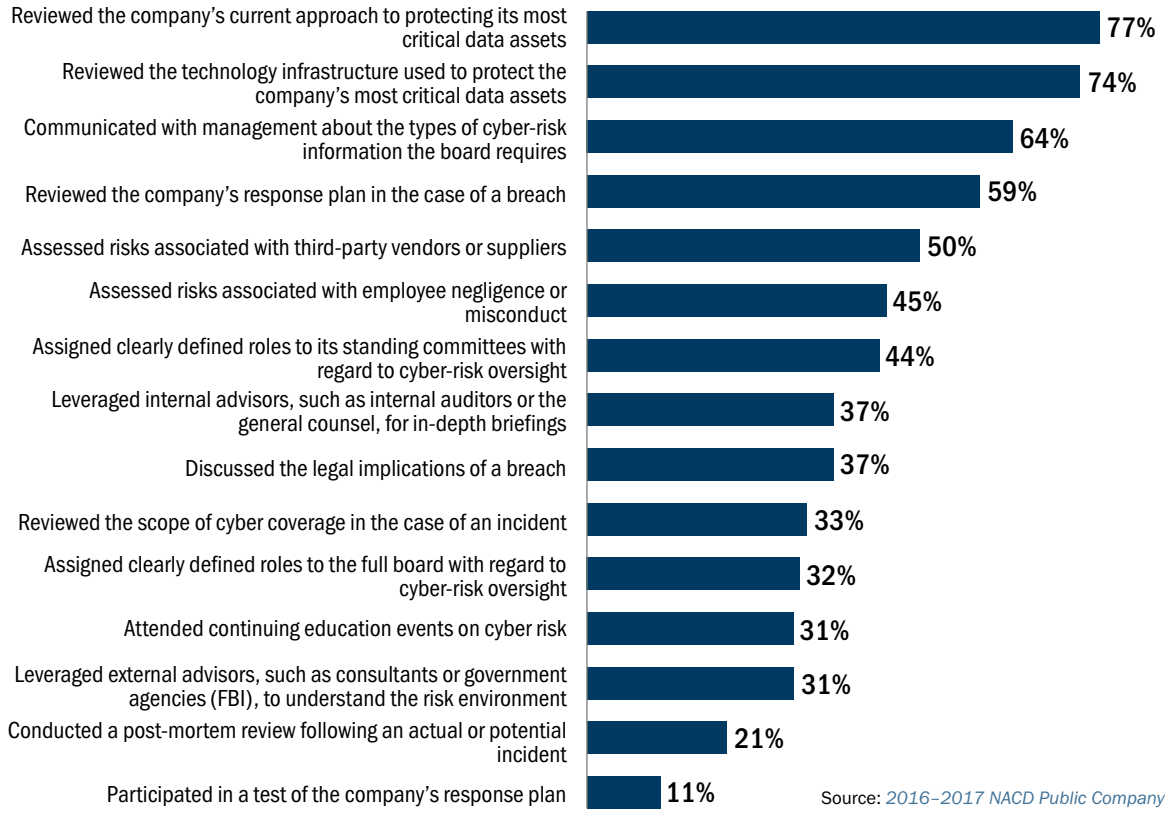
PRINCIPLE 3

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.

In an NACD survey of public-company directors, 89.1 percent of respondents reported that their boards discuss cybersecurity "on a regular basis."[23] See Figure 3 for additional details. Despite this level of activity, however, only about 14 percent of directors believe their board has a "high" level of knowledge of cybersecurity risks.[24] As a director at an NACD forum observed, "[Cybersecurity] is very much a moving target. The threats and vulnerabilities are changing almost daily, and the standards for how to manage and oversee cyber risk are only beginning to take shape."[25] At a different peer-exchange session, another director suggested this useful analogy: "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."[26]

FIGURE 3

Which of the following cyber-risk oversight practices has the board performed over the last 12 months?



Source: *2016–2017 NACD Public Company Governance Survey*

[23] NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p. 28.
[24] NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p. 26.
[25] NACD Audit Committee Chair and Risk Oversight Advisory Councils, *Emerging Trends in Cyber-Risk Oversight*, July 17, 2015, p. 1.
[26] NACD, et al., *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014) (an NACD white paper), p. 3.

RETURN TO TABLE OF CONTENTS

Improving access to cybersecurity expertise

As the cyber threat has grown, the responsibility (and expectations) of board members has grown also. 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 result, 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 organizations, there is no one-size-fits-all approach that will apply everywhere (see "A Cyberexpert on Every Board?"). At an NACD roundtable discussion between directors and leading investors, participants expressed concerns about calls to add so-called "single-purpose" directors—whether narrowly specialized in cybersecurity or other areas—to all boards. As one participant put it, "It can signal risk aversion, a concern that the board will be sued, so we need one of X, Y, and Z—all the [management] skills du jour. But directors aren't running the company."[27]

Nominating and governance committees must balance many factors in filling board vacancies, including the need for industry expertise, financial knowledge, global experience, or other desired skill sets, depending on the company's strategic needs and circumstances. Whether or not they choose to add a board member with specific expertise in the cyberarena, directors can take advantage of other ways to bring knowledgeable perspectives on cybersecurity matters into the boardroom, including the following strategies:

- 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.

A Cyberexpert on Every Board?

In 2008, NACD, the Council of Institutional Investors, and the Business Roundtable codeveloped a set of Key Agreed Principles for corporate governance "intended to assist boards and shareholders in avoiding rote 'box ticking' in favor of a more thoughtful and studied approach." They included the idea that (presuming compliance with all applicable legal, regulatory, and exchange listing requirements) individual boards hold responsibility for designing the structures and practices that will allow them to fulfill their fiduciary obligations effectively and efficiently, and that they are obligated to communicate those structures and practices to stakeholders in a transparent manner. Proposals aimed, for example, at requiring all boards to have a director who is a "cybersecurity expert"—even setting aside the fact that the severe shortage of senior-level cybersecurity talent, with hundreds of thousands of positions vacant in the U.S. alone, makes such proposals impossible to implement—would take the important responsibility for board composition and director recruitment out of the hands of the only group with firsthand knowledge about a specific board's current and future skill requirements. The *Key Agreed Principles* publication goes on to say that "valuing disclosure over the [rigid] adoption of any set of [so-called] best practices encourages boards to experiment and develop approaches that address their own particular needs."

Sources: Internet Security Alliance, *The Cybersecurity Social Contract: Implementing a Market-Based Model for Cybersecurity* (Washington, DC: ISA, 2016), pp. 335–338; NACD, *Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies* (Washington, DC: NACD, 2011), p. 5.

[27] Discussion at a joint meeting of the NACD Advisory Councils for Audit Committee Chairs and Nominating and Governance Committee Chairs, Oct. 5, 2016.

