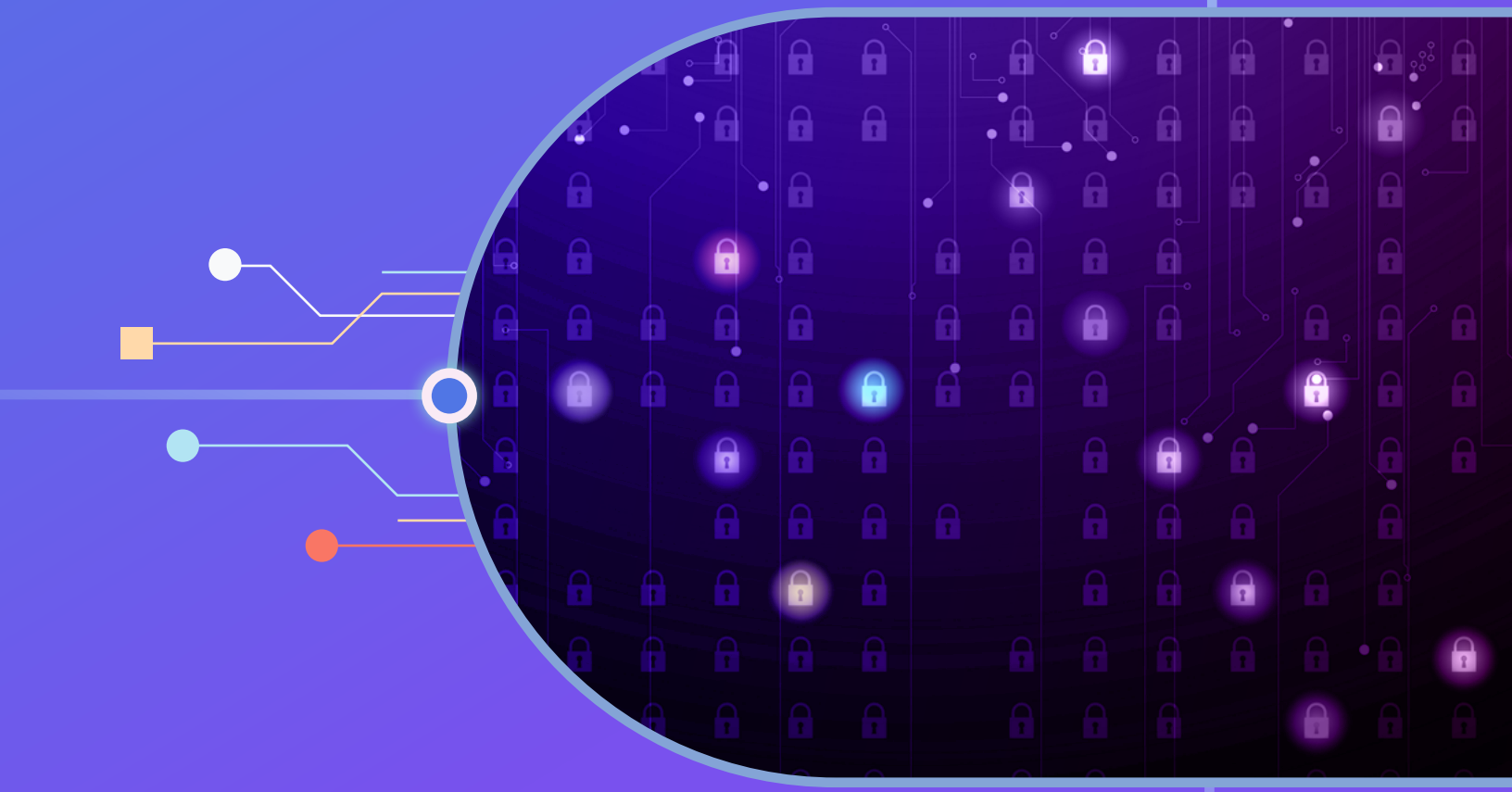
AUDITBOARD

Preparing for the SEC Cybersecurity Disclosure Proposed Rules

Key Steps and Questions



AUDITBOARD

Preparing for the SEC Cybersecurity Disclosure Proposed Rules: Key Steps and Questions

The SEC has come out with a wide range of proposed rules covering topics such as climate risk disclosures, SPACs, and now cybersecurity disclosures. Given the need for consistency and transparency in financial reporting, we believe there is a high likelihood that these rules will come to pass. ***One element of the recent*** SEC Public Company Cybersecurity Disclosure proposed rules ***that stands out is the need for speed*** — four days after the registrant determines that it has experienced a material cybersecurity incident — in disclosing incidents.

