CYBERSECURITY: BOARDROOM IMPLICATIONS

protiviti®
Risk & Business Consulting.
Internal Audit.

DENTONS

NACD®
NATIONAL ASSOCIATION OF
CORPORATE DIRECTORS

National Association of Corporate Directors
2001 Pennsylvania Ave. NW Suite 500
Washington DC 20006
202-775-0509
www.NACDonline.org

Managing Director, Peter R. Gleason
Chief Knowledge Officer, Alexandra R. Lajoux
Research Director, Robyn Bew
Research Manager, Katherine Iannelli
Research Analyst, Adam Lee
Research Analyst, Matt Abedi
NACD Directorship Editor-in-Chief, Judy Warner
Art Director, Patricia W. Smith
Graphic Designer, Alex Nguyen
Publications Editor, Carolyn Fischer
NACD Directorship Senior Editor, Cheryl Soltis Martel

Special Thanks

The National Association of Corporate Directors (NACD) wishes to thank the NACD chapters in Houston, New York City, and Washington, D.C. NACD members, as well as NACD chapter leaders, made this report possible by volunteering their time and opinions about cybersecurity risk.

Introduction

Cybersecurity has become an urgent concern for companies—regardless of size or industry. Data breaches and other cyber threats pose significant competitive, reputational, and litigation risks and require increasingly costly investments in detection and mitigation.

Cyber criminals are stealing up to a terabyte of data each day, resulting in global losses in the hundreds of billions of dollars.[1] In just four years, the average annualized cost of cybercrime to an organization has risen 78 percent. Further, the average time required to detect and respond to a cyber attack has increased by nearly 130 percent.[2]

To help board members address this critical topic, the National Association of Corporate Directors (NACD), Protiviti, and Dentons organized a series of roundtable discussions across the country. The meetings convened three diverse groups of directors with experts in the field of cybersecurity. The purpose of the discussions was to address how cybersecurity is currently challenging boards, frame the key issues of which directors should be aware, and pinpoint areas necessitating guidance with future discussions.

Cyber threats take many forms, and the response to those threats is unquestionably a management-level responsibility. As such, the roundtable discussions focused on implications for the boardroom: how directors can effectively oversee cybersecurity risk, the necessary processes and policies to protect sensitive networks, systems, and data from unauthorized access or attack, and the potential for financial and legal problems created by cyber threats.

Importance of Cybersecurity

Although the risks presented by technology are not new to the corporate arena, the dynamic nature of cybersecurity presents a unique challenge to companies and boards. The increasingly fast pace of technological change creates many targets, thus defense systems are complex and more difficult to manage and control. While new technological developments (e.g., big data, data available at third-party entities—transaction processors, law firms, etc.—cloud computing, mobile computing, new platforms and devices, workplace virtualization, among others) present opportunities for companies to create new markets and innovative business models, they may also present fresh venues for cyber attacks and employee and external party mischief.

Disclosures by affected companies of security breaches and their sources and consequences have conclusively shown that cyber attacks are not just the result of reclusive hacks seeking to make a statement. While these kinds of attacks can occur on a small scale, they are increasingly caused by far larger and more sophisticated cybercrime initiatives involving international crime syndicates and state-sponsored espionage that are playing for far higher stakes. These sophisticated intruders seek to infiltrate systems using myriad approaches (e.g., network intrusions, malware, physical attacks, social tactics, privilege misuse and abuse, etc.) and work hard to operate undetected within systems to accomplish their aims.

Most, if not all, industry sectors are exposed—from the obvious: banks, defense contractors, manufacturers, retailers, federal agencies, power companies, and the telecommunications industry—to other targets, such as: transportation companies, the hospitality industry, food services, healthcare, and professional services firms.

Legislative and Regulatory Attention

In recent years, the federal government has placed greater focus on rules and standards aimed at enhancing cybersecurity. In February 2013, the Obama administration issued an executive order calling for better cyber protections for the nation's critical infrastructure. In response, the National Institute of Standards and Technology issued a preliminary "cybersecurity framework," which was open for public comment as of late 2013.[3]

In both 2012 and 2013, Sen. Jay Rockefeller (D-WV) authored legislation (Cybersecurity Act of 2012 and Cybersecurity Act of 2013) that would impact disclosure requirements for organizations experiencing cybersecurity issues. While the 2012 bill did not pass, the 2013 bill is still in Congress.[4]

