EY Center for Board Matters

Taking charge

How boards can activate, adapt and anticipate to get ahead of cybersecurity risk

EY

Building a better working world

Even the best-run companies will face a crisis, and in today's technology-driven environment, that crisis will likely be a cyber attack.

Whether the situation has a severe impact on a company often depends on the board's preparedness. Smart boards know that the best offense is a strong defense, and an organization's value and reputation can hinge on how well it responds to an unforeseen event.

Keeping cyber **top of mind**

Keeping cyber "top of mind" and part of overall governance

A cyber attack can erode a company's competitive advantage and shareholder value and severely damage its reputation. The advent of new technologies and an ecosystem of digital interconnectedness significantly increase a company's exposure to theft of its "crown jewels," which may include confidential customer data, intellectual property or information about corporate strategy. Cybersecurity threats are not simply an information technology (IT) challenge given the significant impact a breach can have on the overall business.

Cybersecurity is a business risk and should be incorporated into all levels of business strategy and planning.

Boards can start by taking cybersecurity out of the silo of the IT department. Because cyber risk is ubiquitous in the digital age and no company or industry is spared, boards should lead the effort by redefining cybersecurity governance and shifting the mindset about it in the entire organization. It is about transforming the culture so that cybersecurity is viewed not in isolation as an IT issue, but rather as a business risk that is both managed and integrated into the overall business strategy and operations.

Given the pervasive impact that cybersecurity can have on all facets of company operations, the full board should govern cybersecurity. Cybersecurity should be viewed in the context of an enterprise-wide risk that should be managed on an ongoing basis and given the requisite visibility by the full board. However, it is more than just putting cybersecurity on the agenda of every board meeting. It is also ensuring that cyber risk considerations are interwoven into all major discussions and decisions at the board level — whether they are about changes in the business environment or in business strategy and operations (e.g., a merger, acquisition, introduction of a new product, entrance to new markets, implementation of new technologies or software).

For example, during an acquisition, companies will perform financial due diligence on the acquiree to understand the associated business risks. But if cyber risks aren't considered, a company and its board won't fully understand the associated vulnerabilities and hazards they are likely to inherit once the transaction is complete. As organizations adapt to changes in the external business environment and their business strategy and operations, boards need to ensure that the related cybersecurity measures and related risks are adapted to accordingly.

redefine

Boards should redefine cybersecurity governance.

Activate cybersecurity and company resources

To begin addressing cyber risks, organizations need to have a solid foundation of cybersecurity. Cybersecurity knowledge is an area that both management and boards need to cultivate from an enterprise standpoint. According to EY's 2014 Global Information Security Survey, 53% of organizations note that the lack of skilled resources and cybersecurity skills is one of the main roadblocks they face today. Less than 20% of organizations have real-time insight on cyber risks, and cybersecurity tasks are generally not adequately resourced or performed by skilled people. Putting this foundation in place is not an easy task, but boards should call upon management to "activate" its resources and bridge any human capital and knowledge gaps.

While cyber crime is getting more attention in boardrooms around the globe, that interest is not translating into additional resources. Forty-three percent of survey respondents said their organization's total information security budget would stay about the same in the coming year. Another 4% said their budget would actually decrease.

Lack of executive buy-in and board oversight could cause a company to miss the necessary focus and fail to make the required investment. It is the board's responsibility to challenge management so that management is appropriately allocating resources to address cyber risks that are commensurate with the risk levels. Given that technology transcends and impacts all departments and corporate structures, boards should address whether management's cybersecurity plan has sufficient funding and incorporates a cross-functional team involving business leaders of all key departments – such as IT, finance, legal, internal audit and human resources – so that management is taking a holistic and comprehensive approach toward managing cybersecurity.

Keep cybersecurity at the core

Use a cross-functional team to focus on cybersecurity

Responses from EY's Global Information Security Survey

53% note that the lack of skilled resources and cybersecurity skills is one of the main roadblocks they face today

Less than 20% of organizations have real-time insight on cyber risks

43% say their organization's total information security budget would stay about the same in the coming year

Adapt
a dynamic approach toward cyber risk

It is not enough to activate an organization's cybersecurity and resources. Organizations change and so do the threats. Therefore, the foundation of cybersecurity must adapt to keep pace, and boards will need to adapt to these changes as they commit to incorporating cybersecurity as part of their governance responsibilities. To actively oversee cybersecurity strategy and adapt to cyber risks, all boards should work toward establishing a comprehensive cyber framework for their organizations. It starts with knowing where the threats originate and creating a framework for evaluating, prioritizing and adapting to each risk.

