GLOBAL KNOWLEDGE BRIEF

LEADING TRENDS IN CYBERSECURITY, SOX, AND THE SEC

Executive Member Webinar Recap

The Institute of Internal Auditors

Table of Contents

Introduction

A need for collaboration

One of the major headlines in the U.S. business world for 2022 was the proposed cybersecurity risk management, reporting, and record-keeping requirements from the Securities and Exchange Commission (SEC). Stemming from recognition of the increasing frequency of cybersecurity breaches through ransomware and data theft, the impact they have had on investor confidence, and a rapidly changing work environment that is seeing rapid adoption of new digital technologies and remote work, the new rule would require public companies to provide enhanced disclosures related to cybersecurity incidents, as well as strategy and governance of cybersecurity within the organization.

How such disclosures should be enhanced takes a few different forms, and the SEC provides significant details on what precisely its expectations will be should the proposals take effect. In The IIA's recent Executive Member Webinar, *Leading Trends in Cybersecurity, SOX, and the SEC*, David Collins, director of information security at Yellow Corp., and Jonathan Bernadt, chief audit executive at Yellow Corp., provided insight into what organizations can expect from the changes, the challenges they might face should the proposals remain unchanged, and how internal audit can use these changes as an opportunity to confidently participate in dialogues with IT stakeholders on cybersecurity risks, controls, and assurance.

Executive Member Webinars are offered throughout the year and are available exclusively to IIA Executive Members. Be sure to visit the Executive Knowledge Center regularly for resources and upcoming events!

The SEC Proposals

A challenge for organizations and internal audit alike

Understanding the proposals

A need despite costs

Based on rationales provided by the SEC regarding the rule, it is clear that the regulator generally views disclosures provided by publicly traded companies to this point to be lackluster. Specifically, the commission noted that there were several "cybersecurity incidents reported in the media that were not disclosed in a registrant's filings." Additionally, it was noted that the "levels of specificity" in cybersecurity incident disclosures varied wildly, and there was a pattern where the industries with the highest profile incidents tended to provide the least amount of detail in their disclosures.

"The tone and the language make it pretty clear that the SEC staff felt that maybe not all of us, but a lot of us as registrants, haven't been doing enough to disclose our information about cyber breaches and risks," said Bernadt.

Arguably most concerning of all, the commission cited a 2020 study from Audit Analytics that said it took companies an average of 44 days to discover a breach and 53 days to disclose the breach — both figures far from ideal. This concern is most clear in one of the rule's signature changes, which would require material incidents to be disclosed on Form 8-K within four days from the determination that an incident is material.

Making such an extreme shift in the name of rule compliance will inevitably come at a cost to organizations. As the proposals make clear, however, the benefits will outweigh the costs. For example, according to a cited 2016 study from the Council of Economic Advisers, the estimated cost of a cyber incident is between $57 million and $109 million.

"Definitely what came across is they felt this is something of value to shareholders," said Collins. "They want us to understand that knowing how we're allocating capital towards cybersecurity adds value to the investment community."

A Broad Spectrum of Risk

In addition to the four-day timeframe for disclosures, companies would have to include in their 10-K filings processes that identify and manage cybersecurity risks and threats, according to the proposed rule. In an attempt to clarify this requirement, the proposal provides an almost overwhelmingly broad picture of what entails a cybersecurity risk and threat that would require a process. Some cited examples include operational risk, intellectual property theft, fraud, extortion, harm to employees or customers, reputational risk, and violation of privacy laws. However, not every organization operates within the same risk landscape, so the responsibility of designating what constitutes a material risk that requires processes and controls would be left to each individual organization.

Even still, the sheer breadth of the cited risks, combined with the short timeframe for reporting, raises some questions and concerns about how valuable such disclosures could be. “Do you really know all you need to know in that timeframe?” asked Bernadt. “You’re going to be continuously learning about the breadth and scope of a breach for quite a while after. Knowing that, there’s a concern companies are going to be over-conservative in the reporting and then have to file a bunch of amendments.”

“There have been questions about how exactly you are expected to pull these together,” added Collins. “Do [the disclosures] even provide relevant information when you weigh it against compliance challenges trying to track these risks? It will be interesting to watch going forward and see if [the SEC] will back off the aggregation a little bit, because I do think that’s going be a challenge to try and manage.”