Data breaches and other cyber threats are a growing source of significant reputational damage and high-profile litigation, and state attorneys general are issuing inquiry letters to companies in industries such as financial services asking for details about their cyber defense plans.[5]

Cyber Literacy in the Boardroom

Despite the significant escalation of risks posed by cybersecurity, many boards have found it challenging to develop a comprehensive response. Generally, IT expertise is lacking at the board level. In a recent NACD study, more than three-quarters of public company respondents admitted that they personally could use more IT knowledge, and almost 90 percent felt that their board's IT knowledge could be improved.[6] Notably, however, a demand for IT experience generally has not surfaced in director recruitment. Apart from the IT industry, which has an above-average need for directors with IT expertise, this area of expertise was viewed as "most important" for just 7.8 percent of directors by companies recruiting in 2013.

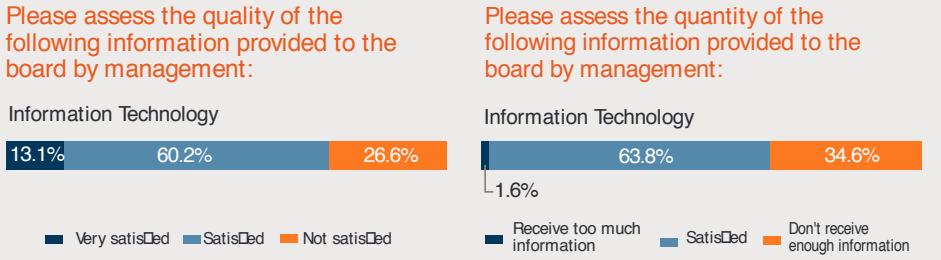
How Much Knowledge Is Enough?

Lack of boardroom expertise, according to many roundtable attendees, makes it challenging for directors to effectively oversee management's cybersecurity activities. Without sound knowledge of—or adequate sensitivity to—the topic, directors cannot easily draw the line between oversight and management. Attendees also noted that in these situations, the board may overly rely on C-suite experts, such as the chief information officer (CIO), chief technology officer (CTO), or chief security officer (CSO), who can lead the dialogue into technical areas beyond the realm of oversight. Once "in the weeds," directors then find it difficult to assess the appropriate level of its involvement in risk management. *"Whenever cyber is raised there is technical devolution,"* observed one director. *"Immediately, directors jump to management and executive level issues, and not board issues."*

A lack of technical comprehension, or even inadequate planning by management for board meetings to discuss cybersecurity, can easily result in poor communication and information sharing from the C-suite. At each roundtable, some of the directors admitted they were often unable to understand the information they receive from management, and they were not confident their board possessed a director with the necessary expertise to provide effective oversight. These views are consistent with the director community at large, as reflected in NACD's most recent survey of public company directors.

Generally, directors are significantly less likely to challenge what is presented at board meetings when they lack knowledge of the topic. In the face of this real and urgent threat to oversight, however, *"[d]irectors should not be experts,"* observed one member of the C-suite. *"Directors are hired for their judgment, not their expertise. But, how often do you challenge the CIO to tell you what you don't know?"* In many boardrooms, the rapid rise of cybersecurity has left directors struggling to find the balance between necessary comprehension and expertise.

The 2013–2014 NACD Public Company Governance Survey asked respondents to rate the quantity and quality of information received from management in five vital areas of oversight. IT was the area with the least amount of satisfaction, in both quality and quantity.



Attendees largely concluded that there is a base level of knowledge that directors should possess in order to oversee a company's exposure to cyber risk and ask the necessary probing questions. *"Cyber literacy can be considered similar to financial literacy,"* observed one director. *"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."*

Building the Board's Cyber Literacy

Directors debated, however, on the best approach to infusing boards with IT literacy. Although board turnover has increased over the last year,[7] some *"fear that it may take several decades to get the whole board cyber literate, and [boards] do not have that much time."* One director recommended that the issue *"begins with the nominating/governance committee."* This approach, according to other roundtable attendees, may prove too reactive.

In addition to board composition, directors cited a lack of available time on the agenda to discuss cybersecurity—a technical topic often requiring more than a cursory review—as a roadblock in becoming cyber literate. To address this, the board can schedule a periodic strategic deep dive, with management and/or outside experts, to educate directors on the necessary aspects of cybersecurity and the business-level risks it presents. Boards are also turning to their independent advisors, such as the external audit firm or outside counsel, to provide a perspective on how the company's cyber defense program compares with others in the industry.

