Cyber-Risk Oversight

DIRECTOR'S HANDBOOK SERIES

2014

NACD®
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Cyber-Risk Oversight

DIRECTOR'S HANDBOOK SERIES
2014

Prepared By Larry Clinton
President & CEO, Internet Security Alliance

NACD®
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS

Acknowledgements

We wish to thank the following individuals for their contributions to this handbook (in alphabetical order by organization); Mark Camillo, Tracie Grella, Mike Snow, and Gil Vega, AIG; Tom Quinn, Bank of NY Mellon; Joe Buonomo and Bob Gardner, DCR; Ed Batts, Jim Halpert, and Nate McKitterick, DLA Piper; Arnold Bell and Larry Trittschuh, GE; Melissa Hathaway, Hathaway Global Strategies; Tanner Doucet and Josh Magri, Internet Security Alliance; Charlie Croom, Lockheed-Martin; J.R. Williamson, Northrup Grumman; Jeff Brown, Raytheon; Gary McAlum, USAA; Marcus Sachs, Verizon; and Richard Knowlton, Vodafone.

National Association of Corporate Directors

MANAGING DIRECTOR **Peter R. Gleason**
CHIEF KNOWLEDGE OFFICER **Alexandra R. Lajoux**
RESEARCH DIRECTOR **Robyn Bew**
SENIOR MANAGER, RESEARCH **Katherine Iannelli**
RESEARCH ANALYST **Adam Lee**
RESEARCH ANALYST **Matt Abedi**
RESEARCH ANALYST **Ted Sikora**
NACD DIRECTORSHIP EDITOR-IN-CHIEF **Judy Warner**
ART DIRECTOR **Patricia W. Smith**
GRAPHIC DESIGNER **Alex Nguyen**
PUBLICATIONS EDITOR **Carolyn Fischer**
NACD DIRECTORSHIP ASSISTANT EDITOR **Jesse Rhodes**

Table of Contents

Introduction

In the past 20 years, the nature of corporate asset value has changed significantly, shifting away from the physical and toward the virtual. One recent study found that 80 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, policymakers, 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, harm to reputation, disruption to critical infrastructure, and new legal and 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. As noted above, the potential effects of a data breach are expanding well beyond information loss to include significant damage in other areas. Second, competitive pressures to deploy increasingly cost-effective business technologies often affect resource investment calculations. These two competing pressures on corporate staff and business leaders mean that conscientious and comprehensive oversight at the board level is essential.

NACD, in conjunction with AIG and the Internet Security Alliance, has identified five steps all corporate 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 risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
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 discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

Some estimates predict that between $9 and $21 trillion of global economic value creation could be at risk if companies and governments are unable to successfully combat cyber threats.

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 multi-staged, stealthy attacks. These attacks, sometimes referred to as advanced persistent threats (APTs), were first deployed against government entities and defense contractors. More recently, they have migrated throughout the economy, meaning that virtually any company is at risk.

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 goal. In other words, if a sophisticated attacker targets a company's systems, they will almost certainly breach them.

In addition, company subcontractors 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. Put simply, companies can't deal with advanced threats if they are unable to stop low-end attacks.[2]

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, 95 percent of incidents are economically motivated, according to some estimates.[3] Cyberattackers routinely attempt to steal all manner of corporate data, including personal information, credit data, business plans, trade secrets, and intellectual property. It is difficult to gauge the total damage from cyberattacks, but estimates generally put it at hundreds of billions of dollars annually.[5] Projections of future losses are even more chilling: according to a 2013 study, between $9 trillion and $21 trillion of global economic value creation in the next five to seven years could be at risk if organizations and governments are unable to adopt successful strategies to combat cyber threats.[6]

Moreover, although many smaller and medium-size companies have historically believed that they were too insignificant to be a target, that perception is wrong. In fact, the majority of cyberattacks are levied against smaller organizations[7] that have fewer security resources. In addition to being targets in their own right, smaller firms are often an attack pathway into larger organizations via customer, supplier, or joint venture relationships, making vendor and partner management a critical function for all interconnected entities.

There is general consensus in the cybersecurity field that attackers are well ahead of the corporations that have to defend themselves. Cyberattacks are relatively inexpensive yet highly profitable, and the required resources and skills are easy to acquire. It is no wonder that many observers believe cyber defense tends to lag a generation behind the attacker. It is difficult to demonstrate return on investment (ROI) for preventing attacks, and successful law enforcement response is virtually nonexistent. According to some estimates, less than 1 percent of cyberattackers are successfully prosecuted.[8]

This does not mean that defense is impossible, but it does mean that corporate boards need to ensure that management is fully engaged in developing defense and response plans as sophisticated as the attack methods, or otherwise put their company's core assets at considerable risk.

