MITSloan
Management Review

The Board's Role in Managing Cybersecurity Risks

WINTER 2018
ISSUE

Cybersecurity can no longer be the concern of just the IT department. Within organizations, it needs to be everyone's business — including the board's.

Ray A. Rothrock
James Kaplan
Friso Van der Oord

Vol. 59, No. 2 | Reprint #59221 | http://mitsmr.com/2zK2Dj2

[CORPORATE GOVERNANCE]

The Board's Role in Managing Cybersecurity Risks

Cybersecurity can no longer be the concern of just the IT department. Within organizations, it needs to be everyone's business — including the board's.

BY RAY A. ROTHROCK, JAMES KAPLAN, AND FRISO VAN DER OORD

Today, more than ever, the demands posed by issues of cybersecurity clash with both the need for innovation and the clamor for productivity. Increasingly, cybersecurity risk includes not only the risk of a network data breach but also the risk of the entire enterprise being undermined via business activities that rely on open digital connectivity and accessibility. As a result, learning how to deal with cybersecurity risk is of critical importance to an enterprise, and it must therefore be addressed strategically from the very top. Cybersecurity management can no longer be a concern delegated to the information technology (IT) department. It needs to be everyone's business — including the board's.

Cybersecurity Enters the Boardroom

Network breaches have become so routine that only the most spectacular events, such as the recent breach at the credit reporting agency Equifax Inc. that affected some 143 million U.S. consumers, make headlines. Corporate boards of directors are expected to ensure cybersecurity, despite the fact that most boards are unprepared for this role. A 2017-2018 survey by the National Association of Corporate Directors (NACD) found that 58% of corporate board member respondents at public companies believe that cyber-related risk is the most challenging risk they are expected to oversee. The ability of companies to manage this risk has far-reaching implications for stock prices, company reputations, and the professional reputations of directors themselves. For example, following a 2013 data breach of Target Corp., in which the personal information of more than 60 million customers was stolen, a shareholder lawsuit charged directors and officers with having fallen short in their fiduciary duties by failing to maintain adequate controls to ensure the security of data. Although the board members were ultimately not found to be at fault, both the company's CEO and CIO resigned.

U.S. case law is based on and generally adheres to the "business judgment rule," which sets a high bar for plaintiffs pursuing legal action against board members. Similar protections for directors are in place in most "common law" countries, including Canada, England, and Australia. The Equifax cyberattack and future corporate breaches may prompt more challenges to the business judgment rule.

The view that directors are not sufficiently prepared to deal with cybersecurity risk has raised alarm bells in boardrooms nationwide and globally. Even as companies increase their investments in security, we are seeing more — and more serious — cyberattacks. If corporate boards are not sufficiently prepared to deal with cybersecurity, how will they be able to determine the effectiveness of current and proposed cybersecurity strategies? How can they know what operationally effective cybersecurity should look like and how it should evolve? And how can directors know what to ask so that they can make the right cybersecurity investment decisions?

Asking the Right Questions

In our work with dozens of companies and in surveys of executives, we have found that many directors currently cannot ask the right questions because they lack meaningful metrics to assess the cybersecurity of their business. In a 2016 poll of 200 CEOs conducted by RedSeal Inc., a cybersecurity analytics company in Sunnyvale, California, 87% of respondents reported needing a better way to measure the effectiveness of their cybersecurity investments, with 72% calling the absence of meaningful metrics a "major

challenge." Often, executives as well as directors spend too much time studying technical reports on such things as the numbers of intrusion detection system alerts, antivirus signatures identified, and software patches implemented.

To improve the situation, companies need to address two issues. First, directors need to have basic training in cybersecurity that addresses the strategic nature, scope, and implications of cybersecurity risk. Within companies, managers involved in operations, security specialists, and directors alike need to adopt a common language for talking about cybersecurity risk. Second, top management needs to provide meaningful data about not just the state of data security as defined narrowly by viruses quarantined or the number of intrusions detected, but also about the resilience of the organization's digital networks. This means having strategies to sustain business during a cybersecurity breach, to recover quickly in its aftermath, and to investigate needed improvements to the digital infrastructure. Networks constantly change, so tracking cyber risks and vulnerabilities over time and adapting accordingly is essential.