Enhancing management's reports to the board

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.[28] Since then, boardroom practices have changed dramatically: As noted on page 13, nearly 90 percent of public-company directors say their boards discuss cybersecurity issues on a regular basis and receive information from a range of management team members (Figure 4). Yet a significant number of directors believe their organizations still need improvement in this area. 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. Less than 15 percent said they were very satisfied with the quality of the information they received, as compared with an approximately 64 percent high-satisfaction rating for information about financial performance.[29]

FIGURE 4

Which representatives from management report to the board about the state of cybersecurity? (Select all that apply)

Source: *2016–2017 NACD Public Company Governance Survey*

NACD survey respondents identified several reasons for their dissatisfaction with management's cybersecurity reporting, including

- difficulty in using the information to benchmark performance, both internally (between business units within the organization) and externally (with industry peers);
- insufficient transparency about performance; and
- difficulty in interpreting the information.[30]

Cybersecurity and cyber-risk analysis are relatively new disciplines—certainly, much less mature than financial analysis—and it will take time for reporting practices to mature. Nonetheless, 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, directors should also be mindful that there might be an inherent bias on the part of management to downplay the true state of the risk environment. 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.[31]

See **Appendices E** and **F** for examples of cyber-risk reporting metrics and dashboards.

[28] Jody R. Westby, Carnegie Mellon University, *Governance of Enterprise Security: CyLab 2012 Report*, (Pittsburgh, PA: Carnegie Mellon University, 2012), p. 7 and p. 16.
[29] NACD, *2016–2017 NACD Public Company Governance Survey* (Washington, DC: NACD, 2016), p. 28.
[30] Ibid.
[31] Sean Martin, "Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's 'Serious,'" *International Business Times*, April 16, 2014.

RETURN TO TABLE OF CONTENTS

PRINCIPLE 4

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

Technology integrates modern organizations, whether workers are across the hall or halfway around the world. But, as noted earlier, the reporting structures and decision-making processes at many companies are legacies of a siloed and unintegrated past, where each department and business unit makes decisions relatively independently, and without fully taking into account the digital interdependency that is a fact of modern life. Directors should seek assurances that management is taking an appropriate enterprise-wide approach to cybersecurity.

Appendices G and H outline U.S. federal government cybersecurity resources available to the private sector to help inform directors' discussions with management about how the organization is utilizing such resources. Appendix I contains considerations for building a relationship with the CISO.

The NIST Cybersecurity Framework

In February 2013, President Obama signed Executive Order 13636—Improving Critical Infrastructure Cybersecurity. The order instructed the National Institute of Standards and Technology (NIST) to develop a cybersecurity framework that could be voluntarily adopted by the private sector.[32]

Released in 2014, the NIST Cybersecurity Framework is a set of standards, methodologies, procedures, and processes that aligns policy, business, and technological issues to address cyber risks. The framework seeks to provide a common language for senior corporate management to use within the organization in developing an enterprise-wide approach to cyber-risk management. It suggests that to start their cybersecurity review, corporations engage in a risk-management process that will determine where the organization sits on a four-tier scale: (1) partial, the lowest tier; (2) risk informed; (3) repeatable; and (4) adaptive, the highest tier.

This level of management may be beyond the practical ability of all organizations, but some elements are available to all companies. According to a 2015 National Cybersecurity Institute study of information-security professionals, over 50 percent of respondents said their companies were using the framework, and adoption rates were over 80 percent in the federal government.[33] Directors should set the expectation that management has considered the NIST Cybersecurity Framework in developing the company's cyber-risk defense and response plans.

[32] Executive Order No. 13636—Improving Critical Infrastructure Cybersecurity, Federal Register 78, no. 33, (Feb. 19, 2013).

[33] Arieanna Schweber, "Adoption rate soars for NIST framework," *InTelligence Blog*, Jan. 12, 2016, and Kevin L. Jackson, "*What has NIST done for me lately?*," *Direct2Dell* (blog), Jan. 4, 2016.

An Integrated Approach to Managing Cyber Risk

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.
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, HR, IT, 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 U.S. 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 total 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.

Source: Internet Security Alliance[1]

[1] 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).

RETURN TO TABLE OF CONTENTS

PRINCIPLE 5

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

Total cybersecurity is an unrealistic goal. Cybersecurity—as with security in general—is a continuum, not an end state, and security is not the equivalent of compliance. Management teams need to determine where, on a spectrum of risk, they believe the firm's operations and controls have been optimized. As with other areas of risk, an organization's cyber-risk tolerance must be consistent with its strategy and, in turn, its resource allocation choices (see "Defining Risk Appetite," page 19). As such, directors and management teams will need to grapple with the following questions:

- **What data, and how much data, are we willing to lose or have compromised?** Discussions of risk tolerance will help to identify the level of cyber risk the organization is willing to accept as a practical business consideration. In this context, distinguishing between mission-critical assets (see "Identifying the Company's 'Crown Jewels,'" page 9) and other data that is important, but less essential, is a key first step.

- **How should our cyber-risk mitigation investments be allocated among basic and advanced defenses?** When considering how to address more sophisticated threats, management should place the greatest focus on sophisticated defenses designed to protect the company's most critical data assets. While most organizations would agree with this in principle, research from the Armed Forces Communications and Electronics Association (AFCEA) indicates that instead companies typically apply security measures equally to all data and functions. The same AFCEA study notes that protecting low-impact systems and 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.[34] Boards should encourage management to frame the company's cybersecurity investments in terms of ROI, and to 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. 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. Beyond coverage for financial loss, these tools can help to mitigate an organization's risk of suffering from property damage and bodily injury resulting from a cyberbreach. Some solutions also include access to proactive tools, employee training, IT security, and expert response services, to add another layer of protection and expertise. 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 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. When choosing a cyber-insurance 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. 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 we assess the impact of cybersecurity incidents?** Conducting a proper impact assessment can be challenging given the number of factors involved. To take

[34] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, October 2013, p. 8.

RETURN TO TABLE OF CONTENTS

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.

Defining Risk Appetite

"Risk appetite is the amount of risk an organization is willing to accept in pursuit of strategic objectives. Thus, it should define the level of risk 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 they willing to bear, and to what level?
- Capacity - What resources are required to manage those risks?

"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* (New York, NY: PwC, 2014), p. 3.

Conclusion

Cybersecurity is a serious enterprise-level risk issue that affects virtually all levels of an organization's operating activities. Several characteristics combine to make the nature of the threat especially formidable: its complexity and speed of evolution; the potential for significant financial, competitive, and reputational damage; and the fact that total protection is an unrealistic objective. In the face of these threats, and despite dramatic increases in private-sector cybersecurity spending,[35] the economics of cybersecurity still favor attackers. Moreover, many business innovations come with increased vulnerability, and risk management in general—IT- and cyber-related security measures in particular—has traditionally been considered to be a cost center in most for-profit institutions.

