TONE at the TOP®

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

Issue 113 | October 2022

Mitigating Cyber Threats

Cybersecurity has become a permanent fixture in the modern risk landscape, and boards face increasing pressure to provide proper oversight of a threat that is multifaceted and constantly evolving. A total of 70% of board directors called cybersecurity "a strategic, enterprise risk" in an NACD Board Survey.[1] A wide range of issues fall under the cybersecurity umbrella — all are critical concerns, including privacy protection; ransomware, malware, and denial-of-service or phishing attacks; inadequate cybersecurity policies; and incident response and recovery plans, to name a few.

Organizations are also facing new regulations that call for them to report on breaches they have experienced. The Cyber Incident Reporting for Critical Infrastructure Act[2], for example, requires reporting that would allow the federal Cybersecurity and Infrastructure Security Agency to provide assistance to victims during cyberattacks, to identify trends, and to share information with other potential victims. The Securities and Exchange Commission has also proposed regulations[3] that would standardize disclosures related to public company cybersecurity risk management, strategy, governance, and incident reporting.

Internal audit, which provides organizations with independent, objective assurance and advice, can be a powerful resource for boards in addressing cyber risks. According to a PwC report[4], "many companies leverage internal audit to review cyber processes and controls, including resilience and response."

Steps to Enhanced Security

As boards consider the cybersecurity threats they face, there are a number of areas where internal audit can make a difference.

Recognizing the risk. Cyber threats have moved to the top of companies' risk rankings. "The growing sophistication and variety of cyberattacks continue to wreak havoc on organizations' brands and reputations, often resulting in disastrous financial impacts," according to *OnRisk 2022*[5] from The Institute of Internal Auditors (IIA). The report, which is based on interviews with board members, C-suite executives, and chief audit executives (CAEs), identified cybersecurity as the top risk this year.

Unfortunately, some company leaders may not fully recognize the threat. In the OnRisk report, of particular concern was the gap between the risk relevance assigned to cybersecurity by CAEs, board members, and executive management. While 97% of CAEs rated cybersecurity as a highly relevant risk to their organization (rating it at 6 or 7 on a 7-point scale), only 87% of board members did so and only 77% of C-suite executives.

The strong relevance rating among CAEs suggests their high level of awareness of cybersecurity issues. That's not surprising, given internal audit's holistic knowledge of an organization. As boards seek to leverage and improve risk assurance beyond financial and compliance risks, they can turn to internal audit to help describe cybersecurity concerns and quantify their potential impact. This can include spotlighting failures in risk coverage, monitoring emerging risks, and making the best use of technology tools in cybersecurity efforts.

Leveraging the value of the Three Lines Model. The IIA's Three Lines Model[6] enables organizations to identify structures and processes that best assist the achievement of objectives and that facilitate strong governance and risk management, including over cybersecurity. The Three Lines Model identifies key roles played by:

- The governing body, which is accountable to stakeholders for organizational oversight.
- Management, which acts to achieve organizational objectives.
- Internal audit, which provides independent and objective assurance on the achievement of those objectives.

Research has shown that cooperation among the three lines has a positive impact on the effectiveness of cybersecurity risk management. According to an article in the *ISACA Journal*[7], internal audit can offer valuable assurance and identify threats and vulnerabilities. This can include identifying cybersecurity trends and stakeholder expectations, making an initial cyber risk assessment, and defining effective audit criteria. In reporting and advising on their findings, "auditors can significantly help the [board of directors] exercise its oversight," the article states.

Ensuring internal audit's input is optimized. In many organizations, audit committees are responsible for addressing all types of risks, including cyber threats.[8] However, some assign cyber concerns to other committees, for a number of reasons. Depending on the size and industry of the organization and the threats it faces, the committee charged with overseeing cyber issues may be a separate cybersecurity committee, a risk committee, a technology committee, the nomination and governance committee, or another committee. Boards may determine that the audit committee already has a full plate or that it may not have the expertise necessary for oversight of cyber concerns, among other reasons.