A few decades ago, when business computers were networked into systems of record, it made sense for organizations to focus exclusively on preventing outside attacks and protecting the network perimeter. However, now that computers have become systems of engagement, strategies geared toward perimeter defense are inadequate. Today's organizations have vast numbers of network connections and human-machine interactions taking place at all hours of the day and night. In this context, security strategies must extend far beyond the walls of a single organization to reflect interactions with suppliers, customers, and vendors. Networks are permeable, and the relevant question is no longer "Will the organization's cyberstructure be compromised?" but "What do we do when it is breached?" For organizations, the old challenge of detecting and neutralizing threats has expanded to include learning how to continue doing business during a breach and how to recover after one. In other words, it has expanded from security alone to security and resilience.

Increasing Resilience

Resilience is essential in any effective cyberdefense strategy. Our cyberadversaries are competent, determined attackers and only have to succeed once. Resilience assumes that attacks are immutable features of the digital business environment and that some fraction of these attacks will inevitably result in breaches. Therefore, creating sufficient resilience both to continue doing business while dealing with a breach and to recover in the aftermath of a breach is the most critical element of a contemporary cyberdefense strategy.

Resilience assumes that attacks are immutable features of the digital business environment and that some fraction of these attacks will inevitably result in breaches.

Adequate organizational resilience is about operating the business while fighting back and recovering. Maintaining this level of performance requires the ability to measure an organization's digital resilience much the way a board oversees its financial health. For board members, no fiduciary obligation is more urgent than overseeing and, where necessary, challenging how executive leadership manages the risks to the company. Managing cybersecurity risk today requires protecting the digital networks essential to conducting business by ensuring effective security and a high level of resilience in response to those inevitable cyberattacks. This can be accomplished through policy, selection of leadership, and allocation of resources. It is a whole-enterprise issue, requiring both full board engagement and superior execution by management.

The 2017-2018 survey by NACD reveals that public company board members are significantly more skeptical about their company's cybersecurity efforts than are C-suite executives. Just 37% of respondents reported feeling "confident" or "very confident" that their company was "properly secured against a cyberattack"; 60% said they were "slightly" or "moderately" confident. Other surveys, including the 2016 poll of CEOs by RedSeal, pointed to similar weaknesses. Given the disconnect between the risk levels and degree of preparedness, we believe that most companies need to become more realistic about their vulnerability.

The problem isn't a lack of investment. In 2017, worldwide spending on information security was expected to reach $86.4 billion and to further increase to $93 billion in 2018, according to Gartner Inc. However, cybercrime losses are rising at more than twice the rate of expenditure increases. Many CEOs continue to focus their attention on keeping hackers out of their networks rather than building resilience for dealing with hackers once they have broken in. Although most CEOs believe that cybersecurity is a strategic function that starts with executives, RedSeal found that 89% of CEOs surveyed treat it less as a whole-business issue than as an IT function, in that the IT team makes all budget decisions on cybersecurity.

Best Practices

Building on insights from the surveys cited above, we have developed a four-part approach to help organizations manage cybersecurity more effectively

The Board's Role in Managing Cybersecurity Risks (Continued from page 13)

and formulate digital resilience strategies. It involves educating company leadership; developing a common language for management and corporate directors to discuss cybersecurity issues; understanding the difference between security and resilience; and making both security and resilience strategic corporate imperatives.

1. Educate company leadership. Cybersecurity risk shouldn't be treated strictly as an IT issue. In terms of risk management, both security and resilience need to be managed as issues of importance to the entire enterprise. Increasingly, directors and senior management are being held accountable for the security and resilience of networks and data. Board members must therefore understand the issues at stake and accept their fiduciary responsibility for their organization's cyberdefense posture. Company leadership must have an unambiguous understanding of the key elements of security and resilience. Both management and directors need to be aware of (1) the limitations of security (no practical cybersecurity strategy can prevent all attacks) and (2) the need for resilience (strategies to sustain business during a cyberattack and to recover quickly in the aftermath of a breach).

In order to be effective, directors need sufficient knowledge to understand and approach cybersecurity broadly as an enterprise-wide risk management issue. Directors need to understand the legal implications of cybersecurity risks as they relate to their company's specific circumstances.

