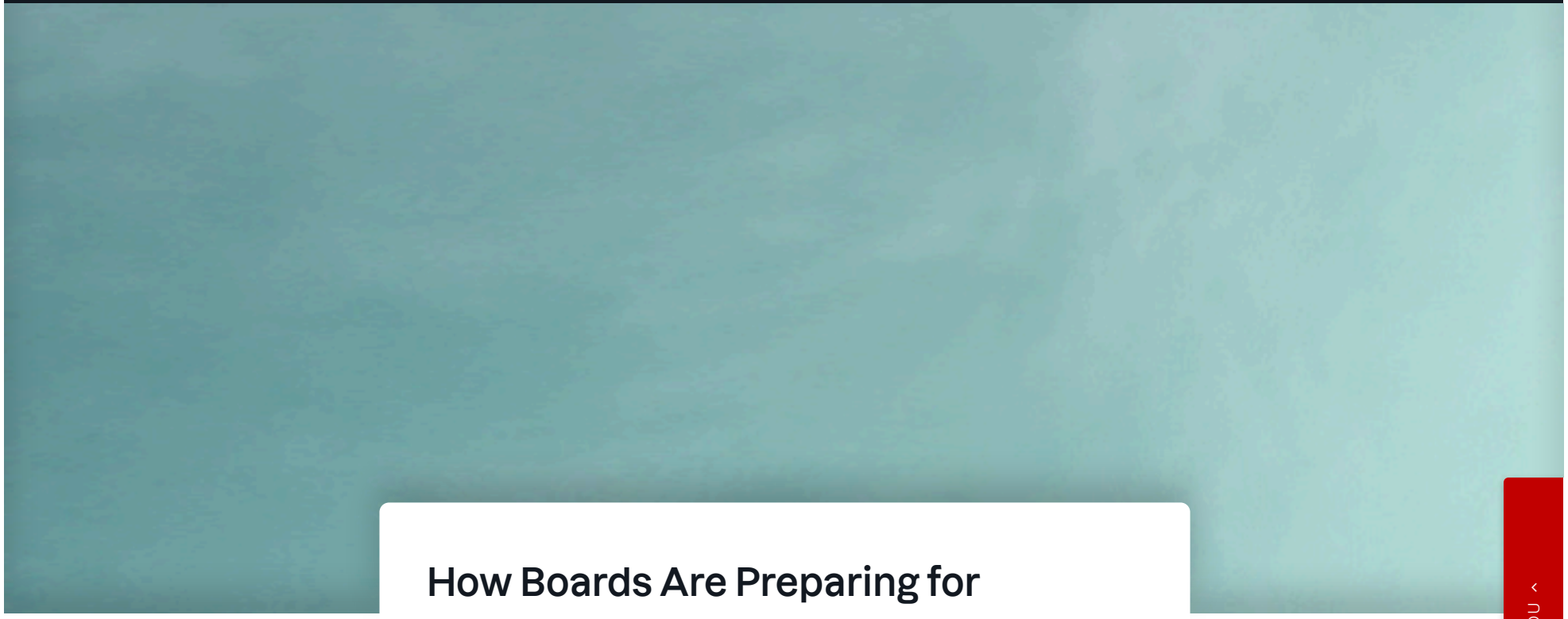

How Boards Are Preparing for Increased Federal Oversight of Cybersecurity

Companies say they haven't seen such wide-ranging board-governance proposals from the SEC since rules implemented after the Great Recession.

AUGUST 18, 2022

RECOMMENDED FOR YOU

incomplete. The SEC hopes to change that.

- At minimum, board members must gain greater fluency with risk management and cybersecurity.
- Boards must hold scenario planning and tabletop exercises and create a cybersecurity subcommittee.

Kevin Kelly wished he had been able to stop his client from wiring a hacker $10 million.

His client is a billion-dollar sporting goods company. The hacker found the name of the company's CEO on LinkedIn and created a bogus email account in the CEO's name. The fraudster then crafted a phony invoice from the company's Southeast Asian supplier of basketballs, lacrosse sticks, and other goods (complete with imitation letterhead) and sent that from the CEO's fake account to the company's CFO, with an order to wire $10 million overseas.

Unfortunately, the scam was spotted too late. And it's one that has become all too common and lucrative in today's network of global supply chains. "Boards and executives are increasingly the targets and casualties in these breaches," says Kelly, the CEO of Halo Privacy, which offers data-privacy solutions to boards, executives, family offices, and the wealthy.

companies—and their boards—would have to quickly disclose cybersecurity incidents. The SEC's proposed rules come amid a wave of cyberattacks that have shut down public companies, private organizations, and governments. "From the perspective of wanting to improve the nation's cybersecurity, this is an overdue measure," says Megan Stifel, chief strategy officer at the Institute for Security and Technology.

The SEC has noted that a key reason for the rules change is that cyber incidents are being reported in the media rather than in company filings. In addition, the agency found that when disclosures are made, the details of the reports are often inconsistent or incomplete. (The most controversial element of the SEC proposal is a requirement that cyber incidents must be disclosed within four days of being labeled a "material" event.)

