whitepaper

SimSpace

Cybersecurity Transparency and the New SEC Regulation

SIMSPACE CYBER FORCE PLATFORM

Contents

Introduction

49% of CEOs globally are concerned or extremely concerned about cyber threats, making cyber the top threat to revenue growth. However, only 33% of members of the board of directors felt they understood cyber vulnerabilities in their organizations. The fast-growing amount of cyber incidents is one of the most critical economic and national security threats today.

By definition, public companies are held to a higher level of transparency than their private counterparts. Due to their accountability to the shareholders, public companies must file a quarterly financial report with the Security and Exchange Commission (SEC). Public companies are also large and critical to the national economy of the countries they operate in. Public companies generally perform at a higher level than other companies.

The board of directors of a public company must look out for the shareholder's best interests, especially by mitigating any risk to the organization. Traditionally, this has meant financial risk, but in their new disclosure rules, the SEC has officially recognized the unique risks posed by inadequate cybersecurity policies.

On March 15, 2022, the ***Cybersecurity Incident Reporting for Critical Infrastructures Act of 2022*** was signed into law. It necessitates that organizations must announce notable cyber incidents, and the act provides protections that encourage businesses to report cyber incidents. The new act mandates transparency of cybersecurity practices, whereas sharing the details of these practices was previously discretionary. The new act also standardizes information sharing.

49%

of CEOs globally are concerned or extremely concerned about cyber threats

The best way to defend against a future breach, is always to practice good cybersecurity hygiene and strengthen your defenses now.

Use Transparency as a Competitive Differentiator

Now that it is a requirement for public companies to disclose cybersecurity practices in their SEC filings, CFOs and corporate leaders can strategically shape their disclosure rather than be reactive. To prepare for the new SEC rule, organizations must advance their people, processes, and technology practices for cybersecurity. The best way to defend against a future breach, is always to practice good cybersecurity hygiene and strengthen your defenses now.

To take a proactive cybersecurity posture in future SEC filings, executive leadership should focus on both understanding that their risks are covered and that their people, process, and technology investments are optimized to defend the organization. There are several concrete steps companies can take now to proactively prepare their cybersecurity posture for the new SEC rules.

1. Update cybersecurity policies and procedures. To protect against a breach or properly disclose information after a breach, clear communication processes must be defined across the infosec, communications, and legal teams. Take time now to define communication processes and understand what would happen in the event of a breach. Reviewing policies will provide the necessary process, oversight, and compliance for the new disclosure requirements.

2. Reassess the board oversight system. The new rule includes a broad set of board-related topics that must be addressed. If your board does not currently oversee cybersecurity issues, the level of involvement the board should have in cybersecurity issues should be considered. Whether your board currently does or does not have any cybersecurity oversight responsibilities, the amount of time the board is currently spending on cybersecurity issues should be assessed and reevaluated.

3. Enhance cybersecurity training for personnel. A consideration of the new SEC rule is that management's role in cybersecurity and expertise must be disclosed in case of a breach. Additionally, executives may also appear on annual reports and proxy statements. Investing in cybersecurity training across the company, especially for executives that may appear on a disclosure, will help prepare for future breaches and disclosure requirements.

4. Minimize the risk of a breach. Improve cybersecurity processes, personnel, and technology to minimize the risk of a breach and, therefore, a disclosure in the first place. A cyber range, such as SimSpace's Cyber Force Platform, allows cybersecurity staff to train to defend against actual attacks and improve their proficiency. SimSpace's military-grade cyber range offers an advanced training curriculum, live-fire events, and customized attack content.

Change the Conversation from Abundance of Coverage to Absence of Weakness

Given that 63% of organizations were breached in the past year, an increase of 4% since the year before, preparing for the worst is imperative. It may not be a question of if your company is breached, but when.

When asked about defenses, CISOs and cybersecurity teams usually brief the board in terms of an "abundance of coverage." For example, having a cybersecurity team of 30 full-time equivalents and an arsenal of 40 cybersecurity tools. However, the number of people and technologies is insufficient to defend against a real-life threat. Additionally, this posturing likely contributes to the bloat of the team and tools.

63%

of organizations were breached in the past year, an increase of 4% since the year before

To prepare for the new SEC regulation, boards and C-suite executives should shift the conversation from an "abundance of coverage" to an "absence of weakness." This shift in intention means instead of concentrating on the people and tools that have already been invested in, focus on how effective these tools are at detecting and remediating real world threats. This type of evaluation can be proven in a cyber range, such as the SimSpace Cyber Force platform.

Just because you have invested in the right tools doesn't mean you know how to use it. Just because you have built a great team doesn't mean they know how to defend your specific organization against industry-specific threats. Rather than assuming you have invested in the right tools and staff with the correct skills, evaluating program holistically in a cyber range can show its overall ability to perform without weakness. There are several quantitative metrics executive leadership can measure in a cyber range and benchmark against similar companies, competitors, or across their industry, and will help build confidence in their cybersecurity program. These include average time to detect a breach, average time to remediate a breach, and performance against advanced persistent threats (APTs).

The Benefits of SimSpace

The world's most advanced commercial cyber range

The world's most advanced commercial cyber range powers the SimSpace Cyber Force Platform, which provides everything needed to keep your people, processes, and technology operating at peak performance. With hyper-realistic simulated environments, you can see how your cyber defenses will respond to attacks. That means you can optimize and consolidate your tech stack, build better training programs, perform more effective candidate evaluations, and leverage actionable insights to make more informed business decisions.

Ready to learn about how SimSpace can help public companies prepare their cybersecurity posture for the new SEC regulation? Click here to request a demo.