2. Develop a common language. Boards must have adequate access to cybersecurity expertise, and their discussions about cybersecurity risk management should be a regular part of each board meeting agenda, with sufficient time allotted. Moreover, board engagement regarding cybersecurity issues should not be restricted to yearly or semiannual reports. A proprietary 2017 McKinsey survey on chief information security officer (CISO) and board reporting found that CISOs who had less-than-productive board interactions felt they needed more time with the board to explain and examine critical issues. One CISO who responded to the survey observed that "board members have to be able to ask questions that may be perceived by others to be ignorant." No question can be considered bad or inappropriate.

Digital security specialists, like all subject-area experts, must be able to communicate effectively with board members and other leaders. Meetings with CISOs and other security professionals mean nothing if technical experts and directors are unable to understand one another. Information security executives must be capable of presenting information at a level and in a format that is accessible to nontechnical corporate directors. Ideally, assessments of cybersecurity, digital resilience, and cybersecurity budgeting should be expressed using metrics that objectively and unambiguously score issues of risk, reward, cost, and benefit. That said, directors should make themselves conversant in basic principles relevant to digital networking and security. The goal is for CISOs and other IT executives to engage in frank, mutually intelligible dialogue with the board and appropriate subcommittees. Wherever possible, IT and CISO reports should be focused on prioritized items on which the board can take action, especially those that can be addressed by the whole company.

Resilience (the ability to respond to incidents and breaches) should be prioritized over the forlorn hope of security alone as a silver bullet.

3. Distinguish between security and resilience. Companies should create a clear distinction between digital security and digital resilience. Digital security focuses on essential security measures, including providing such traditional defenses as effective antivirus and antimalware software, adequate firewalls, and employee education in safe computing practices. Digital security is, therefore, a *security* issue.

In contrast, digital resilience is a *business* issue, which relates to how the whole organization conducts business in a digital environment. For example, balancing data accessibility with the necessity of protecting customer data and intellectual property involves a trade-off between security and interactivity that affects the customer experience, customer service, customer retention, acquisition of new customers, and so on. It is therefore a *business* issue. To the degree that an element of an organization's security implementation impedes business (for example, by arbitrarily restricting access to data), it may provide adequate security. But it is a poor business practice, which makes the company more liable to fail and therefore less resilient.

In assessing the organization's strategic cybersecurity policy, the board must balance resilience against security, with priority given to resilience. Over time, your network *will* be penetrated. Therefore, resilience (the ability to respond to incidents and breaches) should be prioritized over the forlorn hope of security alone as a silver bullet. Security will not enable you to continue to conduct business during a breach. Resilience will. The board must provide necessary leadership in advocating for whole-enterprise resilience policies and practices.

4. Make security and resilience strategic business issues. Directors must set the expectation that management will establish

an enterprise-wide cyber-risk management framework with adequate staffing and budget. The board's discussions with management concerning cybersecurity risk should include identifying which risks to avoid, which to accept, and which to mitigate or transfer through insurance — as well as specific plans associated with each approach.

In concert with top management, the board should create a clear statement of its role in overseeing, evaluating, and challenging the company's digital security and resilience strategies. The statement should clearly define and assign responsibilities and must delineate the differing roles of the board and senior management. Within the board itself, cybersecurity and digital resilience must be the responsibility of all directors and not be relegated to a committee or subcommittee. Nevertheless, boards should consider assigning one cyber-savvy director to take the lead on issues of security and resilience, and, when recruiting new directors, companies should seek out people with appropriate cybersecurity expertise.

The board should continually reassess the overall budget for security and resilience and redirect investments as necessary. Given the reality that the number and seriousness of breaches are growing, it is clear that most organizations need to evaluate their cybersecurity investments more clearly and effectively. Improving the ability to measure and quantify cyber-related risks is vital to this step, because it allows cybersecurity and resilience to be evaluated for their impact on the entire business.

Ray A. Rothrock *(@rayrothrock) is CEO and chairman of RedSeal Inc.* ***James Kaplan*** *(@jmk37) is a partner in the New York office of McKinsey & Co.* ***Friso van der Oord*** *(@Frisovanderoord) is director of research at the National Association of Corporate Directors in Washington, D.C. Comment on this article at http://sloanreview.mit.edu/x/59221.*

Reprint 59221.

MITSloan Management Review

PDFs ■ Reprints ■ Permission to Copy ■ Back Issues