Navigating the Governance of Cybersecurity and Cyber Resilience

With the SEC's new rules emphasizing expedited disclosure of cyber breaches, CFOs must ensure they have robust procedures in place to prevent and respond.

This article was originally published on CFO and legally licensed by Industry Dive. Please direct all licensing questions to legal@industrydive.com.

By Andrea Calise, Colleen Hsia, Kevin S. Schwartz, and Steven A. Cohen

Feb 22, 2024 at 10:00 AM

Cyber breaches are one of the most materially disruptive events a company can encounter. The frequency and breadth of ransomware attacks have grown at an explosive pace, up 95% last year, with the financial impact reaching a record high. The ramifications include operational disruptions, litigation, customer attrition, reputational damage, credit deterioration, and capital market costs.

As a result, cybersecurity has become a top priority in boardrooms and the C-suite with defensive cybersecurity alone considered insufficient. Today, corporate boards and management must widen the aperture to include cyber *resilience*.

With the SEC's new rules emphasizing greater disclosure of cyber risk oversight and expedited disclosure around actual breaches, boards and executive leadership must ensure that they have robust systems, plans, and procedures to prevent and respond.

Below are our top 10 takeaways for public companies regarding cyber risks in 2024.

1. Building Cyber Resilience is a Board Responsibility

Cyber resilience can't just be the domain of the CTO or CISO; it must be a top-board responsibility. With cyber risk directly incorporated into factors shaping ESG models and credit ratings there is little room for error. Ineffective cyber responses are even becoming an attack vector of shareholder activists.

It is essential to have cybersecurity expertise inside the boardroom, whether through new appointments or educating existing directors. All board members should have a clear

understanding of the risk scenarios and know the right questions to ask. Boards should consider additional training and/or expert informational sessions where needed.

Most boards are regularly briefed on cyber risk and are mindful of their "duty to monitor" or "duty of oversight"; it is also essential to keep the board involved when a cyber incident occurs so directors can contribute, monitor, and oversee the situation.

2. Strategic Communications: Don't Forget to Manage the Downstream

The SEC's new four-day disclosure requirement fundamentally changes the cyber incident response approach. Gone are the days of issuing a holding statement and waiting months for forensic investigators to complete their report. Companies need to quickly communicate with stakeholders — including, shareholders, customers, business partners, and ratings agencies — at the outset of an incident before all information is available.

How constituencies perceive management and the board's governance of the matter will have long-term consequences on credibility. This vulnerability is particularly acute for companies with subsidiaries that might create their own messages in the absence of corporate guidance, as well as those with business units that process financial payments for customers and experience more urgent and pressing queries.

3. Beware of Heightened Cybersecurity Risks Around M&A Transactions

The FBI has warned that cybercriminals are increasingly focusing on companies engaged in transactions, as those organizations are more visible and may have blurred management responsibilities and distracted employees.

Management teams should ensure there is a clear plan in place for the merged entities both during and after the transaction, particularly when it comes to determining accountability, decision-making processes, and communications strategies in the case of a cybersecurity incident. Cyber risk should be a focus of diligence before a transaction is agreed upon, and planning for the appropriate allocation of risk until closing and a boots-on-the-ground plan for seamless integration after closing will be an important part of transaction planning going forward.

4. Cyber Events Can Quickly Become Market-Moving Events

The aftermath of a cyber incident is an opportunity for management teams to showcase their resilience — or the opposite. Strategic communications and constituent engagement will be

critical, and dialogue is a two-way street. The SEC required 8-K disclosures will lead to financial markets reacting faster, giving more feedback, and demanding more information. As such, cyber breaches will more quickly become market-moving events, with activists, competitors, and hackers also weighing into the information mix.

Proactive engagement with the financial community and media, alongside additional 8-K disclosures, may become more urgent as additional information comes to light. This is especially important because journalists closely follow news of corporate cyber incidents and look for follow-up disclosures — and may write stories on the absence of or delays in communications.