In our survey, 57% of respondents considered employees as the most likely source of an attack. However, for the first time, the survey found that when combining the different types of external attackers (criminal syndicates, state-sponsored attackers, hacktivists and lone-wolf hackers), these threats are increasingly significant as a potential risk source. Furthermore, as the economy becomes more digitized and the degree of interconnectedness with other parties (such as suppliers, vendors and customers) increases, so does the risk to the company. Therefore, when performing and re-evaluating its risk assessment, boards will need to continuously evaluate, balance and adapt to all risks (both internal and external) posed to the company, including those that are associated with the company's broader network or ecosystem.

To support the improved situational awareness of known and emerging cyber risks, boards need to increase their understanding of all that cybersecurity entails. Effective boards are cognizant of the range of their directors' skills and experiences, and they continuously reassess and adapt so that the current skill sets are commensurate with the company's current risk profile. It may not be necessary to add someone with IT experience to the board to address cybersecurity risk if the board can mitigate its cybersecurity "knowledge gap" in other ways. In some instances, boards are hiring their own experts to educate directors. Others are leveraging independent advisors (e.g., external counsel and external auditors) who can provide perspectives and insights on trends related to cyber risk present in the industry.

Establishing a framework

When establishing a cybersecurity framework, all boards should, at a minimum, understand what needs to be protected (the company's crown jewels) and perform a risk assessment to mitigate the following risks:

- **External attack –** such as corporate espionage or cyberterrorism
- **Internal exposure –** such as poorly trained and/or disgruntled employees and subcontractors
- **Ecosystem threats –** networks connected to third parties (such as business partners, vendors, suppliers and customers)
- **Reputational risk –** such as social media exposure

oversee

Boards should oversee the establishment of a comprehensive cyber framework.

Anticipate and get ahead: leading practices

Anticipate and be in a proactive state of readiness

Companies will likely never be able to prevent a cyber attack, so the best alternative is to be prepared with a well-integrated, enterprise-wide plan for managing cybersecurity. A company's board can help its organization move to a state of readiness against cyber threats by fostering an environment in which cyber threats are anticipated and proactively addressed through a relentless focus on the future environment. Boards need to direct management in planning for the consequences of a cyber breach and be prepared by confirming that management not only adopts an enterprise-wide plan, but also works to perfect the details of the organization's incident response plan. This enables preventive action and response mechanisms to operate smoothly and quickly. Boards should encourage management to rehearse its incident response capabilities to gain the required confidence in the organization's ability to respond effectively to cyber-related threats.

Boards need to confirm that management not only adopts an enterprise-wide plan, but also works to perfect the organization's incident response plan.

Reach out, find out and collaborate

Information can be powerful, and leading boards encourage their organizations to proactively foster relationships with the appropriate agencies (including the local FBI cyber task force) to keep informed of new and emerging trends in attack types, and in the methods, tools and techniques to deal with them beforehand. US Government agencies engage in constant surveillance and are often the first to uncover and bring cyber threats to the attention of an organization. The seriousness of cyber crime has led to greater collaboration between private businesses and public institutions, from the FBI and U.S. Securities and Exchange Commission to the U.S. Department of Homeland Security.

Several agencies have created resources to help companies. Among them is the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). In February 2014, the NIST issued the Framework for Improving Critical Infrastructure Cybersecurity (the Framework), which is the result of collaboration between the government and private sector. The Framework is a set of risk-based standards and leading practices centered around business drivers to manage cybersecurity risks. Utilizing such a framework will allow an organization to better "align its cybersecurity activities with its business requirements, risk tolerances, and resources," the Framework says.

