TONE at the TOP®

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

Issue 119 | October 2023

New SEC Cybersecurity Disclosure Rules: *What Boards Must Do to Get Up to Speed*

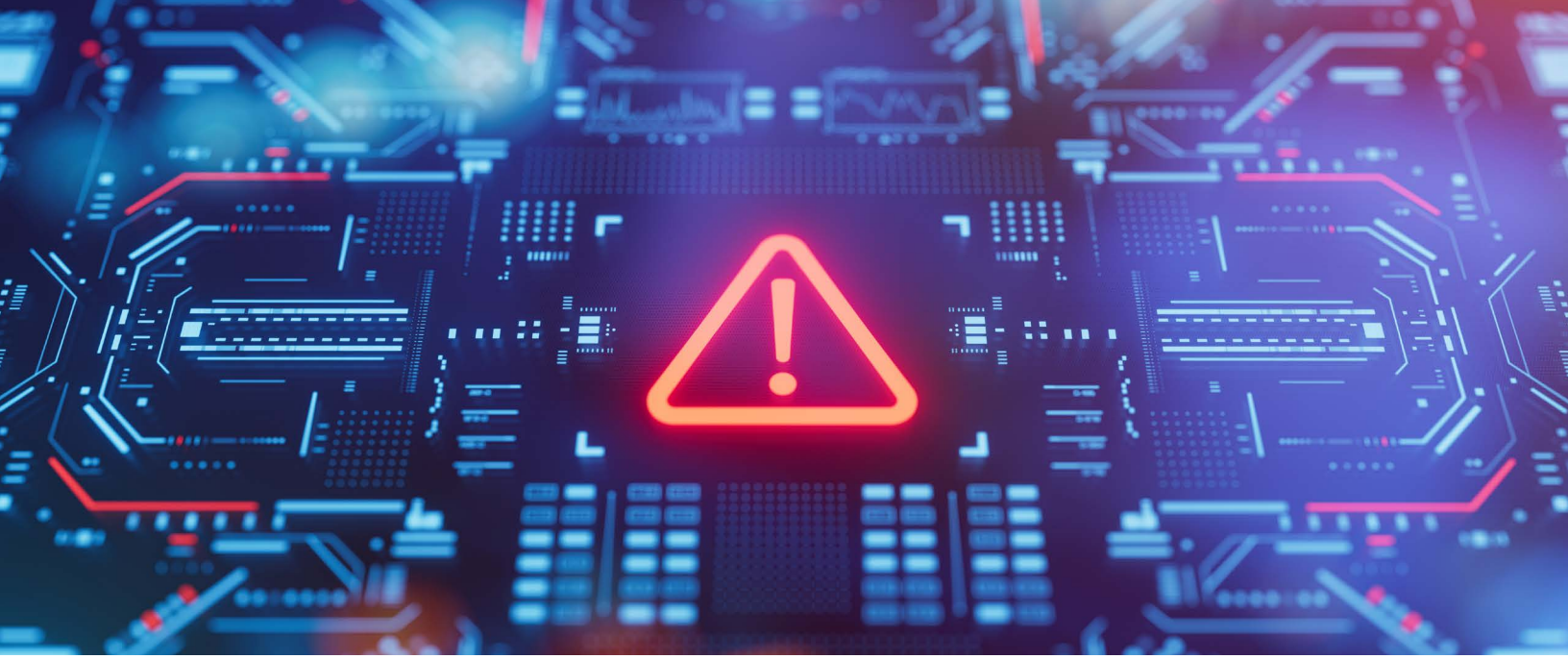
The US Securities and Exchange Commission's new cybersecurity disclosure rules further elevate the importance of vigorous governance over this ubiquitous risk. Given the rules' recent finalization, "publicly traded companies of all sizes are now in a race to comply ahead of the specified deadlines, which are looming," an NACD article noted.[1] Understanding the new rules' impacts and taking steps to ensure compliance should be a top priority for organizations. This issue of Tone at the Top examines the new directives and discusses key contributions that internal audit can make in a company's cybersecurity efforts. It also highlights new responsibilities and other important considerations for board members.

A Growing Threat

Cybersecurity is about protecting an organization's information resources, including computers, network devices, software, and data, from unauthorized access, disruption, or destruction. Yet, with each technological advancement, scammers find new ways to launch cybersecurity attacks, making cyber risk a significant consideration for any enterprise.

The costs of cyber breaches can be devastating: Nearly 60% of private sector cybersecurity leaders who responded to a Cisco study reported experiencing a cybersecurity incident within the last 12 months, and for 41% of those affected the cost was at least $500,000.[2] In addition to any direct financial costs, cybercrime and attacks can impede a company's ability to do business, expose confidential corporate and customer data, and damage their reputation.

It's no surprise, then, that the SEC last summer issued new rules on how publicly traded companies must report material cybersecurity breaches and disclose information on their cybersecurity risk management, strategy, and governance practices. The rule updates and finalizes proposals that were issued in 2022.



The Impact of Cyber Risk

What negative consequences have organizations faced due to cyber incidents and breaches?

Impact	2021 RANK	2023 RANK	2023 PERCENTAGE
Operacional disruption (including supply chain/or partner ecosystem)	1	1	58%
Loss of revenue	9	2	56%
Loss of customer trust/negative brand impac	4	3	56%
Reputational loss	5	4	55%
Defunding of a strategic initiative	N/A	5	55%
Loss of confidence in tech integrity	N/A	6	55%
Negative talent recruitment/retention impact	8	7	54%
Intellectual property theft	2	8	54%
Drop in share price	2	9	52%
Regulatory fines	7	10	52%
Change in leadership	5	N/A	N/A

Source: 2023 Global Future of Cyber Survey, Deloitte, 2023
Note: Based on frequency of top two ranking in 2021, top two box selectopn in 2023

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 230,000 global members and has awarded more than 185,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

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.