The Role of the Board of Directors

The final element of the proposal would require specific disclosures related to the board of directors’ cybersecurity management oversight responsibilities. These could include details on basic responsibilities relating to cybersecurity management, how the board is informed of the risks, how frequently they are informed of the risks, and the level of cybersecurity expertise of individual board members.

This, too, has created concerns. “There’s definitely concern around the naming of the cyber expert on the board of directors,” said Bernadt. “There’s very limited availability of true cybersecurity experts who also have the skill sets to sit on a board in general, and smaller companies may be disadvantaged trying to get such scarce talent to serve on their board. Plus, if you name somebody publicly, are you making them a target of, say, a bad actor of a nation state?”

“The biggest challenge from a technical side regarding this is just basic organizational security,” said Collins. “A lot of CISOs are technologists, so sticking them on a board in a lot of cases doesn’t make much sense. While fulfilling this one little area, they’re not providing in a lot of cases value everywhere else because they just don’t understand the finance side, the business side, or any number of other pieces. The CISOs that are on boards had to learn these things over many years and use that knowledge to fulfill a broader role.”

Where does internal audit fit?

Use Reporting Tools Already in Place

As daunting as compliance with these proposals may sound (assuming the proposals are adopted), the good news for organizations is that the foundation of these reports should already exist within established processes for Sarbanes-Oxley (SOX) disclosures — which in recent years has often been associated with the internal audit function. While this is not to say that new processes and controls from a cyber standpoint will need to be added, protocols for tracking and logging events through the necessary documentation should already be in existence to build upon. In some cases, organizations will already have SOX controls in place tied to cybersecurity.

“There won’t be a one-size-fits-all approach,” said Bernadt. “We’re all going to handle this differently. Some of us are going to add a bunch of entity-level controls around the risk management piece, carve out specific cyber disclosure controls, beef up incident response controls, for example. In our case, I envision talking to our accounting folks and standing up something high-level around risk management processes, and then probably beefing up IR [incident response] controls from there to reflect what’s in the rule.”

Consideration should be given to SOX disclosures regarding scope in order to account for cyber threats properly. Collins noted, for example, rethinking how to properly assess third-party providers might be warranted. “How do you need to modify current controls related to third-party providers? They might not currently be in your SOX scope, but now you need to think about them from a cyber standpoint. If there’s an issue, how will they manage it from their end from a cyber perspective, and how will I get notified about it and what they will be doing about it? Moving forward, they might have to be monitored a lot more closely.”

The Three Lines Model

Leveraging The IIA’s Three Lines Model can be helpful in determining how to manage requirements within the proposed rule. A cybersecurity focus in a three lines context could look like:

1. **First line.** Information security, CISO, and business units who manage their own cyber risks, understand the risks and assets they manage, and manage such risks within an acceptable tolerance.

2. **Second line.** Risk management functions and committees who provide oversight over the activities of the first line functions, and organizationally can challenge how the risks are being managed.

3. **Third line.** Independent assurance and advice from internal audit.

While responsibilities are established and delegated among the lines, no individual line operates siloed from the other and therefore does not have sole responsibility for risk — even the ones they directly manage. Internal audit, from the third line, is in a perfect position to articulate this.

“One of the first questions I always ask my security team when they join the organization is, ‘What is the purpose of security?’ It’s not to secure things; it’s to make money,” said Collins. “That’s why we’re all here. We’re a business, and security is just one piece of that business. When you approach risk from that standpoint, you get a lot more done. You can form more defined relationships with an approach linked by the same goal.”

About The IIA Executive Membership

This knowledge brief is an exclusive benefit of The IIA Executive Membership. This membership delivers all IIA member benefits, plus exemplifies the preeminent membership for a high-level, seasoned internal audit executive. Members access customized tools, tailored content, and peer-to-peer networking focused on leadership, team development, performance, and problem solving.

About The IIA

The Institute of Internal Auditors (IIA) is an international professional association that serves more than 218,000 global members and has awarded 180,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized as the internal audit profession's leader in standards, certification, education, research, and technical guidance throughout the world. For more information, visit theiia.org.

Disclaimer

Copyright

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101