Internal audit typically reports to the audit committee, but the organization may miss out on valuable cyber risk recommendations and assurance if internal audit does not also offer reports to any separate committee that is charged with cybersecurity. Having this relationship with whichever committee oversees cyber issues ensures that internal audit's insights are understood and effectively acted upon.

Identifying hidden threats. Boards may be surprised by the number of seemingly small oversights that can damage cybersecurity efforts and potentially lead to disaster. Internal audit can offer insights to help boards determine how well their organization's audit plan is able to identify overlooked threats and spot emerging risks. According to a Deloitte report[9], just a few of the cyber threats that management typically underestimates include:

- The range of former employees who can still log on to the system and the number of third-party vendors who have access to corporate systems. In both cases, companies may have little idea how many unidentified and unauthorized outside users can gain entry.

About The IIA

The Institute of Internal Auditors, Inc. is a global professional association with more than 218,000 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 401
Lake Mary, FL 32746 USA

Complimentary Subscriptions

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

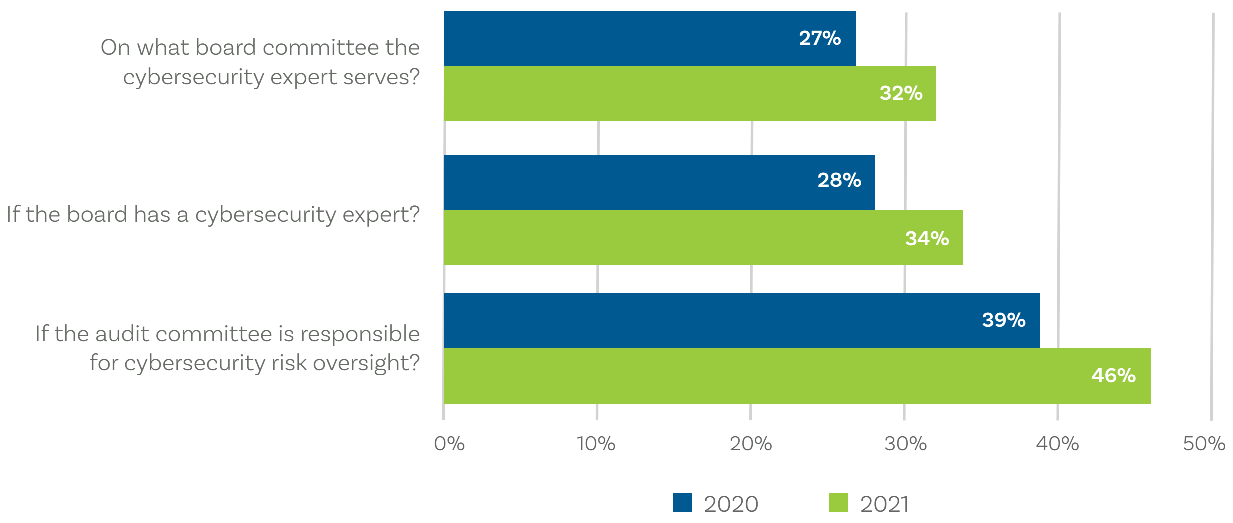
Reader Feedback

Send questions/comments to Tone@theiia.org.

QUESTIONS FOR BOARD MEMBERS

- Are we making the best use of internal audit insight and advice in our strategic planning related to cybersecurity?
- Have we adequately staffed and funded cybersecurity efforts?
- Has the organization defined its risk tolerance when it comes to cybersecurity in financial terms?
- Is a specific committee assigned oversight of cybersecurity?
- Do directors understand the company's procedures in case of a cyber breach and know their own role if it happens?

How Many S&P 500 Companies Disclose:



Source: 2021 Audit Committee Transparency Barometer, Center for Audit Quality, November 2021.

- The number of cloud accounts the company uses. More engagement in the cloud can leave more openings for cyberattacks. The Deloitte report recommends that organizations ask cloud providers about infrastructure resilience, service downtime, performance, and other metrics, as well as about regulatory compliance and independent controls assessments.
- The actual total number of cyber breaches the organization has experienced. Counterintuitively, if the company has experienced few cyberattacks, that may be a warning sign that incidents simply aren't being detected. The internal audit team can help ensure these types of warning signs are being monitored.