Balancing cybersecurity with profitability

Similar to other critical risks, 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 en-

Greater Connectivity, Higher Risk

Due to the immense amount of interconnection among corporate 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.

In 2014, 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.[4]

Other high-profile breaches have been not the result of outside intruders but rather employees or contractors who were given access to the company's network. In 2013, contractor Edward Snowden compromised one of the supposedly most secure organizations in the world—the U.S. National Security Agency—from the inside. A couple of 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.

hance 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 can also create major security concerns if implemented haphazardly. Properly deployed, they could increase security, but only at a cost.

Similarly, trends such as bring your own device (BYOD), 24/7 access to data, 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. These practices, however, can also dramatically weaken the security of the organization.

It is possible for organizations to defend themselves while staying competitive and maintaining profitability. Successful cybersecurity methods, however, cannot simply be "bolted on" at the end of business processes. Cybersecurity needs to be woven into corporate processes—and when done successfully, it can help build competitive advantage. One recent study found that four basic security controls were effective in preventing 85 percent of cyber intrusions:

- Restricting user installation of applications (called "whitelisting").
- Ensuring that the operating system is patched with current updates.
- Ensuring that software applications have current updates.
- Restricting administrative privileges.[9]

The study showed that not only were these core security practices effective, but they also improved business efficiency and created an immediate positive return on investment, even before considering the positive economic impact of reducing cyber breaches.[10]

As one report noted: "Recognize that effective cyber threat risk management can give your company more confidence to take certain 'rewarded' risks (e.g., adopting proper cloud computing methods) to pursue new value."[11]

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

Why Would They Attack Us?

Some organizations feel that because they are relatively small or don't hold substantial amounts of sensitive consumer data, such as credit card numbers or medical information, that they are unlikely to be the victims of a cyberattack. In fact, cyber criminals target companies of all sizes and from every industry, seeking anything that might be of value, including:

- Business plans, including merger or acquisition strategies, bids, etc.;
- Trading algorithms;
- Contracts with customers, suppliers, distributors, joint venture partners, etc.;
- Employee log-in credentials;
- Information about company facilities, including plant and equipment designs, maps, and future plans;
- Product designs;
- Information about key business processes;
- Source code;
- Lists of employees, customers, contractors, and suppliers; and
- Client data.

Source: Internet Security Alliance.

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 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 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.[12]

Cyber risk and the corporate ecosystem

Some of the highest profile data breaches to date have had little to do with traditional hacking. For example, spearphishing—a common e-mail attack strategy that targets specific individuals—is a leading cause of system penetration. Product launches or production strategies that use long, international supply chains can magnify cyber risk. Similarly, mergers and acquisitions (M&A) 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 of the most prominent recent breaches did not actually start within the target company's IT systems, but through vulnerabilities in one of their vendors or suppliers, as the examples in the sidebar, "Greater Connectivity, Higher 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." Corporations are often interconnected with elements of the national critical infrastructure, as well, raising the prospect of corporate insecurity becoming a matter of public security or even affecting national security.

As a result, boards should ensure that management is assessing cybersecurity not only as it relates to the firm's own networks but also with regard to the larger ecosystem in which the company 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.[13] 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.[14]

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?

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.[15] Yet a large percentage of boards continue to assign the majority of tasks related to risk oversight to the audit committee—even though more than half of directors believe risk oversight should be allocated to the full board, and roughly a quarter believe it ought to reside with the audit committee (Figure 1). Directors should consider whether it might be best to assign an indi-

vidual board committee the responsibility for cybersecurity oversight, or whether this responsibility is best left to the full board.

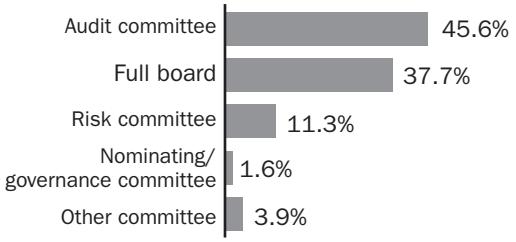
Since cyber risks and threats can change quickly, committees with designated responsibility for risk oversight—and for oversight of cyber-related risks in particular—should receive briefings on at least a quarterly basis. The full board should be briefed at least semiannually, or as situations warrant.

While including cybersecurity as a stand-alone item on board and/or committee meeting agendas is certainly a recommended practice, the issue should also be integrated into full-board discussions involving new business plans and product offerings, (M&A), new market entry, deployment of new technologies, major capital investment decisions such as facility expansions or IT system upgrades, and the like.

