5 Steps to Prepare for the New SEC Cybersecurity Rule

New SEC Regulations Go Beyond Incident Disclosure

The new US Securities and Exchange Commission (SEC) Cybersecurity Disclosure Rule for public companies has captured the attention of C-suite leaders and others across the nation and beyond. The SEC established the rule to protect investors with consistent and comparable information on public companies' cybersecurity.

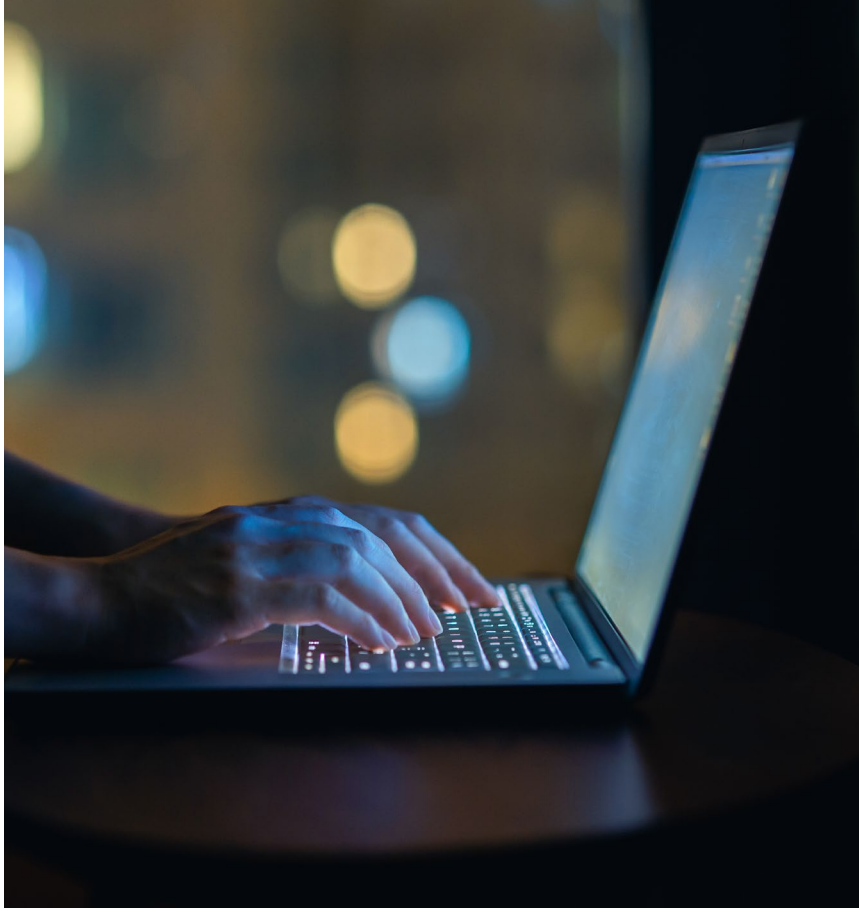
Understanding the New SEC Cybersecurity Rule

The new, far-reaching cybersecurity program disclosures include requirements to determine whether a cybersecurity incident is material within a timely manner and, if so, to provide public disclosure within a specified time.

This new mandate is due to the rise in cybersecurity incidents and their substantial impact on public companies the SEC oversees. This rule was put into place to, among other things, promote consistent reporting across:

- **Regulation S-K Item 106(b) – Risk management and strategy**: An organization's ability, or inability, to manage risks from cybersecurity threats
- **Regulation S-K Item 106(c) – Governance**: Leadership's oversight of risk management and strategy
- **Form 8-K Item 1.05 – Material Cybersecurity Incidents**: Disclosure of a material cybersecurity incident within four business days
- **Form 20-F:** Disclosure by foreign private issuers on governance
- **Form 6-K:** Disclosure by foreign private issuers of material cybersecurity incidents

Guidehouse



Much of the buzz around this new SEC Cybersecurity Disclosure Rule is focused on the four-business-day requirement to disclose a material cybersecurity incident (within a Form 8-K). The SEC defines a material incident as one that would influence the process through which investors make a financial decision. There are exceptions, including if disclosure were to affect national security or public safety, in which case the SEC should be notified to request an extension period. To ensure public companies adhere to appropriate cybersecurity practices, the rule requires annual disclosure (within a Form 10-K or Form 20-F) of their processes for managing cybersecurity risk.

Here's what public companies can do to get ready for this significant new rule.

5 Steps to Prepare for SEC Reporting

Getting an organization ready to comply with the new SEC cybersecurity rule involves these important actions:

1. Develop an Effective Cyber Governance Program

From the cyber practitioner to the board, strong cyber governance enables critical communication with leadership. It also ensures cyber risks are discussed and cyber programs are consistently implemented. With the commitment of top management, a cyber governance program is the foundation from which leaders can execute comprehensive policies and procedures delineating the organization's approach to Cyber Governance, Risk, and Compliance (GRC). This involves defining the roles and responsibilities of those involved and strategically aligning cybersecurity practices with the organization's overarching goals and strategy.