Directors need to continuously assess their capacity to address cybersecurity, both in terms of their own fiduciary responsibility as well as their oversight of management's activities, and many will identify gaps and opportunities for improvement. While the approaches taken by individual boards will vary, the principles in this handbook offer benchmarks and a suggested starting point. Boards should seek to approach cyber risk from an enterprise-wide standpoint:

- Understand the legal ramifications for the company, as well as for the board itself.
- Ensure directors have sufficient agenda time and access to expert information in order to have well-informed discussions with management.
- Integrate cyber-risk discussions with those about the company's overall tolerance for risk.

Ultimately, as one director put it, "Cybersecurity is a human issue."[36] The board's role is to bring its judgment to bear and provide effective guidance to management, in order to ensure the company's cybersecurity strategy is appropriately designed and sufficiently resilient given its strategic imperatives and the realities of the business ecosystem in which it operates.

[35] Steve Morgan, "*Worldwide Cybersecurity Spending Increasing to $170 Billion by 2020*," Forbes, Mar. 9, 2016. See also Piers Wilson, *Security market trends and predictions from the 2015 member survey*, Institute of Information Security Professionals.
[36] NACD, et al., *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014) (an NACD white paper), p. 7.

RETURN TO TABLE OF CONTENTS

APPENDIX A

Questions for the Board to Ask Management About Cybersecurity

Situational Awareness

1. Were we told of cyberattacks that have already occurred and how severe they were?
2. What are the company's cybersecurity risks, and how is the company managing these risks?[1]
3. How will we know if we have been hacked or breached, and what makes us certain we will find out?
4. Who are our likely adversaries?[2]
5. In management's opinion, what is the most serious vulnerability related to cybersecurity (including within our IT systems, personnel, or processes)?
6. If an adversary wanted to inflict the most damage on our company, how would they go about it?
7. Has the company assessed the insider threat?[3]
8. When was the last time we conducted a penetration test or an independent external assessment of our cyber defenses? What were the key findings, and how are we addressing them? What is our maturity level?
9. Does our external auditor indicate we have cybersecurity-related deficiencies in the company's internal controls over financial reporting? If so, what are they, and what are we doing to remedy these deficiencies?

Strategy and Operations

1. What are the leading practices for cybersecurity, and where do our practices differ?
2. Do we have appropriately differentiated strategies for general cybersecurity and for protecting our mission-critical assets?
3. Do we have an enterprise-wide, independently budgeted cyber-risk management team? Is the budget adequate? How is it integrated with the overall enterprise risk management process?
4. Do we have a systematic framework, such as the NIST Cybersecurity Framework, in place to address cybersecurity and to assure adequate cybersecurity hygiene?
5. Where do management and our IT team disagree on cybersecurity?
6. Do the company's outsourced providers and contractors have cybersecurity controls and policies in place? Are those controls monitored? Do those policies align with our company's expectations?
7. Does the company have cyber insurance? If so, is it adequate?
8. Is there an ongoing, company-wide awareness and training program established around cybersecurity?
9. What is our strategy to address cloud, BYOD, and supply-chain threats?[4]
10. How are we addressing the security vulnerabilities presented by an increasingly mobile workforce?

Insider Threats

1. What are the leading practices for combating insider threats, and how do ours differ?
2. How do key functions (IT, HR, Legal, and Compliance) work together and with business units to establish a culture of cyber-risk awareness and personal responsibility for cybersecurity? Considerations include the following:
   a. Written policies which cover data, systems, and mobile devices should be required and should be required for all employees.
   b. Establishment of a safe environment for reporting cyber incidents (including self-reporting of accidental issues).
   c. Regular training on how to implement company cybersecurity policies and recognize threats.

[1] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."
[2] Lexology.com, Ed Batts, DLA Piper LLP, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014.
[3] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."
[4] Lexology.com, Ed Batts, DLA Piper LLP, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014.

RETURN TO TABLE OF CONTENTS

3. How have we adapted our personnel policies, such as background checks, new-employee orientation, training related to department/role changes, employee exits, and the like, to incorporate cybersecurity?
4. How do our operational controls, including access restrictions, encryption, data backups, monitoring of network traffic, etc., help protect against insider threats?
5. Do we have an insider-incident activity plan that spells out how and when to contact counsel, law enforcement and/or other authorities, and explore legal remedies?

Supply-Chain/Third-Party Risks

1. How do we balance the financial opportunities (lower costs, higher efficiency, etc.) created by greater supply-chain flexibility with potentially higher cyber risks?
2. How much visibility do we currently have across our supply chain regarding cyber-risk exposure and controls? Which departments/business units are involved?
3. What will need to be done to fully include cybersecurity in current supply-chain risk management?
4. 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. Written cybersecurity policies.
   b. Personnel policies, such as background checks, training, etc.
   c. Access controls.
   d. Encryption, backup, and recovery policies.
   e. Secondary access to data.
   f. Countries where data will be stored.
   g. Notification of data breaches or other cyber incidents.
   h. Incident-response plans.
   i. Audi ts of cybersecurity practices and/or regular certifications of compliance.
5. How difficult/costly will it be to establish and maintain a viable cyber-vulnerability and penetration-testing system for our supply chain?
6. How difficult/costly will it be to enhance monitoring of access points in the supplier network?
7. Do our vendor agreements bring new legal risks or generate additional compliance requirements (e.g., FTC, HIPAA, etc.)?
8. Are we indemnified against security incidents on the part of our suppliers/vendors?

Incident Response

1. How will management respond to a cyberattack?[5] Does the company have a validated incident-response plan?[6] Under what circumstances will law enforcement and other relevant government entities be notified?[7]
2. For significant breaches, is our communication adequate as information is obtained regarding the nature and type of breach, the data impacted, and the ramifications to the company and the response plan?[8]
3. Are we adequately exercising our cyber-preparedness and response plan?
4. What constitutes a material cybersecurity breach? How will such events be disclosed to investors?

After a Cybersecurity Incident

1. How did we learn about the incident? Were we notified by an outside agency, or was the incident discovered internally?
2. What do we believe was stolen?
3. What has been affected by the incident?
4. Have any of our operations been compromised?
5. Is our cyber-incident response plan in action, and is it working as planned?

[5] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."
[6] Ibid.
[7] Ibid.
[8] Ibid.

RETURN TO TABLE OF CONTENTS

6. Whom must we notify about this incident (materiality), whom should we notify, and is our legal team prepared for such notifications?
7. What is the response team doing to ensure that the incident is under control and that the hacker no longer has access to our internal network?
8. Do we believe the hacker was an internal or an external actor?
9. What were the weaknesses in our system that allowed the incident to occur (and why)?
10. What steps can we take to make sure this type of event does not happen again?
11. What can we do to mitigate any losses caused by the incident?