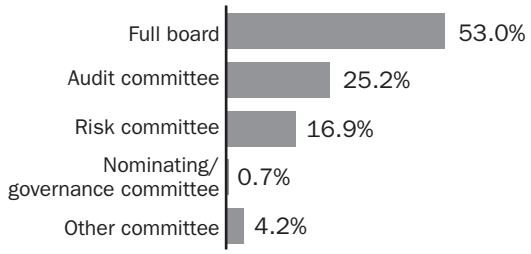
Figure 1

Allocation of Responsibility for Risk Oversight

Current allocation of responsibility:



In your opinion, where should risk oversight responsibility be allocated?



Source: National Association of Corporate Directors (NACD), *2013–2014 NACD Public Company Goverance Survey* (Washington DC: NACD, 2014).

PRINCPLE 2

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

Although the corporate liability with respect to cyberattacks is evolving, boards should be mindful of the legal risks posed to the corporation, and potentially to directors on an individual or collective basis. For example, high-profile attacks may spawn lawsuits, including shareholder derivative suits alleging 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 breaches of customer data and their consequences.

Particular areas of consideration for directors include maintaining records of boardroom discussions related to cyber risks, and determining what to disclose in the event an incident occurs.

Board minutes

Board minutes should reflect that 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. These discussions might include updates about specific risks, as well as reports about the company's overall cybersecurity program and the integration of technology with corporate strategy, policies, and business activities.

Public disclosures

In October 2011, the Securities and Exchange Commission's (SEC's) Division of Corporate 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 in recent years 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."[16]

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.[17]

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 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; and"
- A "[d]escription of relevant insurance coverage."[18]

Between 2011 and 2013, the SEC contacted some 50 companies to press for further disclosure and information regarding corporate cybersecurity and cyber incidents.[19] Additionally, the SEC stated that for 2014 its examination priorities would include, among other things, "information reported by registrants in required filings with the SEC," including on cybersecurity.[20]

While guidance from the Division of Corporate Finance is not an SEC rule or regulation, the SEC has broad power to audit, investigate, or subpoena a company pursuant to its broad "books and records" requirements. Compliance with this requirement may prove useful in a litigation context, particularly when a corporation is the victim of a cyberattack. If a company has not disclosed cyber threats pursuant to the SEC's guidance, and suffers even a modest reduction in its share price following such an incident, it risks a lengthy and costly process to resolve private lawsuits alleging inadequate public disclosure.

See Appendix A for a list of suggested questions that directors can ask management in the event of a cyber breach.

Accordingly, directors should ask management to solicit external counsel's point of view on potential disclosure considerations as a forward-looking risk factor 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.

SEC Cybersecurity Examinations

The SEC Office of Compliance Inspections and Examinations (OCIE) published a Risk Alert in April 2014 that provided additional information about its activities to assess cybersecurity preparedness among selected broker-dealer and registered investment advisor firms. The document included a sample list of requests for information in areas including cyber-risk identification, protection of firm networks and information, risks associated with vendors and other third parties, and detection of unauthorized activity. It can be viewed here.

PRINCIPLE 3

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

NACD's *Public Company Governance Survey* found that fully 87 percent of respondents reported that their board's understanding of IT risk needed improvement.[21] While "IT risk" is a broad term that encompasses many different types of risk, director confidence about their boards' understanding of cyber risk is low. Directors who participated in NACD roundtable discussions on cybersecurity late in 2013 admitted that the lack of adequate knowledge has made it challenging for them to "effectively oversee management's cybersecurity activities." Participating board members also suggested that "without sound knowledge of—or adequate sensitivity to—the topic, directors cannot easily draw the line between oversight and management," and that once in the technical "weeds," directors "find it difficult to assess the appropriate level of [the board's] involvement in risk management."[22]

See Appendix B for suggested questions to help directors assess their board's level of understanding of cybersecurity issues.

Improving access to cyber expertise

As a result, some companies are considering whether to add cyber and/or IT security expertise directly to the board via the recruitment of new directors. 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 cyber arena, directors can take advantage of other ways to bring knowledgeable perspectives on cybersecurity matters into the boardroom, including:

- Scheduling "deep dive" briefings from third-party experts, including specialist cybersecurity firms, government agencies, industry associations, etc.;
- Leveraging the board's existing independent advisors, such as external auditors and outside counsel, who will have a multi-client and industry-wide perspective on cyber-risk trends; and
- Participating in relevant director education programs, whether provided in-house or externally.