Expanding Disclosures on Cybersecurity Management, Incidents

The SEC's rules are aimed at enhancing and standardizing cybersecurity disclosures by public companies subject to the reporting requirements of the Securities Exchange Act. The new rules enhance what companies must report relating to risk management, strategy, governance, and cybersecurity incidents that are deemed to be material. The new rules include requirements for registrants to:

- Describe how they assess, identify, and manage cybersecurity threats and whether any risks have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition. They must also disclose material cybersecurity incidents and describe the material aspects of the nature, scope, and timing of each incident.

- Detail how the board oversees cyber risks and management's role in assessing and managing material risks. The SEC decided not to adopt a proposed requirement on disclosing the board's cybersecurity expertise.

- Foreign private issuers are subject to the same rules and must also furnish information on material cybersecurity incidents that they make or are required to make public or otherwise disclose in a foreign jurisdiction, to any stock exchange, or to security holders.

- File a Form 8-K generally within four business days of an organization determining that a cyber incident is material. (Delays in disclosure may be allowed if the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC in writing.)

Key Considerations for Boards

Many organizations are performing gap assessments to understand how well they are currently identifying, analyzing, managing, and recovering from cyber events. Given the new rules, boards should ensure that management is determining whether the existing assessment process will support a four-day turnaround, said George Barham, CIA, CRMA, CISA, director, Standards and Professional Guidance, at The Institute of Internal Auditors (IIA). And while the IT team will identify incidents, the determination of materiality should include input from other areas, such as the finance, legal and regulatory teams, to gain a broad-based perspective.

Board members should also be aware that materiality has both quantitative and qualitative elements. "It's about more than just the dollar impact," Barham said. It also involves legal and regulatory considerations. If the company operates in the European Union, for example, an incident may fall under the General Data Protection Regulation (GDPR). Strategic considerations may also be a factor in materiality if, for example, the incident involved exposure of trade secrets or other information that give the organization a competitive edge. The materiality determination should include any considerations that might have an impact on an investor's analysis of the company, Barham said.

Because the regulation's Item 106 addresses the board's roles and responsibilities, the annual 10-K is the place where organizations should document their governance of cybersecurity. It might report, for example, that the audit committee of the board is responsible for reviewing cyber risk, which is often the case, and could also cover how management reports to the audit committee or board on cybersecurity issues. As part of board members' responsibilities, they should understand the qualifications of who is addressing cybersecurity issues at the management level and how cyber threats are managed and mitigated.

Internal Audit's Contribution

Internal auditors are often responsible for identifying and testing key internal controls that help mitigate cybersecurity-related risks, including referencing widely adopted control frameworks. In light of the new rules, organizations' governing bodies and senior management will need independent, objective, and knowledgeable assurance to validate the effectiveness and efficiency of cybersecurity response and recovery controls. Internal audit can provide this assurance in conformance with its own professional standards as well as with widely accepted control frameworks, particularly those used by the organization's IT and information security functions. Internal auditors can also offer advisory services as companies determine how best to protect against cyber risks.

As organizations determine how to address the new requirements, some specific roles for the chief audit executive and the internal audit team can include:

- Consult with boards, executive management, and cybersecurity risk management leaders on the rules' expected impact from financial, strategic planning, compliance, and audit plan perspectives.
- Update risk assessments regarding compliance with the new regulations and support the organization's preparations to meet the requirements. If internal audit is not already involved in cybersecurity risk assessments, it could start contributing to this process.
- Report on whether current cybersecurity controls are designed appropriately and operating effectively for the organization to comply with the new rules.

"Cybersecurity is typically considered one of the highest risk areas that organizations have to manage," Barham noted, so it is certainly already on internal audit's radar. That means that internal audit is aware of the related risks and the internal controls necessary to mitigate those risks. Internal audit can also provide the information and insights boards need to meet their cybersecurity governance responsibilities under the new rules. In addition to the perspective that management provides, internal audit can offer an independent and objective viewpoint on how cyber risks are managed and disclosed. It can advise the audit committee on incorporating cybersecurity risk and regulations into the audit plan and report on how well the organization is preparing to comply with the SEC rules and how well it implements them going forward.

Meeting the Deadline

For incident disclosures, or Forms 8-K, the rules become effective 90 days after their publication in the Federal Register or Dec. 18, 2023 (smaller reporting companies have up to an extra 180 days to comply). Form 10-K disclosures will be due beginning with annual reports for fiscal years ending on or after Dec. 15, 2023. The NACD noted that although the new rules don't address board members' qualifications, they do, "elevate the role of all leadership, including the board, CEOs, and chief information security officers, in risk management." As board members address their new responsibilities, they can turn to internal audit for the valuable assurance and insight they will need to tackle cybersecurity concerns.

QUESTIONS FOR BOARD MEMBERS

- How is the organization ensuring it will be prepared to comply with the new SEC rules?
- What kinds of controls are already in place to prevent or mitigate cyberattacks? How successful have they been?
- Are new controls or reporting procedures being put in place to address the new SEC rules? If so, what are they?
- Has the organization experienced any material cyber incidents in the last two years? How were they addressed and what improvements could be made?
- What kind of assurance or advice from internal audit can help the board meet its cyber risk oversight responsibilities?

"Time Is of the Essence with SEC's Approved Cybersecurity Disclosure Rules," James Turgal, NACD, September 12, 2023.
Cisco Cyber Security Readiness Index: Resilience in a Hybrid World Cisco, March 2023.