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

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 (FBI), Department of Homeland Security, U.S. Secret Service).
- Regulatory agencies.
- U.S. 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.

RETURN TO TABLE OF CONTENTS

APPENDIX B

Cybersecurity Considerations During M&A Phases

Companies involved in transactions are often prime targets for hackers and cybercriminals, because the value of confidential deal-related information is high, and the short timelines, high-pressure environment, and significant workloads associated with transactions can cause key players to act carelessly and potentially make mistakes. Cybersecurity vulnerabilities exploited during a transaction can pose risks to the deal's value and return on investment:

Short-term risks

- Paralyzed operations as a result of ransomware or malware.
- Transaction period might be used by threat actors to gain entry and conduct reconnaissance, an event which often is not detected until well after the deal closes.
- Theft of inside information, including valuations, bids, etc.
- Warranty claims, a change of deal terms, or a reduction in the deal's value.
- Forensic investigations related to a data breach.

Long-term risks

- Exposure to risk from regulatory and other lawsuits.
- Regulatory investigation and penalties.
- Loss of customers, and associated hits to sales and profit.
- Reputational damage.
- Loss of market share to competitors without a known data breach.

Directors should ask management to conduct a cyber-risk assessment for each phase of the transaction's lifecycle to confirm that 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. According to published reports, hackers have already broken into the networks of several large U.S. law firms, signaling that thieves are scouring the digital landscape for more sophisticated types of information than credit card accounts. Law firms, financial advisers, and other associated firms are attractive to hackers because they hold trade secrets and other sensitive information about corporate clients, including details about early-stage deal exploration that could be stolen to inform insider trading or to gain a competitive advantage in deal negotiations.

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. There are four primary ways that information is at risk:

- A hacker works into the network through holes in its defenses, starting with a company's Internet-facing computers.
- A hacker launches a social engineering attack against a company employee.
- Company insiders (employees, contractors, vendors) release sensitive data and information, either intentionally or as a result of negligence.
- Information is exposed through vulnerabilities in third-party vendors or service providers.

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 begins:

- Conducting "dark web" (anonymously-run and difficult-to-access websites favored by hackers) searches about the target, their systems, data, and intellectual property. This helps identify whether the company is already on hackers' radar, if systems or credentials are already compromised, and if there is sensitive data for sale or being solicited.
- Researching malware infections in the target company and holes in their defenses visible from the outside. This 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.
- 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.

Due Diligence and Deal Execution Phases

During these phases, the company should perform confirmatory cybersecurity due diligence. 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 defer approving the transaction until remediation is complete, or decide to back out of a transaction if the risks that are identified warrant such action. Identification of cybersecurity risks during the diligence phase can be accomplished by performing cybersecurity diligence that is tailored to discover these risks:

- 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 cyber-related data privacy laws or other applicable regulations and requirements.
- Identify recent data breaches or other cybersecurity incidents.

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 and upsides can then be factored into the initial price paid and into performance improvement investments that will raise the transaction value, enabling a robust transaction proposal to be presented to shareholders for approval.

Integration Phase

Post-deal integration poses a range of challenges related to people, processes, systems, and culture. Cyber risks add another dimension of complexity and risk to this phase of the transaction. Hackers take advantage of the inconsistencies that exist between the platforms and technology operations of the company and the newly-merged or acquired entity at this phase.

Integration teams need to have the expertise to explore and delve into the smallest of details to identify and mitigate cyber risks such as the following:

- 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.

Post-Transaction Value Creation Phase

After a transaction is completed, continued monitoring of cyber risks by management will create numerous opportunities for portfolio improvement and growth.

Management should continue to evaluate the cyber maturity of the merged or acquired entity by benchmarking it against industry standards and competition, just as they do with the core business. Low maturity could impact growth projections and brand reputation due to cyber incidents and possible fines. A breach or compliance issue could cause regulators to investigate, leading to a financial loss or stalling of post-transaction exit plans. Cyber issues can also lead to legal action by customers and suppliers causing value loss and lower returns.

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.

RETURN TO TABLE OF CONTENTS

APPENDIX C

Questions Directors Can Ask to Assess the Board's "Cyber Literacy"

1. What do we consider our most valuable assets? How does our IT system interact with those assets? Do we believe we can ever fully protect those assets?
2. Do we think there is adequate protection in place if someone wanted to get at or damage our corporate "crown jewels"? What would it take to feel confident that those assets were protected?
3. Are we investing enough so that our corporate operating and network systems are not easy targets for a determined hacker?[1]
4. Are we considering the cybersecurity aspects of our major business decisions, such as M&A, partnerships, new product launches, etc., in a timely fashion?
5. Who is in charge? Do we have the right talent and clear lines of accountability/responsibility for cybersecurity?[2]
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?[3]
8. Does the company have insurance that covers cyber events, and what exactly is covered?[4]
9. Is there director and officer exposure if we don't carry adequate insurance?[5]
10. What are the benefits beyond risk transfer of carrying cyber insurance?[6]

[1] NACD, et al., *Cybersecurity: Boardroom Implications* (Washington, DC: NACD, 2014) (an NACD white paper).
[2] Lexology.com, Ed Batts, DLA Piper LLP, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014.
[3] Ibid.
[4] StaySafeOnline.org, the National Cyber Security Alliance, and Business Executives for National Security, "Board Oversight."
[5] Ibid.
[6] Ibid.

RETURN TO TABLE OF CONTENTS

APPENDIX D

Assessing the Board's Cybersecurity Culture

In 2010, the *Report of the NACD Blue Ribbon Commission on Board Evaluation* defined boardroom culture as "the shared values that underlie and drive board communications, interactions, and decision making. It is the essence of how things really get done."[1] Five years later, at the National Association of Corporate Directors' (NACD's) first Global Cyber Summit, more than 200 directors from Fortune Global 500 companies and cybersecurity experts discussed several ways in which boardroom culture can support—or hinder—management's cybersecurity efforts. In the words of one participant:

> *Boards need to change their mindsets. We have to move from asking, "What's the likelihood we'll be attacked?" to saying, "It's probable that we've been attacked"; from viewing cybersecurity as a cost to viewing it as an investment that helps us stay competitive; from expecting management to prevent or defend against cyber threats to asking how quickly they can detect and respond to them.*[2]

Directors wishing to incorporate a cybersecurity component into their boards' self-assessments can use the questions in the table below as a starting point.

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.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	We classify cyber risk as an enterprise-wide risk.	
Our cybersecurity discussions with management focus primarily on reviews of past events (e.g., historical breach data).	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Cybersecurity is incorporated into forward-looking discus-sions with management (e.g., new product/service development, M&A/joint ventures, market entry).	
The board receives information about cybersecurity exclusively from management.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	The board receives firsthand information about cybersecurity from non-management sources.	
Information about emerging cyber threats or potential issues is filtered through the CEO.	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	The CEO encourages open access and communications between and among the board, external sources, and management about emerging cyber threats.	