Enhancing management's reports to the board

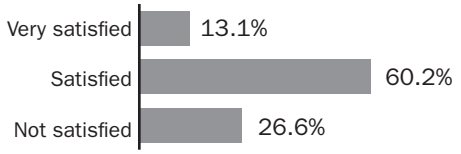
A 2012 survey found that fewer than 40 percent of boards regularly receive reports on privacy and security risks, and 26 percent rarely or never receive such information.[23] In a more recent study, only 12 percent of board members said they frequently receive briefings on cyber threats specifically.[24] Boards that do not have updated information on the company's cybersecurity situation cannot effectively oversee or approve management priorities.

NACD's *Public Company Governance Survey* (Figure 2) provides further evidence that 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 IT was rated lowest, with more than one-third of all corporate board members reporting they didn't receive enough infor-

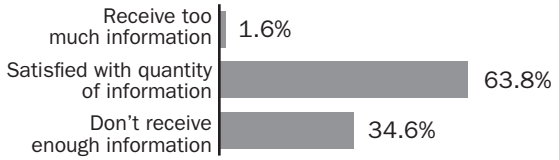
Figure 2

Director Satisfaction With Management's Reporting on IT Issues

Quality of information provided by management:



Quantity of information provided by management:



mation about IT, and only 13 percent said they were very satisfied with the quality of the information they received.[25]

See Appendix C for examples of cyber-risk reporting metrics and dashboards, and Appendix D for suggested questions directors should ask management about cybersecurity matters.

In reviewing reports from management, directors should be mindful 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.[26]

PRINCIPLE 4

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

Technology integrates modern corporations, whether workers are across the hall or halfway around the world. But, as noted earlier, many corporate structures and decision-making processes 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 modern corporate fact of life. Directors should seek assurances that management is taking an appropriate enterprise-wide approach to cybersecurity.

An Integrated Approach to Managing Cyber Risk

1. Establish ownership of the problem on a cross-departmental basis. A senior manager with cross-departmental authority, such as the CFO, 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, human resources, IT, and risk management.
3. Meet regularly and develop reports to the board. Executives should be expected to track and report metrics that quantify the business impact of cyber-threat risk management efforts. Internal audits to evaluate cyber-threat risk management effectiveness should be conducted as part of quarterly reviews.
4. 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.
5. Develop and adopt a total cyber-risk budget of sufficient resources. Cybersecurity is more than IT security, thus the budget for cybersecurity should not be exclusively tied to one department.[27]

Source: Internet Security Alliance.

The NIST Framework

In February 2013, President Barack 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.[28]

The NIST 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 risk management approach to cybersecurity. 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. Directors should set the expectation that management has considered the NIST Framework in developing the company's cyber-risk defense and response plans.

See Appendix E for the U.S. Department of Homeland Security's Critical Infrastructure Cyber Community guidelines for conversations with management about the NIST Framework.

PRINCIPLE 5

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

Total cybersecurity is an unrealistic goal. As with other areas of risk, a company's cyber-risk tolerance must be consistent with its strategy and, in turn, its resource allocation. As such, directors and management teams will need to grapple with questions including:

- **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 7) 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 against 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.[29] 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 and the company's asset priorities will change over time.

- **What options are available to assist us in transferring certain cyber risks?**
  Organizations of all industries and sizes have access to end-to-end solutions that can assist in mitigating and transferring some portion of cyber risk. 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 cyber breach. 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. 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.

- **How should we assess the impact of cyber events?**
  Conducting a proper impact assessment can be challenging given the number of factors involved. To take just one example, publicity about data breaches can substantially complicate the risk evaluation process. Stakeholders—including employees, customers, suppliers, investors, the press, the public, and government agencies—may see little difference between a comparatively small breach and a large and dangerous one. As a result, damage to corporate reputation and share price 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 their priorities for cyber-risk management.

Conclusion

Cybersecurity is a serious corporate risk issue affecting virtually all levels of significant business activity. 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,[30, 31] the economics of cybersecurity still favors 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 the board itself; ensure directors have sufficient agenda time and access to expert information in order to have well-informed discussions with management; and 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."[32] 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.

APPENDIX A

Questions Directors Can Ask Management Once a Cyber Breach Is Found

1. How did we learn about the breach? Were we notified by an outside agency, or was the breach found internally?
2. What do we believe was stolen?
3. What has been affected by the breach?
4. Have any of our operations been compromised?
5. Is our crisis response plan in action, and is it working as planned?
6. Is the breach considered "material information" requiring prompt disclosure, and if so is our legal team prepared for such notifications? Who else should receive notification about this breach?
7. What steps is the response team taking to ensure that the breach is under control and the hacker no longer has access to our internal network?
8. Do we believe the hacker was an internal or external actor?
9. What were the weaknesses in our system that allowed it to occur (and why)?
10. What steps can we take to make sure this type of breach does not happen again, and what efforts can we make to mitigate any losses caused by the breach?