5. Resist the Urge to Say Too Much Too Soon

There is often a desire to state publicly, as soon as possible, that the situation is under control. And where the facts are solidly reliable in short order, this is a good idea. But that is rarely the case. Often companies learn more and revise their assessments with the benefit of hindsight and further investigation, and that includes discovering new pockets of damage.

Resist the pressure to be definitive before the facts are known. Investors are becoming increasingly tolerant of companies taking the time necessary to understand the situation before communicating fully. A cyber breach is often the result of misfeasance and is likely to be a surprise. And while investors and boards don't like surprises, they like multiple surprises even less. Nothing destroys management's credibility like a retraction.

6. Implementation, Not Just Design

While developing a state-of-the-art cybersecurity and reporting architecture is critical, any weak links in the chain of implementation can render such infrastructure moot. While many companies' cyber departments devote attention to best practices in cybersecurity risk management, it is equally important to ensure that such practices and processes are pressure-tested on an annual basis.

Known risks and vulnerabilities should be reported to senior executives and the board, and the board should include implementation as a separate part of the question as they exercise oversight. Third-party systems, too, warrant pressure-testing as much as do internal controls — indeed, the weak link in cybersecurity might well be at supply-chain partners or outsourced vendors.

7. Litigation Must be Contemplated Among the Heightened Cyber-Related Risks

The SEC has now acted on its long-simmering determination to instigate litigation against companies involved in cyber incidents, including specifically naming information security officers, as evidenced by the SEC's recent complaint against SolarWinds and its CISO for fraud and internal control failures relating to the company's cybersecurity risk and incident disclosures.

While it remains to be seen whether the SEC will succeed in proving its claims, the complaint leaves no doubt about the prospect of robust cyber-related litigation, including against top corporate cyber leadership. Companies should carefully scrutinize their current cybersecurity-related policies and procedures to identify and address any notable gaps between existing approaches and new SEC standards.

8. Where the Government Leads, the Plaintiffs' Bar Follows

The cyber security litigation risks also extend beyond the SEC and other agencies to include litigation by the plaintiffs' bar. While the timing and procedural bounds of this litigation may differ, and even the forum (or fora) will likely change, corporate management and boards must anticipate and respond to the risks of cyber-related litigation in this broader arena. Companies should anticipate the possibility of shareholder disclosure suits, oversight/fiduciary duty suits, customer and data-provider information suits.

9. AI is Being Used Both to Attack and Defend

Many businesses are incorporating the benefits of AI into their processes and products, including crafting AI-powered threat-detection systems and tools to make possible real-time, dynamic monitoring of companies' AI systems.

Conversely, the cybersecurity landscape is being transformed by generative AI that empowers sophisticated, machine-based, and personalized attacks at scale, leaving static defense regimes vulnerable. As one report put it, generative AI can lead to "novel phishing attacks, new automated creation of malicious code, sustained attack campaigns, and even deep fakes designed to elicit human trust" — and can "augment malicious actors at every stage of the attack kill chain." Driving a 'security mindset' and culture of awareness through all levels of a corporation is an important first step in combating these increasingly sophisticated attacks.

10. Organize and Pressure Test Your Company's Architecture of Cyber Resilience

Crisis preparedness teams need to be recast for new-world scenarios. Companies and their advisors must be ready across legal, communications, IT, technical incidence response, forensics, audit, data breach notification, call center and monitoring, and ransom negotiation.

An architecture of preparedness requires financial support to cover the costs of such risks and assure that proper lines of communication, decision-making authority, and plans of response are well-understood by all involved before a cyber crisis strikes. These contingency plans should be reviewed and tested with tabletop simulations at least annually to make sure they are adequate in scope, in light of rapidly evolving practices and threats.

Andrea Calise is president of U.S. strategy and communications at Teneo, Colleen Hsia is senior managing director at Teneo, and Kevin S. Schwartz and Steven A. Cohen are partners at Wachtell, Lipton, Rosen & Katz.