4

The number of business days a company will have to report a cyberattack, according to the SEC's new proposed rules

"Cybersecurity must be managed as a material business risk, not just as a technical matter," says Phil Reitinger, president and CEO of the Global Cyber Alliance, a former CISO at Sony, and a top cybersecurity official in the Obama administration. "Ignorance of the financial elements of a business is no excuse for mismanagement by the board, and cybersecurity should and will be treated the same. If a board lacks the current capability to set policy and engage in oversight, then it needs to staff up."

Bolstering the board's oversight

As part of the proposed rules, companies would be required to disclose the board's cybersecurity expertise and oversight responsibilities. The draft

> **Boards and executives are increasingly the targets and casualties in these breaches.**
>
> Kevin Kelly, CEO, Halo Privacy

"Often, boards have not had that conversation about cybersecurity as board-level expertise," she says. To prepare for the regulations, she advises companies to begin asking questions such as: Should cybersecurity be on the audit committee or should it have its own committee? "Wherever they land with the answers, it almost doesn't matter," she says. "But companies and boards have to have had the conversation."

Wilson Sonsini, the Silicon Valley law firm that advises the world's biggest names in technology, argued in a letter to the SEC that cybersecurity concerns should not be elevated above other key issues involving risk. The firm is concerned that the regulations "may cause companies to prioritize cybersecurity expertise on the board of directors to the detriment of other cybersecurity measures and other desired experience."

At a minimum, however, board members need to gain greater fluency with risk management and cyberdefense, says Justin Greis, a McKinsey partner who focuses on digital issues. "Board members will need to understand and be able to describe—and probably defend—their company's cybersecurity posture,"

Indeed, Fortune 100 companies like Citigroup and GM are investing heavily in cybersecurity expertise in light of the SEC proposal, up to the board level, says Jonathan Day, CEO of Tapestry Networks, which advises corporate boards on strategy and governance. “They are bringing in directors who have deep experience in this area,” he says.

How much strategy to disclose?

Another element of the proposed rules is a provision that requires boards to periodically disclose company policies and procedures related to identifying and managing cybersecurity risks, as well as management’s role in implementation. The provision could force companies to give away too much information, some experts maintain.

> **Boards will likely have to engage on cybersecurity matters more closely than ever.**
>
> Justin Greis, partner, McKinsey & Company

“Overreporting intellectual-property risks could enable competitors to gain a potential advantage,” says McKinsey’s Greis. “Oversharing about cyberdefense could give hackers an opportunity to leverage the disclosed information to compromise company networks.”

Cybersecurity risk is like financial risk

To Kelly of Halo Privacy, the adjustments that companies and boards would need to make to adapt to these new rules are not unlike the major changes that were needed following the Great Recession of 2008 when he was CEO of executive search firm Heidrick & Struggles.

> **Fortune 100 companies like Citigroup and GM are investing heavily in cybersecurity expertise in light of the SEC proposal, up to the board level.**

At that time, the SEC beefed up requirements for financial risk disclosure and placed responsibility with the board's audit committee. The SEC required timely disclosures, with a stern threat of enforcement for companies that failed in their duty.

Given the magnitude of the current cybersecurity crisis, Kelly expected the SEC to require a board committee dedicated to the issue, with regular calls and meetings. He also wonders whether the SEC should enforce term limits on board members to keep cybersecurity expertise fresh.

McKinsey's Greis says some companies are already exploring the idea of establishing a subcommittee devoted entirely to cybersecurity. "It can be

To increase preparedness, cybersecurity and corporate board experts also recommend holding detailed scenario planning and tabletop exercises, as well as off-site board meetings with cybersecurity experts, to experience viscerally what could happen during a cybersecurity breach.

Even though companies may bristle at the SEC's increased oversight, they recognize that the proposed rules have resulted from a lack of planning and action. "Without a plan, companies are putting a ton of people at risk," Kelly says.

Cleaveland of UC Berkeley says many organizations are already prioritizing cybersecurity planning and strategies. "Most sophisticated and mature boards are not preparing for this regulation through a compliance mindset," she says. "They are already on this journey."

Holly Rosenkrantz

Holly Rosenkrantz is a former White House and business reporter for Bloomberg News. She specializes in analytical and investigative research, covering legal, finance, security, healthcare, and technology issues.

Technology & Innovation Reporting - National Government Coverage - Pacific Region
Technology & Innovation Reporting - Pacific Region

Tanium Subscription Center

Get Tanium digests straight to your inbox, including the latest thought leadership, industry news and best practices for IT security and operations.

SUBSCRIBE NOW

Related

Cyber Insurance?

to Imagine the 'Unknown Unknowns'

Survival Guide

The Power of Certainty™

Tanium AEM empowers IT operations and security teams to identify, manage, and execute change safely and reliably – at scale, with confidence, and in real time.

SEE A DEMO →

Focal Point Magazine

Tanium Blog

Let's Converge Podcast

Downloads

Events

Training

Certifications

Support

Resource Center

Tanium Account

Customers

Success Stories

Partners

Partner Finder

Become a Partner

Partner learning hub

Legal

Privacy Policy

Terms of Use

CCPA Notice of Collection

Do Not Sell or Share My Personal Information

English