Source: National Association of Corporate Directors (NACD), *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014).

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.
- Crisis communications advisors.
- Law enforcement agencies (e.g., Secret Service, FBI).
- Regulatory agencies.
- U.S. Computer Emergency Response Team.

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

APPENDIX B

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 comfortable that those assets were protected?
3. Are we investing enough so that our corporate operating and network systems are not easy targets by a determined hacker?[1]
4. Are we considering the cybersecurity aspects of our major business decisions, such as mergers and acquisitions, 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 future 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 directors and officers exposure if we don't carry adequate insurance?[5]
10. What are the benefits beyond risk transfer of carrying cyber insurance?[6]

---

[1] National Association of Corporate Directors (NACD), *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014), www.nacdonline.org/Resources/Article.cfm?ItemNumber=8486.

[2] Ed Batts, DLA Piper, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014, www.dlapiper.com/en-us/us/insights/publications/2014/01/cybersecurity-and-the-duty-of-care/.

[3] *Id.*

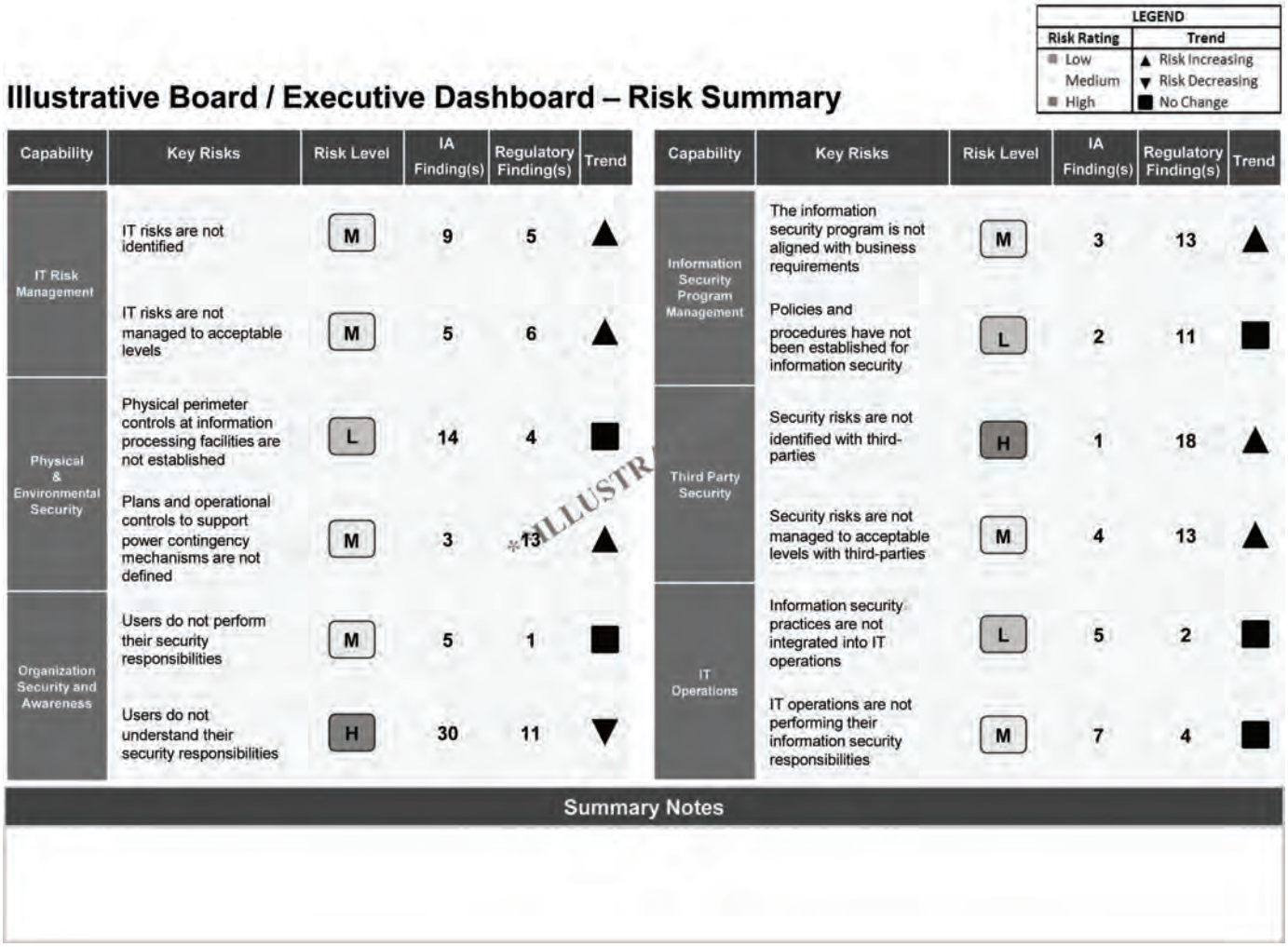
[4] National Cyber Security Alliance and Business Executives for National Security, "Board Oversight," Mar. 5, 2014, www.staysafeonline.org/re-cyber/board-oversight/.

