TONE at the TOP®

Providing senior management, boards of directors, and audit committees with concise information on governance-related topics.

Issue 106 | August 2021

Confronting the Cybersecurity Monster

Cyber risk affects organizations of all sizes and in all industries, and it appears to be here to stay. One survey of global boards and executives ranked cyber threats as a top ten risk in 2021, and respondents expect them to be a major risk in 2030, as well. Indeed, global cybercrime is expected to jump 15% per year, with its annual impact predicted to hit $10.5 trillion by 2025, according to Cybersecurity Ventures. The cyber research company calls it the "greatest transfer of economic wealth in history."

Cybersecurity events may take the form of ransomware, attacks on remote work resources, supply chain attacks, phishing, or any number of other criminal practices. They can hobble a company, wipe out significant enterprise value, and subject it to liability or publicity that damages its reputation. The costs of a data breach are high and growing, averaging $4.24 million in 2021, up almost 10% in one year, based on IBM data.

What's more, the COVID-19 pandemic has only created new vulnerabilities that have yet to be fully understood or addressed.

Managing the Dangers

With so much at stake, there are a number of steps that boards can take to enhance their oversight of cyber risks. Throughout the process, internal audit can serve as a critical partner. Working in collaboration with the organization's cybersecurity experts, the internal audit team can provide objective verification that the organization's plans are being executed as intended and that they are adequate to the task. "They can tell the board whether there is a large exposure or a false sense of security," said Sandy Pundmann, CIA, a retired senior partner at Deloitte Risk and Financial Advisory.

There are various board strategies to help address cyber risk. Pundmann and others recommend that boards maintain a keen grasp of their organizations' cyber-risk profile, embrace their oversight role, and practice healthy skepticism to ensure they have a clear-eyed understanding of strengths, weaknesses, and vulnerabilities.

Establish oversight roles and schedule regular updates. While fewer than 10% of boards today have a dedicated cybersecurity committee led by a qualified board member, that number is expected to rise to 40% by 2025, according to a Gartner, Inc. survey. The expected increase may be driven by the expansion of digital business during the pandemic, and the embrace of remote work and its additional potential risks.

About The IIA

The Institute of Internal Auditors, Inc. is a global professional association with more than 200,000 members in more than 170 countries and territories. The IIA serves as the internal audit profession's chief advocate, international standard-setter, and principal researcher and educator.

The IIA

1035 Greenwood Blvd.
Suite 149
Lake Mary, FL 32746 USA

Complimentary Subscriptions

Visit www.theiia.org/Tone to sign up for your complimentary subscription.

Reader Feedback

Send questions/comments to Tone@theiia.org.

Today, responsibility for cybersecurity oversight may be difficult to pinpoint because it is often dispersed among management and various committees, Pundmann said. One committee should be assigned responsibility and should discuss the topic at every meeting, she added. Cybersecurity should also be on the full board's agenda a minimum of twice a year.

Recognize the threat level. Cybersecurity is more than an IT issue. "Whether it is in advance of or during an incident, you should not just leave [cybersecurity] to the chief information officer and the technical team," said John Noble, former director of the United Kingdom's National Cyber Security Centre, in a McKinsey podcast. "Leaders need to decide how to manage the tensions between usability, security, and cost, and that is very much where we need the board challenging and testing processes."

Dive deeper. Boards should be aware of whether their organizations are regularly evaluating and enhancing their cyber risk assessments. The internal audit team is often called upon to perform an initial assessment or project, perhaps an attack and penetration audit, but that's only a first step, Pundmann warned. Companies need a multifaceted strategy to prevent, detect, and respond to cyber events. The effort should include an assessment of the ongoing steps the company is taking to understand attacks, the effectiveness of the measures being undertaken, how incidents and responses are monitored, and the mechanics and success of the company's response. The full strategy assessment can start at the committee level, but it should be discussed by the full board, she said.

As a Deloitte publication noted, the first line against cyber risk is made up of business units and IT, which address risk in their daily decisions and operations. The organization's second line is information and technology risk management leadership, who take on governance and oversight. The internal audit function is increasingly the third line, conducting an independent review of security measures and performance.

Understand what sets this risk apart. Organizations and their boards are familiar with risks, but cybersecurity is different for a couple of reasons. First, it is highly specialized and the threats are ever-changing, putting them beyond the expertise of many board members. Second, internet use is pervasive across most organizations, so the risks and their impact are multifaceted and complex. "Enterprise access to the internet is fundamental to delivering value, and all those transactions that rely on access to the internet are inherently unsafe," said one participant in a panel discussion of the Cyber Risk Director Network. "That's not true of any other aspect of risk that boards deal with."