Addressing concerns in business partner relationships. Gartner predicts[10] that by 2025, 60% of organizations will consider cybersecurity risk when engaging in third-party transactions and business engagements. Today, only 23% of security and risk management leaders monitor third-party cybersecurity exposure in real time, and they may limit their screening to immediate vendors and suppliers rather than their entire supply chain.

Once again, audit leaders, C-suite executives, and board members are not in sync on their opinions, according to OnRisk 2022. While CAEs rated organizational capability in this area at 37%, executives believe it stood at 53% and directors at 57%. Lower CAE confidence in this area likely stems in part from the higher relevance rating they assign to this risk, which was 17 points higher than directors' rating (77% vs 60%).

In any case, boards should ensure they gain the full value of internal audit's input and experiences in this area. Because internal audit works with teams throughout the organization, it can alert the board to cyber risks associated or identified with a particular vendor or across the entire supply chain. When the organization's business partners want reassurance about the reliability of its cybersecurity safeguards, internal audit can provide the kinds of data and assurance they are seeking.

Optimizing Resources

As organizations wrestle with daunting cybersecurity concerns, they will need to optimize all their existing resources. Boards can improve their company's security by understanding and taking advantage of the value that internal auditors can bring throughout the organization by identifying opportunities for enhancing efficiencies and effectiveness.

Endnotes

1 Principles for Board Governance of Cyber Risk, National Association of Corporate Directors, Internet Security Alliance, and World Economic Forum, In Collaboration with PwC, March 2021.

2 https://www.cisa.gov/circia

3 https://www.sec.gov/rules/proposed/2022/33-11038.pdf

4 Overseeing Cyber Risk: The Board's Role, PwC, January 2022.

5 OnRisk 2022: A Guide to Understanding, Aligning, and Optimizing Risk, The Institute of Internal Auditors, 2021.

6 The IIA's Three Lines Model: An Update of the Three Lines of Defense, The Institute of Internal Auditors, July 2020.

7 "How Effective Is Your Cybersecurity Audit?," Matej Drašček, et al., ISACA Journal, June 1, 2022.

8 "Cybersecurity: An Evolving Governance Challenge," Harvard Law School Forum on Corporate Governance, Phyllis Sumner, et al., March 15, 2020.

9 Internal Audit: Risks and Opportunities for 2022, Deloitte, 2021.

10 Predicts 2022: Cybersecurity Leaders Are Losing Control in a Distributed Ecosystem, Sam Olyaei, et al., Gartner, January 24, 2022.

Quick Poll Question

What board committee is charged with overseeing cybersecurity risk management for your organization?

○ Audit committee

○ Cybersecurity committee

○ Technology committee

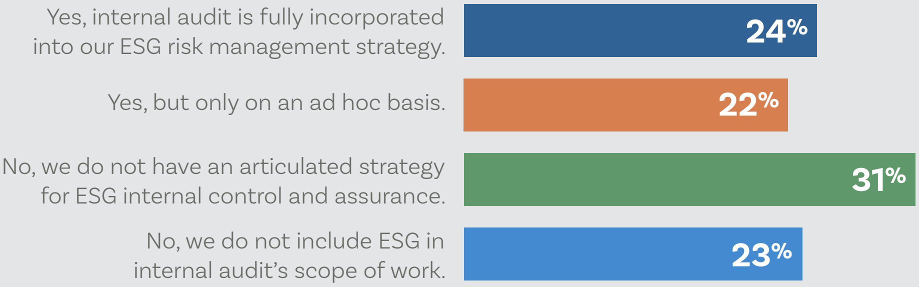
○ Nomination and governance committee

○ Other

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

QUICK POLL RESULTS

Does your organization leverage internal audit for ESG assurance?



Yes, internal audit is fully incorporated into our ESG risk management strategy. 24%
Yes, but only on an ad hoc basis. 22%
No, we do not have an articulated strategy for ESG internal control and assurance. 31%
No, we do not include ESG in internal audit's scope of work. 23%

Source: Tone at the Top June 2022 Survey.