[5] *Id.*

[6] *Id.*

APPENDIX C:

Sample Cyber-Risk Dashboards



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

Illustrative Board / Executive Dashboard – Risk Summary

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	■

Summary Notes

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

Illustrative Board / Executive Dashboard – Risk Summary (continued)

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	■
Identity & 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

Executive Dashboard – Business Unit View

Capability	Key Risk	BU#1		BU#2		BU#3		BU#4		BU#5	
		Risk Level	IA / Regulatory Findings	Risk Level	IA / Regulatory Findings	Risk Level	IA / Regulatory Findings	Risk Level	IA / Regulatory Findings	Risk Level	IA / Regulatory Findings
IT Risk Management	IT risks are not identified	L ⇧	6 ⇩	L –	4 ⇧	M ⇧	1 ⇧	L ⇩	2 –	L ⇧	1 ⇧
	IT risks are not managed to acceptable levels	L ⇩	4 ⇧	L ⇩	1 –	L ⇧	3 ⇩	L ⇧	2 ⇩	M –	1 –
Physical & Environmental Security	Physical perimeter controls at information processing facilities are not established	M ⇩	7 ⇧	L ⇩	4 –	L ⇧	1 ⇩	M ⇧	4 ⇩	L –	2 –
	Plans and operational controls to support power contingency mechanisms are not defined	M ⇩	6 ⇧	L ⇩	5 –	L ⇧	2 ⇩	M ⇧	2 ⇩	L –	1 –
Information Security Program Management	The information security program is not aligned with business requirements	M ⇩	1 –	L –	5 –	H ⇩	4 ⇩	L –	3 –	M –	3 –
	Policies and procedures have not been established for information security	M ⇩	3 –	L –	2 –	H ⇩	4 ⇩	L –	2 –	L –	2 –
Third Party Security	Security risks are not identified with third-parties	L ⇩	6 –	L ⇧	4 –	L ⇩	3 ⇩	M –	5 ⇧	L –	1 –
	Security risks are not managed to acceptable levels with third-parties	L ⇩	4 ⇧	L ⇩	3 –	L ⇧	4 ⇩	L ⇧	4 ⇩	L –	2 –

Trending
⇧ Risk is Increasing ⇩ Risk is Decreasing
– Risk is Neutral

Key Risk Thresholds
H High M Med L Low

APPENDIX D:

Questions for the Board to Ask Management About Cybersecurity

Situational Awareness

1. Were we told of cyberattacks that 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 biggest vulnerability in our IT systems?
6. If an adversary wanted to deal the most damage to our company, how would they go about it?
7. Has the company assessed the inside threat?[3]
8. Have we had a penetration test or external assessment? What were the key findings, and how are we addressing them? What is our maturity level?
9. Does our external auditor indicate we have deficiencies in IT? If so, where?

Corporate Strategy and Operations

1. What are leading practices for cybersecurity, and where do our practices differ?
2. Do we have an appropriately differentiated strategy 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?
4. Do we have a systematic framework, such as the NIST Framework, in place to address cybersecurity to assure adequate cyber hygiene?
5. Where do management and our IT team disagree on cybersecurity?
6. Do the company's outsourced providers and contractors have cyber controls and policies in place and clearly monitored? Do those policies align with the 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 of an increasingly mobile workforce?

Incident Response

1. How will management respond to a cyberattack?[5] Is there a validated corporate incident response plan?[6] Under what circumstances will law enforcement and other relevant government entities be notified7
2. For significant breaches, is our communication adequate as information is obtained regarding the nature and type of breach, the data impacted, and 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 those events be disclosed to investors?

---

[1] National Cyber Security Alliance and Business Executives for National Security, "Board Oversight," Mar. 5, 2014, www.staysafeonline.org/re-cyber/board-oversight/ [hereinafter National Cyber Security Alliance].

[2] Ed Batts, DLA Piper, "Cybersecurity and the Duty of Care: A Top 10 Checklist for Board Members," Jan. 23, 2014, www.dlapiper.com/en-us/us/insights/publications/2014/01/cybersecurity-and-the-duty-of-care/ [hereinafter Batts].