[1] *Report of the NACD Blue Ribbon Commission on Board Evaluation: Improving Director Effectiveness* (Washington, DC: NACD, 2010), p. 7.

[2] Italicized quotations are from participants in the Global Cyber Summit, held Apr. 15–16, 2015, in Washington, DC. Discussions were conducted under the Chatham House Rule.

RETURN TO TABLE OF CONTENTS

APPENDIX E

Board-Level Cybersecurity Metrics

Which cybersecurity metrics should be included in a board-level briefing? This question is deceptively simple. Similar to virtually every other division and function within the organization, the cybersecurity function collects and analyzes a tremendous volume of data and there is little consensus on which are the critical few pieces of data that should be shared with a board audience. Adding to the challenge is the fact that cybersecurity is a relatively new domain, with standards and benchmarks that are still developing or evolving.

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. More often than not, boards see a high volume of operational metrics which provide very little strategic insight on the state of the organization's cybersecurity program. Metrics that are typically presented include statistics such as "number of blocked attacks," "number of unpatched vulnerabilities," and other stand-alone, compliance-oriented measures, that provide little strategic context about the organization's performance and risk position.

As a starting point, directors can apply the same general principles used for other types of board-level metrics to cybersecurity-related reporting (see Sidebar, "Guiding Principles for Board-Level Metrics").

Guiding Principles for Board-Level Metrics

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

Source: NACD

In addition, the following recommendations provide a starting point for the types of cybersecurity metrics that board members should consider requesting from management.

1. What is our cyber-risk appetite? This is a fundamental question and one that the chief information security officer (CISO) should work with the chief risk officer (CRO) function to address. This type of collaboration can produce qualitative and quantitative data points for presentation to the board that provide context around cyber-risk appetite.
2. What metrics do we have that indicate risk to the company? One organization has implemented a cybersecurity risk "index" which incorporates several individual metrics covering enterprise, supply chain, and consumer-facing risk.
3. How much of our IT budget is being spent on cybersecurity-related activities? How does this compare to our competitors/peers, and/or to other outside benchmarks? These metrics will support conversations about how management determines "how much spending is enough," and whether increasing investments will drive down the organization's residual risk. Additional follow-on questions include these:
   - What initiatives were not funded in this year's budget? Why?
   - What trade-offs were made?
   - Do we have the right resources, including staff and systems, and are they being deployed effectively?
4. How do we measure the effectiveness of our organization's cybersecurity program and how it compares to those of other companies? 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 an apples-to-apples comparison within industry sectors.
5. How many data incidents (e.g., exposed sensitive data) has the organization experienced in the last reporting period? This metric will inform conversations about trends, patterns, and root causes.

RETURN TO TABLE OF CONTENTS

6. Value chain relationships typically pose increased risk for companies given the degree of system interconnectivity and data-sharing that is now part of everyday business operations. How do we assess the cyber-risk position of our suppliers, vendors, JV partners, and customers? How do we conduct ongoing monitoring of their risk posture? How many external vendors connect to our network or receive sensitive data from us? This is a borderline operational metric, but it can help support discussions with management about residual risk from third parties. There are service providers within the cybersecurity market place that provide passive and continuous monitoring of companies' cybersecurity postures. A growing number of firms use these services to assess their high-risk third-party relationships as well as their own state of cybersecurity.
7. What operational metrics are routinely tracked and monitored by our security team? While operational metrics are the domain of the IT/Security team, it would be beneficial for directors to understand the breadth and depth of the company's cybersecurity monitoring activities for the purposes of situational awareness.
8. What metrics do we use to evaluate cybersecurity awareness across the organization? Data about policy compliance, the implementation and completion of training programs, and the like will help to inform conversations about insider risks at various seniority levels and in various regions and divisions.
9. How do we track the individuals or groups that are exempt from major security policies, activity monitoring, etc.? These measures will indicate areas where the company is exposed to additional risk, opening the way for discussions about risk/return trade-offs in this area.

RETURN TO TABLE OF CONTENTS

APPENDIX F

Sample Cyber-Risk Dashboards

Illustrative Board / Executive Dashboard – Risk Summary

Financial Services Example

LEGEND	
Risk Rating	**Trend**
Low	▲ Risk Increasing
Medium	▼ Risk Decreasing
High	■ No Change

Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
IT Risk Management	IT risks are not identified	M	9	5	▲
	IT risks are not managed to acceptable levels	M	5	6	▲
Physical & Environmental Security	Physical perimeter controls at information processing facilities are not established	L	14	4	■
	Plans and operational controls to support power contingency mechanisms are not defined	M	3	13	▲
Organization Security and Awareness	Users do not perform their security responsibilities	M	5	1	■
	Users do not understand their security responsibilities	H	30	11	▼
Information Security Program Management	The information security program is not aligned with business requirements	M	3	13	▲
	Policies and procedures have not been established for information security	L	2	11	■
Third Party Security	Security risks are not identified with third-parties	H	1	18	▲
	Security risks are not managed to acceptable levels with third-parties	M	4	13	▲
IT Operations	Information security practices are not integrated into IT operations	L	5	2	■
	IT operations are not performing their information security responsibilities	M	7	4	■

ILLUSTRATIVE

Summary Notes

RETURN TO TABLE OF CONTENTS

Illustrative Board / Executive Dashboard – Risk Summary (continued)

Financial Services Example

LEGEND	
Risk Rating	**Trend**
Low	▲ Risk Increasing
Medium	▼ Risk Decreasing
High	■ No Change