2. Purposefully Understand Business Risk

Understanding the relationship between cyber risks and business continuity is a key first step for an effective risk management program. Performing a business impact assessment can help organizations gain insights into this relationship. This assessment should include understanding the totality of the technology enterprise, from individual assets to third-party connections, including their partners, developing a strong data governance program, and understanding the supply chain. Establishing this enterprise view, coupled with the current technology risk management process (NIST Risk Management Framework) and understanding the current cyber threats, builds a program with full awareness of true business risk.

3. Implement an Effective Cybersecurity Program

Establishing a well-developed cybersecurity program requires the following actions:

- **Establish Cybersecurity Policies and Requirements:** Robust cybersecurity policies include guidance on items such as access controls, data classification, endpoint and network security, security culture, mobile device management, and security compliance. Well-defined cybersecurity policies enable consistent security practices across an organization and promote a security-first culture, both of which are important to the organization and the SEC.

- **Conduct Frequent Education and Awareness Campaigns:** Fostering a culture of cybersecurity awareness and imparting best practices to employees are essential for a successful cybersecurity program. Education and awareness require varying approaches, such as hosting engaging security workshops, conducting simulated phishing exercises, and communicating through various workplace channels.

- **Implement Risk Management Processes:** Addressing risks promptly and developing a strategy to avoid, reduce, transfer, or ultimately accept a risk can help an organization shift its focus to what matters the most. This involves tasks such as:
    - Identifying and safeguarding critical assets
    - Conducting thorough risk assessments
    - Performing vulnerability scanning and remediation
    - Utilizing a Security Operations Center (SOC) for continuous monitoring
    - Implementing effective incident detection and response measures
- **Ensure Oversight and Enforcement:** Continuous monitoring and periodic audits ensures organizational compliance and enables communication for a healthy and effective governance process identifying accepted business risks.

4. Develop and Implement a Robust Compliance Program

Continuously conducting and safeguarding compliance is a cyber GRC cornerstone. It enables organizations to ensure adherence to standards and other best practices, navigate ethically, mitigate legal risks, and cultivate trust among stakeholders. Essential facets of compliance include meeting stringent information technology and operational technology standards, legal and regulatory mandates, the robust enforcement of policies, and meticulous data protection and privacy requirements. Moreover, integrating comprehensive monitoring systems to audit these requirements and establishing remediation mechanisms to catch and rapidly rectify non-compliance are critical in today's cyber environment.

5. Prepare for Incident Action

Cyber incidents happen, even in organizations with diligent cyber governance programs. An incident action plan is, therefore, essential. Steps to prepare include:

- **Develop an Incident Response Plan (IRP)**: An IRP and corresponding playbooks are fundamental to an organization's ability to respond to cybersecurity incidents effectively. The playbooks should highlight scenarios such as a data breach or a ransomware-related data or systems lockdown, including third-, fourth-, and fifth-party lockdowns. A strong IRP orchestrates cybersecurity incident procedures, ensuring a strategic and structured approach to responding, remediating, and recovering following an incident.
- **Develop a Business Continuity Plan (BCP):** A BCP revolves around maintaining an organization's business processes following a disruption. The NIST SP 800-34 Rev.1 contains federal guidelines and criteria for developing a BCP. A business impact analysis identifies critical business functions and processes, which helps prioritize business processes. A BCP with strategically outlined resource allocation, personnel roles, and technology and data recovery plans ensures a robust response to disruptions and facilitates effective business continuity.
- **Develop a Disaster Recovery Plan (DRP):** A vital DRP element is strategically coordinating and running hypothetical exercises on relocating operations to an alternate, secure site for a seamless resumption of operations. Essential steps in a relocation plan include assessing the alternate location's preparedness, ensuring accessibility to systems and data, relocating personnel, and validating the restoration of critical business operations.
- **Perform Periodic Tabletop Exercises (TTX):** A TTX is a simulated scenario-based activity where key stakeholders gather to test their response actions to a hypothetical incident. The TTX begins by stating the scenario and facilitating a discussion between participants on how they would respond. This includes intervening moves by others, such as cyber attackers and press reports. A TTX helps to assess an organization's readiness to respond to an incident and helps assess their IRP, BCP, and DRP, revealing an organization's contingency planning strengths and weaknesses and identifying areas for improvement.

Guidehouse

SEC Regulations Reinforce Cybersecurity Reality

Developing, implementing, exercising, and maturing a robust cybersecurity program can enable organizations to maintain business resilience and provide executives and security personnel with visibility into their organization's overall security posture. An effective program helps prevent incidents and, when incidents occur, activates well-prepared and tested continuity-of-operations protocols. The evolving threat landscape requires organizations to maintain business resilience to effectively mitigate risks as incidents occur. The new SEC regulation reinforces this reality by requiring disclosure of cyber-resilient practices such as prevention, detection, business continuity, contingency, and recovery after a cybersecurity incident. Failing to implement these essential elements of a mature cybersecurity program may raise concerns for or lose the confidence of investors.

Contacts

Marianne Bailey, Partner
Cybersecurity
mbailey@guidehouse.com

Nong Nai, Director
Cybersecurity
nnai@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,000 professionals in over 55 locations globally. Guidehouse is led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit guidehouse.com.

https://guidehouse.com/service/cybersecurity

https://twitter.com/GHTechSolutions https://www.linkedin.com/showcase/guidehouse-technology-solutions/