[3] National Cyber Security Alliance, *supra* note 1.

[4] Batts, *supra* note 2.

[5] National Cyber Security Alliance, *supra* note 1.

[6] *Id*.

[7] *Id*.

[8] *Id*.

APPENDIX E

Critical Infrastructure Cyber Community Leadership Team Agenda

The U.S. Department of Homeland Security's Critical Infrastructure Cyber Community recently produced an agenda designed to help facilitate conversation about cybersecurity with organizational leadership. These practices can be used by the board to set expectations for senior management. Boards will want to ensure that their management team can follow and communicate these practices in dealing with cybersecurity issues throughout the enterprise, and can assist in conversations about how to best implement the NIST Framework.

1. **Overview of cyber threat:** Be able to communicate your organization's current cyber-threat environment clearly and in layman's terms. This strategy is important for being able to project your understanding of the organization's cyber environment on executive members of the leadership team who may not have an information technology background.

2. **Understanding risk:** Facilitate a discussion about how your company uses information technology to support your core business functions, how you allocate cybersecurity resources, and how you maintain and improve your state of preparedness. This includes discussing and defining the company's most important values or goals, and what information security vulnerabilities pose the greatest threat to these values.

3. **Discuss the state of existing company security plans:** When did you first develop your plans, and when did you last update them? Do these plans address cyber-risk management and physical risk management? Do they address the questions in the sections above?

4. **Next steps:** After discussing the current state of cybersecurity strategies within the organization, the next steps include defining what areas are high priority and need immediate attention, and what items are necessary to handle in the short, medium, and long term. It is also important at this stage to discuss how often the leadership team will meet to discuss cybersecurity.

5. **Discussion of government resources:** Discuss which cyber-risk management resources would be beneficial to your company. These might include:
    a. Cyber threat and risk information sharing and collaboration.
        i. HS Enhanced Cybersecurity Services (ECS), DHS Cyber Information Sharing and Collaboration Program (CISCP).
    b. Evaluation of cybersecurity capabilities and operational resilience.
        i. DHS Cyber Resilience Review (CRR).

Source: U.S. Department of Homeland Security, "C3 Voluntary Program Leadership Team Agenda." For more on the Critical Infrastructure Cyber Community, see www.us-cert.gov/ccubedvp.

Endnotes

[1] Ocean Tomo, "Intangible Asset Market Value," April 2011, www.oceantomo.com/productsandservices/investments/intangible-market-value.
[2] Verizon RISK Team et al., *2013 Data Breach Investigations Report*, March 2013, www.verizonenterprise.com/DBIR/2013/download.xml [hereinafter Verizon RISK].
[3] Help Net Security, "Cybersecurity Concerns Becoming a Boardroom Issue," Mar. 6, 2014, www.net-security.org/secworld.php?id=16482.
[4] Nicole Perlroth, "Hackers Lurking in Vents and Soda Machines," *New York Times,* Apr. 7, 2014.
[5] McAfee and the Center for Strategic and International Studies, *The Economic Impact of Cybercrime and Cyber Espionage*, July 2013, www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.
[6] Tucker Bailey et al., "The Rising Strategic Risks of Cyberattacks," *McKinsey Quarterly*, May 2014, www.mckinsey.com/insights/business_technology/the_rising_strategic_risks_of_cyberattacks.
[7] Verizon RISK, *supra* note 2.
[8] Robert M. Regoli et al., *Exploring Criminal Justice: The Essentials* (Burlington MA: Jones & Bartlett Learning, 2011), 378.
[9] AFCEA Cyber Committee, *The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment*, Oct. 2013, www.afcea.org/mission/intel/documents/EconomicsofCybersecurityFinal10-24-13.pdf [hereinafter *The Economics of Cybersecurity*]. *See also* Internet Security Alliance, *Sophisticated Management of Cyber Risk* (2013), http://isalliance.org/publications/2013-05-28_ISA-AIG_White_Paper-Sophisticated_Management_of_Cyber_Risk.pdf [hereinafter *Sophisticated Management*].
[10] *Id.*
[11] Verizon RISK, *supra* note 2.
[12] Internet Security Alliance and American National Standards Institute, *The Financial Management of Cyber Risk: An Implementation Framework for CFOs* (2010) [hereinafter *Financial Management of Cyber Risk*].
[13] National Association of Corporate Directors (NACD), *Cybersecurity: Boardroom Implications* (Washington DC: NACD, 2014), www.nacdonline.org/Resources/Article.cfm?ItemNumber=8486 [hereinafter *Cybersecurity: Boardroom Implications*].
[14] *Id. See also* KPMG Audit Committee Institute, *Global Boardroom Insights: The Cyber Security Challenge*, Mar. 26, 2014, www.kpmg.com/global/en/issuesandinsights/articlespublications/pages/aci-cyber-security-challenge.aspx.
[15] National Association of Corporate Directors (NACD), *Report of the Blue Ribbon Commission on Risk Governance: Balancing Risk and Reward* (Washington DC: NACD, 2009).
[16] Division of Corporate Finance, Securities and Exchange Commission (SEC), "CF Disclosure Guidance," Oct. 13, 2011, www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.
[17] *Id.*
[18] *Id.*
[19] Mary Jo White, Letter from the Securities and Exchange Commissioner, to the Chairman of the U.S. Senate Committee on Commerce, Science, and Transportation (May 1, 2013), www.commerce.senate.gov/public/?a=Files.Serve&File_id=7b54b6d0-e9a1-44e9-8545-ea3f90a40edf.
[20] National Exam Program, Office of Compliance Inspections and Examinations, SEC, "Examination Priorities for 2014," Jan. 9, 2014, www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf.
[21] National Association of Corporate Directors (NACD), *2013–2014 NACD Public Company Governance Survey* (Washington DC: NACD, 2013) [*Public Company Governance Survey*].
[22] *Id.*
[23] Jody R. Westby, Carnegie Mellon University, *Governance of Enterprise Security: CyLab 2012 Report*, May 16, 2012, http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf.
[24] Ponemon Institute, *Cyber Security Incident Response: Are We as Prepared as We Think?,* Jan. 2014, www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf.
[25] *Public Company Governance Survey*, *supra* note 21.
[26] Sean Martin, "Cyber Security: 60% of Techies Don't Tell Bosses About Breaches Unless It's 'Serious'," *International Business Times*, Apr. 16, 2014, http://www.ibtimes.co.uk/cyber-security-60-techies-dont-tell-bosses-about-breaches-unless-its-serious-1445072.
[27] *Financial Management of Cyber Risk*, *supra* note 12. *See also Sophisticated Management*, *supra* note 9.