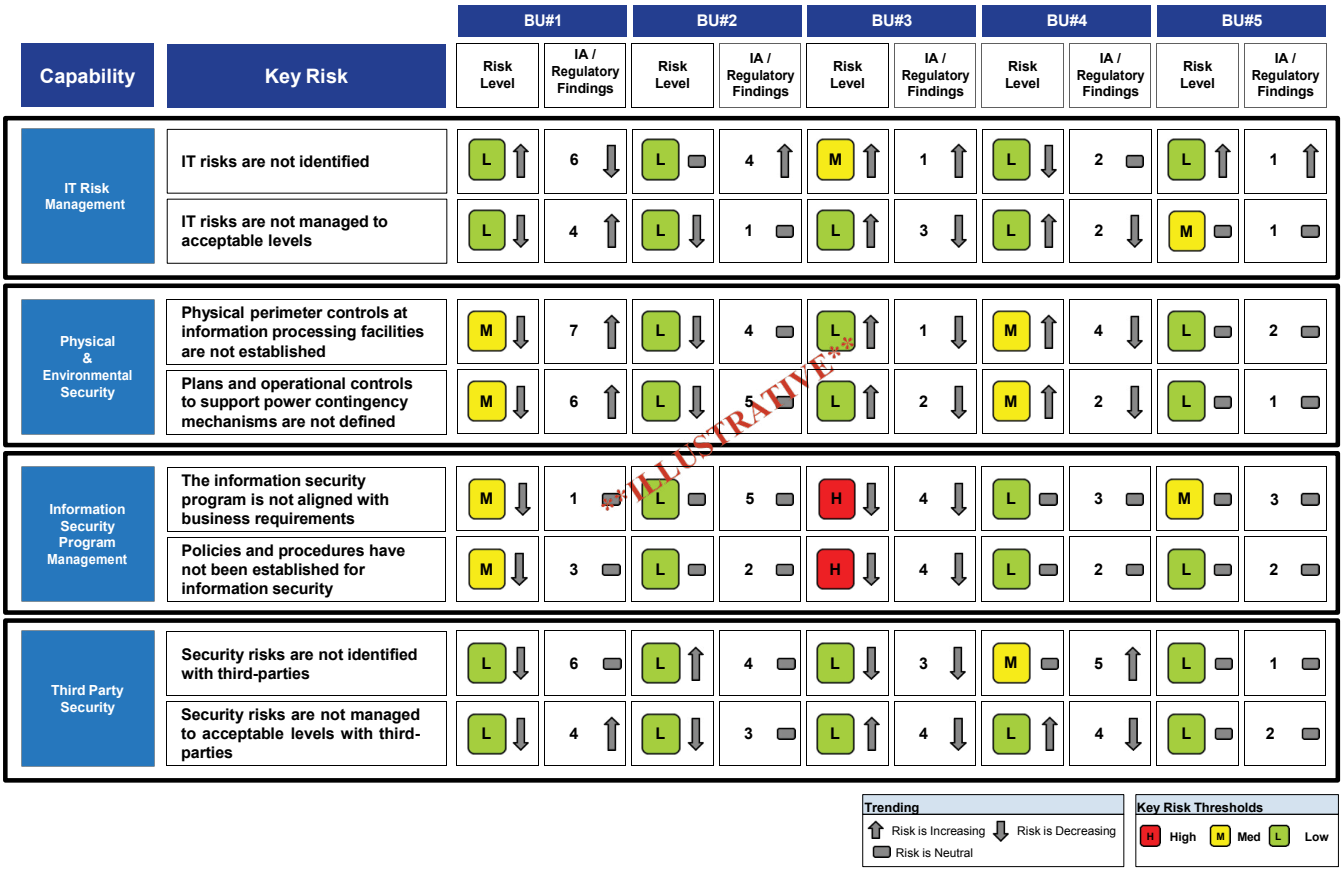
Capability	Key Risks	Risk Level	IA Finding(s)	Regulatory Finding(s)	Trend
Business Continuity	Disaster recovery processes and procedures are not defined	L	3	1	▲
	Ability to recover from an outage has not been tested	H	18	13	▲
IT Compliance Management	Adequate mechanisms to monitor and remediate compliance issues are not implemented	L	6	3	■
	Compliance with legislative, statutory, regulatory or contractual obligations are not identified	L	1	1	■
Identify & Access Management	Privileged access is used to compromise data	M	6	10	▲
	Terminated user access is not removed appropriately	M	5	10	▲
Threat & Vulnerability Management	Internal and external vulnerabilities go unmanaged	H	13	34	▲
	Internal and external security threats go unmanaged	M	11	12	▲
Information & Asset Inventory	Processes and procedures for classifying, labeling and handling information and assets are not established	L	1	4	■
	Identification and assignment of ownership for assets containing sensitive information has not been performed	L	0	1	■
Information Protection	Process for monitoring and tracking sensitive information throughout its lifecycle is not established	H	11	21	▲
	Failure to restrict collection of personal information for only necessary purposes	M	9	4	▲

Summary Notes

RETURN TO TABLE OF CONTENTS

Executive Dashboard – Business Unit View

Financial Services Example



RETURN TO TABLE OF CONTENTS

Cyber-Risk Heat Map—Retail Example

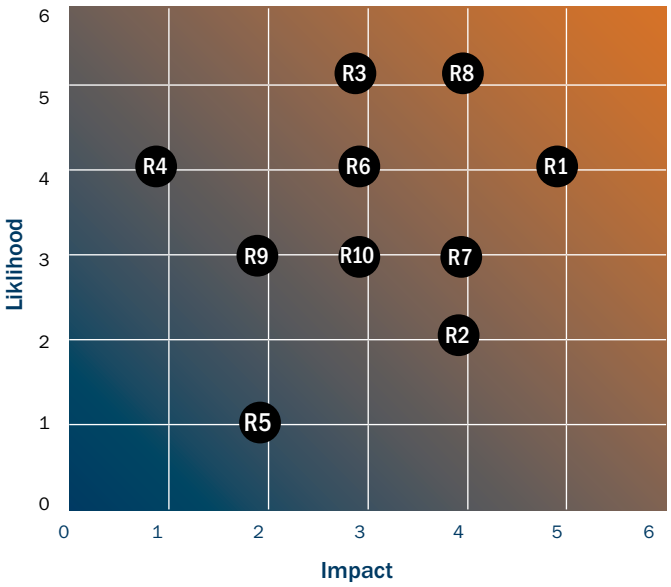
Source: KPMG

Cybersecurity Risks

Cybersecurity management and business decision making are closely related to risk management. Executives and board members need to understand and monitor the cyber risks that may hinder the organization's ability to achieve its goals. These risks are represented by key risk indicators (KRIs) that are directly derived from the organization's strategy. For example, if a retail company's strategy is to grow through increased revenue and market share on e-Commerce channels, then the downtime of online shopping sites directly affects the realization of the strategy, becoming a KRI.

Another perspective on risk may be provided via benchmarking. Executives often want to know their organization's status compared to industry peers or best practices. Benchmarks related to organizational maturity levels and framework compliance are available in the marketplace.

Top 10 Risks



Top Risks

Risk	Description	Level	Trend	Comments
R1	**Loss or alteration of intellectual property**	Very High	↑	Existing system does not allow control of administrators. Analysis for change of system in progress.
R2	**Sensitive consumer data disclosure**	Medium	↓	Inventory of repositories is at 80%. Identified repositories are compliant with risk appetite.
R3	**Unavailability of online sales channels**	High	→	Penetration test identified severe vulnerabilities in configuration. Changes in progress
R4	**Strategic information leakage**	Very High	↑	Increased impact with new business project. IT acquisition and awareness trainings in process.
R5	**Financial Fraud**	Medium	→	Recent audit findings identified failures in user management processes. Changes in progress

Source: *Feel Free Cyber Security Dashboard: Monitor, Analyse, and Take Control of Cyber Security* (KPMG Advisory N.V., 2015), p. 10. Used with permission from KPMG.

