# What CISOs must know to comply with new SEC cybersecurity disclosure rules

verizon business

Public companies are busy shoring up their cybersecurity operations and documenting their cybersecurity risk management and incident disclosure processes to comply with new U.S. Securities and Exchange Commission (SEC) requirements after the SEC adopted final rules to enhance and standardize disclosure about cybersecurity incidents.

This is especially true after the SEC's decision to charge a software company and its chief information security officer (CISO) with fraud due to misleading disclosure of the company's cybersecurity practices and failure to disclose known cybersecurity risks.

For CISOs, pressure is rising to document incidents and quantify their potential effects.

When the SEC finalized its cybersecurity disclosure rules last summer, it introduced a requirement for public companies to disclose their processes used to assess, identify and manage material cybersecurity risks – along with the related board oversight of those risks and management's role in assessing and managing those risks. The new rules also put in place a four business day countdown clock for disclosing cybersecurity incidents when they are deemed material.

The challenge for CISOs and companies' disclosure teams is in quantifying the effect of a cybersecurity incident to assess materiality and how best to adapt to and comply with new SEC disclosure and reporting requirements.

## Materiality and the four business day reporting requirement

To overcome the challenges, CISOs must first realize that the new SEC rules require disclosure of "material" cybersecurity incidents, not all incidents. Materiality is determined based on standards in U.S. case law and generally refers to what a reasonable investor would consider material in making an investment decision. "This is worth close examination and legal review," said Sam Junkin, Global GRC Practice and Americas GRC Delivery Leader for Verizon Cyber Security Consulting.

To reach a materiality determination, companies should enlist cross-functional stakeholders, including the CISO, the board of directors and C-suite, legal, public relations, and other partners whose involvement will help inform which incidents meet the materiality threshold. Because SEC rules focus on material incidents, which often affect an organization's brand, reputation, revenue or stock price, "being able to quantify those factors is key," Junkin said.

It's important to note that the four business day deadline for disclosure only starts after the company determines that an incident is material. In other words, as soon as you determine that a specific event meets the materiality threshold, that's when the timer starts for disclosing the incident.

It's crucial to build an effective plan for compliance with the new cybersecurity disclosure requirements. This is where third-party support and validation can help CISOs put the right cybersecurity controls in place. This will aid in compliance not just for the SEC rules but for various other regulatory oversight requirements as well.

## What CISOs need to know to comply, lower risk and quickly respond to incidents

As regulatory scrutiny rises and organizations, along with their CISOs, work to avoid growing penalties for lack of compliance, the best path forward is to be prepared. "CISOs must now prepare for material breaches before they happen and not wait until after a cyberattack to respond," Junkin said.

This is where Verizon is uniquely well-positioned to help.

As a leading cybersecurity provider, Verizon provides comprehensive cybersecurity support services and patented, award-winning solutions to help CISOs quickly respond so they can:

- **Streamline compliance.** To make the efforts involved in achieving regulatory compliance easier, CISOs must understand and quantify the effect of a breach, including the costs of downtime. Verizon's Cyber Risk Programs and governance, risk and compliance (GRC) teams can help CISOs quantify the effect of breaches across nearly every industry. CISOs can rely on these quantifiable points to help persuade their boards and other key decision-makers about the importance of cybersecurity protection. "As compliance requirements grow, honing in on ways to standardize and streamline compliance across your organization's specific oversight requirements is paramount," said Junkin.

  In addition to current Cyber Risk Programs and GRC solutions and services, Verizon is launching an automated cyber risk quantification tool to further streamline breach quantification for CISOs.

- **Reduce threats upfront.** To reduce rising threats and regulatory requirements, CISOs must improve risk management. Verizon offers a broad array of support services and solutions, such as its integrated threat intelligence and Managed Detection and Response services. These solutions enable CISOs to wrap their arms around the steps needed to proactively prepare for incidents and continually monitor and track activities across an organization's attack surface. Verizon Managed Detection and Response provides always-on protection that can help quickly identify security incidents and limit their impact.

- **Quickly respond to incidents.** CISOs need multiple skilled resources to respond quickly to incidents. Hiring and retaining security experts, however, is a serious challenge. And in the event of a large data breach, even a fully staffed team can need help.

  To overcome staffing issues, Verizon offers Rapid Response Retainer services, providing much-needed incident response support when organizations discover a breach. Verizon's incident response team can help CISOs establish where a breach occurred, understand how it came into the organization and determine how long the threat actor was inside organizational networks. This service was designed to help reduce the time it takes to respond to and limit the scope of an incident as well as to respond more effectively. Rapid Response Retainer not only augments your response team but also gives CISOs additional investigative capabilities.

  "It no longer makes sense to try to keep every aspect of cybersecurity in-house," Junkin said. "A partnered approach enables CISOs to augment their core team with on-demand capabilities that are usually quite hard to find," he added.

  In the event of an incident, CISOs can enlist Rapid Response Retainer support via a mobile app or a 24/7 emergency hotline or by contacting their designated liaison. It's also important to note that Verizon is vendor-agnostic. Rapid Response Retainer works with any security technology already in place and can help guide incident response across a CISO's entire organization. When an incident occurs, it will also help shift the narrative from reacting to proactively preparing to respond and disclose cybersecurity incidents.

Verizon stands ready to help. We keep up with the rapidly changing nature of cyber threats by processing billions of security events each year, analyzing evolving threats at our global security operations centers, performing forensic investigations for companies around the world, and sharing our knowledge through industry-recognized research and advice as published in Verizon's annual Data Breach Investigations Report (DBIR).

If you have questions or need help, contact your Verizon Business Account Manager, reach out to us here or learn more by visiting verizon.com/business/products/security.

verizon business