[28] Executive Order No. 13636–Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11604 (Feb. 19, 2013), www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[29] *See The Economics of Cybersecurity*, *supra* note 9.

[30] Helen Domenici and Afzal Bari, "The Price of Cybersecurity: Improvements Drive Steep Cost Curve," Ponemon Institute-Bloomberg Government Study, Jan. 31, 2012.

[31] Ponemon Institute IT Security Tracking Study Estimates, Feb. 2012.

[32] *See Cybersecurity: Boardroom Implications*, *supra* note 13.

NACD Director's Handbook Series

Recent publications in the Director's Handbook Series:

A Guide for Directors of Privately Held Companies

A Practical Guide: Fundamentals for Corporate Directors

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

Board Leadership for the Company in Crisis

Corporate Director's Ethics and Compliance Handbook

Getting Behind the Numbers

The Board of Directors in a Family Owned Business

The Onboarding Book

About the Contributors

NACD's mission is to advance exemplary board leadership—for directors, by directors. We deliver the knowledge and insights that board members need to confidently navigate complex business challenges and enhance shareowner value. We amplify the collective voice of directors in setting a substantive policy agenda.

NACD was founded in 1977 as the only national membership organization created for and by directors. Today, more than 14,000 directors and key executives from public, private, and nonprofit companies rely on us for board development, resources, education, and connections.

American International Group Inc. (AIG) is a leading international insurance organization serving customers in more than 130 countries. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. 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 | YouTube: www.youtube.com/aig | Twitter: @AIG_LatestNews | LinkedIn: http://www.linkedin.com/company/aig.

The Internet Security Alliance (ISA) is a multi-sector trade association that sees cybersecurity not as an IT issue, but as an enterprise-wide risk management issue. ISA's mission is to combine technology with economics and public policy to create a sustainable system of cybersecurity. ISA is focused on three main goals, thought leadership, public advocacy and creating standards and practices that effectively promote cybersecurity. In 2008 ISA published its cybersecurity social contract which argued that traditional government regulation would be ineffective and counter-productive against the growing cyber threat. Instead, ISA proposed that government work with industry to identify effective standards and practices and motivate voluntary adoption of these standards and practices by deploying market incentives. In 2011, the ISA "social contract" was embraced by the House GOP task force on cybersecurity and in 2013 the ISA approach was adopted in President Obama's executive order on cybersecurity.

National Association of Corporate Directors
2001 Pennsylvania Ave. NW, Suite 500
Washington DC 20006
Phone: 202-775-0509 | Fax: 202-775-4857
NACDonline.org

ISBN 978-0-943176-80-2