RETURN TO TABLE OF CONTENTS

APPENDIX G

Department of Homeland Security Cybersecurity Resources

The Internet Security Alliance strongly recommends that companies and other entities do not wait until after they have experienced a cyberbreach or other cyber event to contact government agencies. All organizations can benefit from proactively establishing relationships with local law enforcement and/or FBI personnel in their area, instead of initiating communication during a time of cyber emergency. What follows in Appendix G are suggestions from the Department of Homeland Security regarding the resources and processes they provide to organizations in the wake of a cyber event. It should be noted that this material was prepared in the fourth quarter of 2016 and may be subject to revision.

The Department of Homeland Security (DHS) can help organizations be more secure both before and after a cyber incident.

As an analogy, think of cyber incidents as crimes like arson, and DHS as firefighters. When arson occurs or is suspected, firefighters and police work together to determine what happened. The police are there to catch the perpetrator, but the firefighters are there to put out the fire. Like firefighters, when a cyber incident occurs, DHS is there to help. It can help companies find the adversary on their network, kick the attackers off, figure out what they've done, get the organization back on its feet again, and offer recommendations to help improve cybersecurity posture. Other law enforcement agencies focus on pursuing and catching cybercriminals.

Firefighters don't just respond to fires, and we don't just respond to incidents. Firefighters also spend a lot of time making buildings less likely to catch fire in the first place, like installing smoke detectors and inspecting buildings to make sure they comply with building codes. Similarly, DHS spends a lot of time helping organizations decrease the likelihood of a cyber incident: it promulgates cybersecurity best practices, shares information on cyber threats, and performs voluntary cybersecurity assessments.

Should an organization request DHS' help responding to a cyber incident, its identity will be kept confidential, and the information shared with us can be received as Protected Critical Infrastructure Information (PCII), which means it can't be shared with regulators or be disclosed in Freedom of Information Act requests or in civil litigation.

DHS offers the following cybersecurity resources to private-sector organizations:

Best Practices

- **Cybersecurity Framework**
  DHS encourages all companies to adopt the National Institute of Standards and Technology Cybersecurity Framework, which consists of standards, guidelines, and best practices for cybersecurity. The prioritized, flexible, repeatable, and cost effective approach of the Framework helps companies manage cyber risk. For more information, visit www.nist.gov/cyberframework.
- **Cyber Security Advisors**
  Cyber Security Advisors (CSAs) are regionally-located DHS personnel who can help prepare and protect companies from cyber threats. CSAs are located in Atlanta, Boston, Chicago, Dallas, Houston, Los Angeles, New York, and Pittsburgh. To contact a CSA, email cyberadvisor@hq.dhs.gov.
- **Risk Assessments**
  DHS offers several types of free risk assessments, which can be conducted as self-assessments or facilitated onsite by DHS personnel. These assessments range from questionnaires to actual technical penetration tests by red teams, and can be strategic or tactical. Contact a CSA to request a risk assessment for your company.

Information Sharing

- **Bulletins & Alerts**
  DHS posts alerts and bulletins regarding cyber threats, vulnerabilities, and mitigation strategies on www.us-cert.gov/ncas. To receive this information via email, email cobalt@us-cert.gov. Alerts, advisories, and other information products regarding control systems can be found on https://ics-cert.us-cert.gov/. To receive this information via email, visit https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new.
- **Information Sharing and Analysis Organizations**
  DHS recommends that all companies join or form an Information Sharing and Analysis Organization (ISAO). Like Information Sharing and Analysis Centers (ISACs), the purpose of ISAOs is to gather, analyze, and dissemi-

RETURN TO TABLE OF CONTENTS

nate cyber threat information, but unlike ISACs, ISAOs are not necessarily organized according to industry sector. The ISAO model enables more companies to share threat information with the government and with each other by offering a more flexible approach to self-organized information sharing activities that don't necessarily correspond to a specific sector. For more information, visit www.ISAO.org.

- **Automated Indicator Sharing**
  DHS' Automated Indicator Sharing (AIS) capability is a system for sharing cyber threat indicators. The intent is for companies to set up a server to share indicators with DHS' AIS server. DHS will send those indicators out to the private sector in real time in combination with indicators we receive from law enforcement, the intelligence community, and our own efforts to protect the Federal Government. Companies that submit indicators are anonymized, unless they request otherwise. Companies also get liability protection for the indicators they share with DHS through AIS. To connect to AIS, you will need to sign a short Terms of Use and set up a TAXII server. Participation in AIS is free. For more information, visit www.us-cert.gov/ais.
- **Cyber Information Sharing and Collaboration Program**
  Through our Cyber Information Sharing and Collaboration Program (CISCP), DHS and participating companies share information about cyber threats, incidents, and vulnerabilities, which allows participants to better secure their networks. CISCP provides a collaborative environment where analysts learn from each other to better understand emerging cybersecurity risks and effective defenses. For more information, visit www.dhs.gov/ciscp.
- **Enhanced Cybersecurity Services**
  DHS's Enhanced Cybersecurity Services (ECS) program is an intrusion prevention capability that helps U.S.-based companies protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers, who in turn use that information to block certain types of malicious traffic from entering customer networks. For more information, visit www.dhs.gov/ecs.

Incident Response

- To report a cyber incident to DHS, call 1-888-282-0870 or visit www.us-cert.gov/report.
- To report an industrial control systems cyber incident to DHS, call 1-877-776-7585 or email ics-cert@hq.dhs.gov.

APPENDIX H

U.S. Federal Government Cybersecurity Resources

The Internet Security Alliance strongly recommends that companies and other entities do not wait until after they have experienced a cyberbreach or other cyber event to contact government agencies. All organizations can benefit from proactively establishing relationships with local law enforcement and/or FBI personnel in their area, instead of initiating communication during a time of cyber emergency. What follows in Appendix H are suggestions from the Department of Justice regarding the resources and processes they provide to organizations in the wake of a cyber event. It should be noted that this material was prepared in the fourth quarter of 2016 and may be subject to revision.

Federal Government Resources for Cyber-Incident Reporting

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyberattacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice.

Directors should confirm that relevant members of management are aware of reporting protocols and have established relationships with local, regional and/or national offices of key agencies, as appropriate. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report a Cyber Incident to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include

- who you are;
- who experienced the incident;
- what sort of incident occurred;
- how and when the incident was initially detected;
- what response actions have already been taken; and
- who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to

- the local field offices of federal law enforcement agencies;
- their sector specific agency; and
- any of the federal agencies listed in the Key Federal Points of Contact section.

The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding

RETURN TO TABLE OF CONTENTS

to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact

- **Threat Response**
  - Federal Bureau of Investigation (FBI)
    FBI Field Office Cyber Task Forces: www.fbi.gov/contact-us/field
    - Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.