Key Considerations for Board□ Management Dialogue

As directors and executives continue to grapple with threats to their companies' cybersecurity, they should ensure boardroom agendas include discussion on key information targets, threat detection and response plans, disclosure considerations, and efforts to raise awareness of cyber risks across the company—the human factor.

Attendees largely agreed that the need for policies and processes supporting cybersecurity oversight is an urgent matter. *"Most policies currently in place,"* observed one director, *"are too weak to reasonably ensure that systems are not breached."*

But where should the board begin? According to a 2012 security report from Carnegie Mellon,[8] less than one-third of boards are addressing risk management in relation to IT operations or computer and information security. *"Cybersecurity,"* noted one attendee, *"is another risk that needs to be folded into risk and strategy."* Throughout the roundtables, expert attendees stressed that directors should have a clear idea of what cyber risk is, and is not. *"Cyber is not an IT issue, but a process issue and risk management issue,"* noted one director. Keeping cyber risk out of the realm of IT also removes it from the view that cybersecurity is only a cost center to the company or, similarly, solely a technology issue.

Identifying High-Value Information Targets

The first step companies should take, according to experts, is for management to identify the balance between security and ease of usability within an organization's IT structures which is right for the company. *"The board should ask management to provide a strategy that takes care of the worst possible scenarios and focuses on protecting the organization's 'crown jewels,'"* noted an expert in cybersecurity.

"Crown jewels" refers to the highest value targets that absolutely must be protected—a breach of these assets (including sensitive information) would most significantly harm the organization. The board should ensure that management's security strategy begins with these targets and works outward.

It is important to value such assets from the perspective of the organization, as well as the perspective of external actors. To this point, the 2013 *Verizon Data Breach Investigations Report*[9] states:

> Some organizations will be a target regardless of what they do, but most become a target because of what they do. If your organization is indeed a target of choice, understand as much as you can about what your opponent is likely to do and how far they are willing to go.

When assessing potential opponents, however, companies can easily fall into several traps. First, the likely intent of the breach maybe difficult to predict, but will shape the type of information sought, and thus what should be protected. For example, if a competitor initiates the cyber attack it may be after intellectual property. If the initiator is simply a hacker trying to disrupt a firm's operations, *"the crown jewels may not necessarily be of interest."* Further, the organization's management should design the strategy under the assumption that cyber attackers will be able to breach the organization's systems. *"Do not just harden the perimeter, because hackers will get in,"* recommended several attendees. *"Accept that they can get in, and then design the strategy with the assumption they are already 'inside.'"*

Once the board has approved a strategy designed with the organization's key targets in mind, directors should work with management to define the set of relevant risks and risk thresholds that will be reported to the board. This focus should include the business, reputational and legal ramifications of cyber threats, in addition to the obvious technological considerations. Throughout the roundtable discussions, several attendees recommended using the risk factor disclosure of the proxy statement and the materiality standard as a framework: *"What are the risks you need to disclose to investors?"* noted one expert. *"Then, think about those in the cyber context."*

After identification of potential cybersecurity threats and the organization's key targets, directors should ensure that the team assembled by management is prepared and thoroughly involved in the organization's efforts to address cyber threats. The organization will face certain issues in advance of, and following, potential and occurring breaches. In addition, the legal team must be ready to advise and handle reporting around cybersecurity issues—even if none have yet arisen. Further, involvement of reasonably foreseeable harms by cyber threats may allow the organization to invoke privilege in regard to communications with the legal team and those directed by the organization's legal counsel. The successful use of this privilege could prove invaluable if and when claims and litigation arise as a result of breaches and attacks.

Formulating Cyber Threat Detection and Response Plans

Cybersecurity is not a one-time event and should not be treated as such. According to one recent study, the average U.S. company is the victim of two successful cyber attacks every week.[10] The management team, with board oversight, must constantly evaluate the company's position, the cyber threats which it potentially faces, and its ability to respond to these threats. This includes monitoring the financial and legal harm that could result from a successful breach. This evaluation should be conducted from an internal and external perspective, over time, and as the organization's business model changes.