Relying on existing standards and guidance, the Framework helps organizations manage and implement leading practices around cybersecurity risk management by providing a common language and mechanism to[i]:

- Describe their current cybersecurity posture
- Describe their target state of cybersecurity
- Identify and prioritize opportunities for improving the management of risk
- Assess progress toward the target state
- Foster communications among internal and external stakeholders

While adoption is voluntary, organizations are encouraged to use the Framework, and it is becoming the standard for identifying gaps and managing cybersecurity. Boards should ask management the following: which standards are being applied for benchmarking the security framework (e.g., NIST Framework or another acceptable security standard framework)?

Government resources, such as InfraGard and the Cyber Information Sharing and Collaboration Program (CISCP), can help companies gather information on emerging cyber threats and trends. Boards can also encourage organizations to share knowledge and coordinate cybersecurity activities with all other players (such as suppliers) in an organization's wider ecosystem. A shared solution not only tightens the protective layers in and around an organization's ecosystem but also may be much more effective than going it alone. The sharing of information across a business ecosystem in a larger group can be the secret ingredient for organizations to have a greater chance at understanding, scoping and mitigating intrusions in their networks to increase an organization's resiliency against cyber attacks.

Monitor and hold accountable

Boards are encouraged to engage in the oversight of cybersecurity programs and provide a heightened level of accountability around performance measurements relating to cybersecurity. Leading practices suggest a focus on metrics, which will help the board determine whether management is appropriately adapting to potential cyber threats and responding to them swiftly.

Metrics should focus not only on the total number of breaches but also on the success of the company's response to a breach. Among the statistics to monitor are the following:

- How many breaches were there?
- How far did hackers get into the system?
- How quickly did management address or react to the breach? Were they swift enough?
- What were the results of penetration testing on third parties?

Determining benchmarks will allow boards to assess whether responses were swift and successful and also whether identified gaps are tolerable. Boards can also consider hiring external experts to review the company's cybersecurity plans and benchmark those plans against comparable companies.

Boards can also help achieve a cultural shift and permanent behavior changes toward raising cybersecurity awareness by defining a cybersecurity performance metric that employees are measured against (such as number of breaches of information security protocols). Metrics, however, are only a part of the monitoring necessary for a company to determine its cybersecurity effectiveness. It is also important to evaluate the company's incident response plan and determine whether it includes specific roles for the board, general counsel, public officials and others.

Most organizations understand that cybersecurity is not a problem to solve but a business risk that must be managed, and the board must set the tone for confronting the challenge. The board needs to confirm that senior management recognizes cybersecurity as a leading business concern. Not only are cyber threats growing, but organizations are often not able to quickly respond to known vulnerabilities in their cyber defenses. The goalpost keeps moving, so organizations and boards will need to cope with a never-ending cycle of improvement and re-evaluation of cyber risks. Ultimately, there is no one-size-fits-all approach to managing cybersecurity risk, as each organization will have varying degrees of risk tolerance and unique cyber threats. But the common thread for all organizations is that they must view cyber threats as a risk against the entire business, requiring a well-integrated, enterprise-wide response that eventually transforms them from being an easy target to being truly prepared for an attack.

What to look for

Leading boards expect regular (e.g., quarterly) updates from the chief information officer on information security and cyber threat intelligence that is both meaningful and actionable. The report should address the following:

- **Identification.** Which are the top three to five threats that are most relevant to the organization?
- **Protection.** Which actions have been taken to mitigate these threats?
- **Detection.** What mechanisms are being used to detect incidents? What activity has been seen since the last report?
- **Response and recovery.** How did the company respond to each incident?

i. *Framework for Improving Critical Infrastructure Cybersecurity; Version 1.0, National Institute of Standards and Technology, February 12, 2014.*

Boards can raise cultural awareness of cybersecurity risks.

Contacts

Ruby Sharma
Ernst & Young LLP
+1 212 773 0078
ruby.sharma@ey.com

Mark Manoff
Ernst & Young LLP
+1 212 773 1954
mark.manoff@ey.com

Download the Flipboard app on your mobile device and search for the Center for Board Matters to access current articles on board and governance topics.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About the EY Center for Board Matters
Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters is committed to bringing together and engaging with boards, audit committee members and investors to exchange ideas and insights. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content and practical tools and analysis to boards, audit committees, institutional investors and others interested in governance topics.

SCORE no. CF0135

BSC No. 1503-1410577MW

ED None

This publication and other EY board and audit committee resources are available online at ey.com/boardmatters.