QUESTIONS FOR BOARD MEMBERS

- How often does the board receive updates on the organization's cybersecurity threats and the steps being taken to address and manage cyber risks?
- Is the organization tackling cybersecurity as an enterprise risk issue and not exclusively as an IT concern?
- Does the board take a proactive role in monitoring cyber risks or does it assume all is well unless told otherwise?
- Does the board have a dedicated cybersecurity committee? If not, does another committee, such as the audit committee, have oversight responsibility for cybersecurity?

Get a real-life example. In a tabletop exercise, *which can be run by internal audit, other management, or outside party,* the board and management can oversee a simulated attack to determine how the organization responds, how investors are notified, and how customers or business partners are affected. (Pundmann even worked with one board that requested that only the CIO and CEO were aware the situation was simulated, to make the exercise as realistic as possible.) Once the organization has assessed its response, the board can receive an update on changes that have been made or are under way.

Internal audit also can be a pivotal player in another valuable exercise: A maturity model visualization, which offers a high-level enterprise view of cyber risks and compares where the organization is to where it should be, all in a layperson's terms. Because it's not possible to monitor and address all risks, these exercises can also help clarify which targets are the most critical so that the organization can enhance prevention and detection in those areas, Pundmann said.

Don't let risks take you by surprise. As the embrace of technology expands, so do the risks associated with unfamiliar emerging technologies. Even a new ERP system can pose security challenges that should not be missed, Pundmann noted. Many companies mistakenly wait until there's trouble with a new system before planning how to deal with issues. "Make sure you have a security plan from the beginning for your cyber and control strategy," she said.

Organizations involved in mergers and acquisitions can also face new vulnerabilities. "If you are acquiring a company, ask what risks you are taking on as you connect your businesses," she advised. Companies working with supply chains or other third parties may also be exposed to risks from those sources. In addition, in the compliance arena, organizations should be aware of relevant regulations, such as the Securities and Exchange Commission rules on cybersecurity disclosures.

Leveraging Internal Audit Resources

Cyber threats can be daunting, but internal audit can provide a unique and independent perspective on the organization's risks and the best ways to address them. Boards that are proactive in their monitoring of cybersecurity issues and fully leverage the value that internal audit can offer should be in a better position to effectively address cybersecurity risks.

WHAT IS YOUR BOARD MISSING?

60% of organizations don't have a head of cybersecurity who sits on the board or at executive management level.

59% of organizations say that the relationship between cybersecurity and the lines of business is at best neutral, to mistrustful or nonexistent.

20% of boards are extremely confident that the cybersecurity risks and mitigation measures presented to them can protect the organization from major cyberattacks.

36% of organizations say cybersecurity is involved right from the planning stage of a new business initiative.

Source: *"The Risky Six: Key Questions to Expose Gaps in Board Understanding of Organizational Cyber Resiliency,"* IIA Global and EY, March 30, 2021.

[1] *Executive Perspectives on Top Risks for 2021 and 2030*, Protiviti and NC State University's ERM Initiative, 2021.
[2] *"Cybercrime to Cost the World $10.5 Trillion Annually by 2025,"* Steve Morgan, *Cybercrime Magazine*, November 13, 2020.
[3] *Cost of a Data Breach Report*, IBM, 2021.
[4] *"Gartner Predicts 40% of Boards Will Have a Dedicated Cybersecurity Committee by 2025,"* Gartner press release, January 28, 2021.
[5] *"Boards and Cybersecurity,"* McKinsey and Company podcast, February 2, 2021.
[6] *"Cybersecurity and the Role of Internal Audit: An Urgent Call to Action,"* Sandy Pundmann, Deloitte, 2017.
[7] *"Cybersecurity: An Evolving Governance Challenge,"* Harvard Law School Forum on Corporate Governance, March 15, 2020.
[8] *"Commission Statement and Guidance on Public Company Cybersecurity Disclosures,"* Release Nos. 33-10459; 34-82746, Securities and Exchange Commission, February 26, 2018.

Quick Poll Question

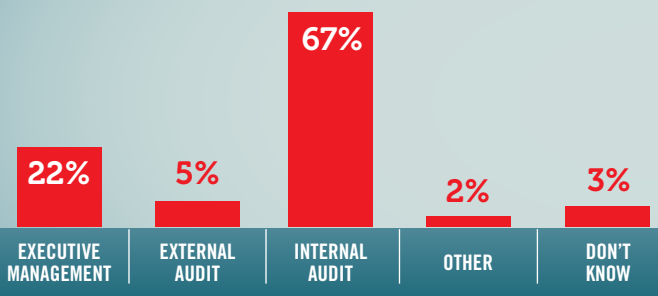
Does your board have a member with cybersecurity expertise?

- ❑ Yes
- ❑ No
- ❑ Don't know

Visit www.theiia.org/Tone to answer the question and learn how others are responding.

QUICK POLL RESULTS

Who does the board rely on primarily to provide assurance on the effectiveness of risk management and internal control?



Source: Tone at the Top June 2021 survey.