There are multiple ways directors can ask management teams to assess the organization's position, and security of key targets. Two examples are:

- Scenario development: Directors noted the lack of available resources to sufficiently address cyber threats, protection, and breaches. Further, an unanticipated cyberattack can result in significant unplanned expenditures. As one expert noted: *"When your company is hacked, do not start spending money like a drunken sailor."* In order to provide clarity to which areas should receive the most focus, experts recommended developing a *"scenario matrix,"* which plots possible scenarios by probability and impact. Key, however, is to highlight the low probability, high-impact scenarios. According to one director: *"Do not ignore the catastrophic event scenario."*
- Detection and response plans: Given the potential impact and frequency of cybersecurity attacks, it is obvious that companies—regardless of size or industry—should have a breach response plan. But that is not enough: *"Having a breach plan is not the issue,"* said one attendee. *"Has the board discussed it? Has it been rehearsed throughout the organization?"* Further, depending on the severity and nature of the breach and the industry, regulatory agencies will most likely need to be alerted. Companies should therefore identify the appropriate regulators and should decide at which point those appropriate regulators should be alerted in a security breach.

Disclosure Considerations

In 2011, the Securities and Exchange Commission (SEC) staff issued guidance on the obligations of public companies to disclose cybersecurity risks and cyber incidents. Advice from the SEC Division of Corporation Finance is not a rule, regulation, or official statement. Issuers who choose to ignore this advice, however, and fail to assess and disclose material cybersecurity risks, do so at the risk of filing delays and other regulatory action, as well as increased exposure to the plaintiff bar.

Under this guidance, disclosures on cybersecurity risk should adequately describe the nature of the material risk, and how the risk affects the issuer.[11] In recent remarks,[12] Chairman Mary Jo White indicated that despite the evolving nature of technological change, disclosure of cybersecurity threats and breaches will continue to rely on the standard of materiality.

> When the Commission adopted rules decades ago requiring a description of the company's business, risk factor disclosure, and MD&A, there were no such things as smartphones, tablets, or even the internet. And, so it was not thinking about the risks presented by cybersecurity attacks or breaches.
>
> Even though cybersecurity attacks were not specifically contemplated, the disclosure requirements generally cover these risks. That is because, even in the absence of a line item requirement, the basic standard of "materiality" governs. Depending on the severity and impact of the cybersecurity attacks, disclosure is either required or not.

Examples of Appropriate Cybersecurity Disclosures

Depending on the issuer's particular facts and circumstances, and to the extent material, the SEC staff provided the following examples of appropriate disclosures:

- Discussion of aspects of the issuer's business or operations that give rise to material cybersecurity risks and the potential costs and consequences.
- To the extent the issuer outsources functions that have material cybersecurity risks, description of those functions and how the issuer addresses those risks.
- Description of cyber incidents experienced by the issuer 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.
- Description of relevant insurance coverage.

The determination of what is and is not material is a matter of judgment. For example, a risk assessment should determine whether there is material information regarding cybersecurity risks and cyber incidents that is required to be disclosed in order to make other required disclosures, in light of the circumstances under which they are made, not misleading.

The Human Factor

Leading practices and policies surrounding cybersecurity are rendered ineffective if employees are not trained in their use. *"People are the constant weakness,"* observed one director. *"Cybersecurity is a human issue. Often the biggest problems are caused by an inadvertent actor."* The actions are frequently the result of careless behavior rather than malicious—30 percent of companies experience a security incident as a result of employee activities on a social networking site.[13]

Throughout the series, participants repeatedly emphasized the need for ongoing training and consistent implementation of appropriate procedures in order to embed cybersecurity awareness into corporate culture at all levels. Successful companies *"make IT a [broad-based] issue. Data privacy and cyber security should be part of the company's brand."* The *"'human security perimeter,'"* observed one expert, *"is as important a line of defense as the 'technology security perimeter.'"*

Once clear standards and practices are established, companies must focus on employee education and awareness. A strong communications program that heightens the overall awareness of cyber risk greatly complements strong technical security controls (e.g., antivirus, antispyware, and web-filtering technology). To reduce the negative impact of cyber threats on the business, all employees should understand how the organization's commitment to security translates into specific policies and required procedures, avoid risky behavior and respond quickly once an attack has been detected.

Conclusion

Boards today must acknowledge two very important realities about cybersecurity: first, it is impossible to ensure 100 percent protection, and second, it is difficult to benchmark the organization's standing in an environment where there is very little sharing beyond what is disclosed in public reports.