    Internet Crime Complaint Center (IC3): www.ic3.gov
    - Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.
  - National Cyber Investigative Joint Task Force
    NCIJTF CyWatch 24/7 Command Center: 1-855-292-3937 or cywatch@ic.fbi.gov
    - Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.
  - United States Secret Service
    Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): www.secretservice.gov/contact/field-offices
    - Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.
  - United States Immigration and Customs Enforcement/Homeland Security Investigations (ICE/HSI)
    HSI Tip Line: 1-866-347-2423 or www.ice.gov/webform/hsi-tip-form
    HSI Field Offices: www.ice.gov/contact/hsi
    HSI Cyber Crimes Center: www.ice.gov/cyber-crimes
    - Report cyber-enabled crime, including: digital theft of intellectual property, illicit e-commerce (including hidden marketplaces), Internet-facilitated proliferation of arms and strategic technology, child pornography, and cyber-enabled smuggling and money laundering.
- **Asset Response**
  - National Cybersecurity and Communications Integration Center (NCCIC)
    1-888-282-0870 or NCCIC@hq.dhs.gov or www.us-cert.gov/report
    - Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

APPENDIX I

Building a Relationship With the CISO

Not long ago, the notion of a senior executive whose efforts were dedicated to ensuring the company's cybersecurity was an alien concept to businesses outside of the technology arena. Times have changed; dedicated C-suite managers responsible for controlling digital risk are on the rise in medium- and large-sized companies in many different industries, a consequence of conducting business in today's always-connected world.

According to one study, 54 percent of companies worldwide employ a chief information security officer (CISO), a percentage that's higher in North America.[1] Another survey found that organizations with CISOs in seat were more likely to have dedicated incident-response teams and plans in place, and were more confident about the strength of their company's defenses against threats such as malware.[2]

As the corporate information-security function becomes more mature, a new question has arisen: How can the board effectively communicate with the security executive? The individual occupying that position is responsible for managing vast amounts of operational, reputational, and monetary risks, so a relationship of trust with the board is essential.

At NACD's inaugural global Cyber Summit, 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."[3]

Many board members now seek to establish an ongoing relationship with the CISO, and include the security executive in discussions about cybersecurity matters at full-board and/or key-committee-level meetings.

The questions and guidelines below can assist directors in establishing or enhancing a relationship with the CISO. They also can help board members improve their communications with the CISO and—more broadly—they can help boards to gain 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 that are most appropriate to the issues and circumstances at hand.

1. 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?[4]
- 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 our industry and generally? What role does the CISO play in cybersecurity budget allocation and investment decisions? Which security tools or other investments were below the "cut" line in the budget?
- What is the CISO's administrative reporting relationship (e.g., CIO, CTO, COO, head of corporate security, other)? Does it differ from the functional reporting relationship? If

[1] PwC, Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security® Survey 2016 (New York, NY: PwC, 2015), p. 26, and see Paul Solman, "Chief information security officers come out from the basement," *Financial Times*, Apr. 29, 2014.

[2] Kris Monroe, "Why are CISOs in such high demand?," *Cyber Experts Blog*, Feb. 8, 2016.

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

[4] 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).

not, what protocols are in place to ensure that the CISO has an independent channel to escalate issues and to provide prompt and full disclosure of cybersecurity deficiencies?[5]

- 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 and related control systems?
  - For example, 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?

2. Spend time with the security team before an incident occurs.

- A crisis is the wrong time for directors to get acquainted with the CISO and key staff. Board members can arrange to visit the security team and receive orientations firsthand from personnel situated on the front lines of cybersecurity, perhaps scheduled in conjunction with a regular board meeting or site visit. These sessions will provide valuable insights and learning opportunities for board members. 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.
- Directors can also ask the security executive for an assessment of their personal cybersecurity situation, 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.

3. 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/or
  - 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?

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?

[5] A 2014 study of global information security issues found that organizations with CISOs reporting outside the CIO's office have less downtime and lower financial losses related to cybersecurity incidents as compared with those who report directly to the CIO. See Bob Bragdon, "Maybe it really does matter who the CISO reports to," *The Business Side of Security* (blog), June 20, 2014.

- Does the CISO (or the information security team) have relationships with public-sector stakeholders such as law enforcement agencies (e.g., FBI, INTERPOL, U.S. Secret Service), regulatory agencies' cybersecurity divisions, the U.S. 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?

4. 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 provides a higher 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?

5. 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?
- What was our most significant "near miss" on cybersecurity in the past quarter? How was it discovered? What was our response? 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?

NACD Director's Handbook Series

Recent publications in the Director's Handbook Series:

Corporate Director's Ethics and Compliance Handbook

A Guide for Directors of Privately Held Companies

Getting Behind the Numbers

A Practical Guide: Fundamentals for Corporate Directors

The Onboarding Book

Board Dynamics: How to Get Results From Your Board and Committees

Success at the Top: CEO Evaluation and Succession

Oversight of Corporate Sustainability Activities

Governing the Global Company

The Family Business Board, Volume 1

The Family Business Board, Volume 2

RETURN TO TABLE OF CONTENTS

About the Contributors

The National Association of Corporate Directors (NACD) empowers more than 17,000 directors to lead with confidence in the boardroom. As the recognized authority on leading boardroom practices, NACD helps boards strengthen investor trust and public confidence by ensuring that today's directors are well-prepared for tomorrow's challenges. World-class boards join NACD to elevate performance, gain foresight, and instill confidence. Fostering collaboration among directors, investors, and governance stakeholders, NACD has been setting the standard for responsible board leadership for 40 years. To learn more about NACD, visit NACDonline.org.

The Internet Security Alliance (ISA) is a trade association focused exclusively on cybersecurity. ISA works with organizations like NACD and the Center for Audit Quality to promote effective enterprise cybersecurity. ISA is also a prominent force on public policy. In 2011 the House Republican Cybersecurity Task Force embraced ISA's "Cyber Security Social Contract." In 2013 President Obama reversed his previous regulatory policy and also embraced the ISA's market-based approach. ISA was the only trade group to brief the team at the Republican National Convention on cybersecurity in 2016. ISA's mission is to integrate advanced technology with economics and public policy to create a sustainable system of cybersecurity. ISA's goals are to promote thought leadership, effective policy advocacy, and sound security practices.

American International Group, Inc. (AIG) is a leading global insurance organization. Founded in 1919, today we provide a wide range of property casualty insurance, life insurance, retirement products, mortgage insurance and other financial services to customers in more than 100 countries and jurisdictions. Our diverse offerings include products and services that help businesses and individuals protect their assets, manage risks and provide for retirement security. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com and www.aig.com/strategyupdate | YouTube | Twitter: @AIGinsurance | LinkedIn.

National Association of Corporate Directors

2001 Pennsylvania Ave. NW, Suite 500
Washington DC 20006

Phone: 202-775-0509 | Fax: 202-775-4857

NACDonline.org