Directors cannot ignore, though, the critical role they have in overseeing the organization's security against cyber attacks. Although strategies will vary based on company size and industry, there are actions every board can take. By identifying and agreeing on the organization's key targets ("crown jewels"), receiving regular reports on cyber risk, overseeing management's periodic testing of the effectiveness of cyber breach response plans, ensuring cyber awareness is embedded in tone at the top, and keeping an eye on what is coming "around the corner," directors can play a key role in improving the effectiveness of their company's cyber strategy.

Ten Questions Directors Can Ask Management in Planning for a Breach

1. How will we know we have been hacked or breached, what makes us certain or how will we find out?
2. What are best practices for cybersecurity and where do our practices differ?
3. In management's opinion, what is the biggest weakness in our IT systems? If we wanted to deal the most damage to the company, how would we go about it?
4. Does our external auditor indicate we have deficiencies in IT? If so, where?
5. Where do management and our IT team disagree on cybersecurity?
6. Were we told of cyber attacks that already occurred and how severe they were? For significant breaches, is the communication adequate as information is obtained regarding the nature and type of breach, the data impacted, and potential implications to the company and the response plan?
7. What part of our IT infrastructure can contribute to a significant deficiency or material weakness?
8. What do we consider our most valuable assets; how does our IT system interact with those assets; do we think there is adequate protection in place if someone wanted to get them or damage them; what would it take to feel comfortable that they were protected? Do we believe we can ever fully protect those assets? How should we monitor the status of their protection?
9. Are we investing enough so our corporate operating and network systems are not easy targets by a determined hacker?
10. Where can we generate more revenue and marginal profitability by making changes in IT?

Ten Questions Directors Can Ask Management Once a 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. Whom do we have to notify about this breach (materiality), whom should we notify, and is our legal team prepared for such notifications?
7. What steps is the response team taking to ensure that the breach is under control and the hacker no longer has access to the 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?

Endnotes

[1] *C/NET, Cyberattacks Account for up to $1 Trillion in Global Losses* (July 22, 2013), http://news.cnet.com/8301-1009_3-57594989-83/cyberattacks-account-for-up-to-$1-trillion-in-global-losses/.

[2] According to data from the 2013 *Cost of Cyber Crime Study* conducted by the Ponemon Institute and sponsored by HP Enterprise Security Products.

[3] National Institute of Standards and Technology, U.S. Department of Commerce, http://www.nist.gov/cyberframework/ (last updated Dec. 16, 2013).

[4] *See* Cybersecurity Act of 2013, S. 1353, 113th Cong. (2013).

[5] Dentons, *Are You Doing Enough to Prevent Cyber Attacks?: New York State Asks Life, Health, and Insurance Companies for Proof* (2013), http://www.dentons.com/en/insights/alerts/2013/june/17/are-you-doing-enough-to-prevent-cyber-attacks.

[6] According to data from *2013–2014 NACD Public Company Governance Survey*. *See* National Association of Corporate Directors (NACD), *2013–2014 NACD Public Company Governance Survey* (Washington DC: NACD, 2013).

[7] *Id*.

[8] Jody R. Westby, *Governance of Enterprise Security: CyLab 2012 Report, How Boards and Senior Executives Are Managing Cyber Risks* (Carnegie Mellon University, CyLab, May 16, 2012).

[9] Verizon, *Data Breach Investigations Report* (2013).

[10] InformationWeek, *Cybercrime Costs Skyrocket* (Oct. 8, 2013), http://www.informationweek.com/traffic-management/cybercrime-costs-skyrocket/d/d-id/1111861?

[11] Protiviti, *Protiviti Flash Report: SEC Staff Provides Guidance on Public Companies' Disclosure Obligations Relating to Cybersecurity Risks and Cyber Incidents* (Oct. 17, 2011).

[12] SEC Chairman Mary Jo White, Speech at the 2013 NACD Board Leadership Conference (Oct. 14, 2013).

[13] Protiviti, *Data Security: Social Networking and the New Human Security Perimeter* (2009), http://www.protiviti.com/en-US/Documents/POV/POV-Data-Security-and-Social-Networking-Protiviti.pdf.

2001 Pennsylvania Ave. NW
Suite 500
Washington DC 20006
Phone: 202-775-0509
Fax: 202-775-4857
www.NACDonline.org

NACD®
NATIONAL ASSOCIATION OF CORPORATE DIRECTORS