Speed in reporting is huge in terms of a company's ability to discover the breach, collect the right information, and involve key stakeholders to ensure that the disclosure is accurate, complete, and transparent. This monumental task requires an integrated approach to pull everything together quickly and accurately — and the time to start preparing is now.

In addition to cybersecurity incident disclosure, the SEC has also proposed to require enhanced and standardized disclosure on registrants' cybersecurity risk management, strategy, and governance.

To help you assess your organization's readiness to comply with the proposed rules, we've outlined steps to consider when responding to the SEC's potential new four-day time limit for disclosing cybersecurity breaches, and created sample questions for consideration when disclosing your company's cybersecurity risk management, strategy, and governance.

Speed in reporting is huge in terms of a company's ability to discover the breach, collect the right information, and involve key stakeholders to ensure that the disclosure is accurate, complete, and transparent.

Cybersecurity Incident Disclosure Steps to Consider

In the event of a cybersecurity breach under the SEC's proposed four-day time limit for cybersecurity disclosures, there are certain steps that must take place between the moment the incident takes place and when you disclose. These steps are intended to help you evaluate whether your organization has the means to comply today, and where you may need to proactively build out capabilities.

Step 1. Identify and Document the Incident

Based on the SEC's proposed rule, the clock on the four-day disclosure window starts when a company "determines that it has experienced a material cybersecurity incident." Obviously, ***the main priority will be to mitigate the breach, but now the cyber defense or incident response team will need to document the incident for disclosure***. The documentation must include the following details:

- When the incident was discovered and whether it is ongoing.
- A brief description of the nature and scope of the incident.
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose.
- The effect of the incident on the registrant's operations.
- Whether the registrant has remediated or is currently remediating the incident.

Ideally, this information should be compiled in a tracking system for all cybersecurity incidents. A single tracking system will become critical for an integrated risk approach and aggregated incidents.

Step 2. Evaluate the Incident for Materiality

Before the proposed rules are adopted for compliance, your organization needs an internal definition of materiality. Rule 405 under the Securities Act defined the term "material" as follows: "[W]hen used to qualify a requirement for the furnishing of information as to any subject, [materiality] limits the information required to those matters to which an average prudent investor ought reasonably to be informed before purchasing the security registered."

Once materiality is defined, train your incident response team to understand when a security incident could reach the level of a material incident that would require disclosure. This training will help ensure all relevant incidents that could possibly be considered material are reported and are reviewable by a separate function. The segregation of duties principle should be applied here to avoid having the incident response team grade their own homework. Ultimately the final decision on whether to disclose should be validated by someone not on the incident response team, possibly from the general counsel or another second line of defense team such as internal audit, risk management, or compliance.

Step 3. Draft the Disclosure

Drafting the disclosure is a delicate task. Even though you want to be transparent and inform your stakeholders, you know that disclosing sensitive information regarding exploits, vulnerabilities or internal architectural details could further jeopardize your operational security. Luckily no one team is responsible for drafting the disclosure. ***The job of drafting and reviewing the disclosure can be completed by an integrated committee composed of the incident response team, legal, risk management, and others***. The key is to include enough people for a comprehensive review while still meeting the four-day window allowed by the proposed rule.

Step 4. Review Incidents for Materiality in Aggregate

The SEC's proposed rule includes a requirement to evaluate past cybersecurity incidents to determine if previously undisclosed individually immaterial cybersecurity incidents have become material in the aggregate. One approach could be to conduct an incident retrospective as part of a quarterly or month-end financial close process. ***If after reviewing all of the incident reports in a given timeframe, it is determined that a series of smaller incidents are material in aggregate, you would follow the process defined for drafting the disclosure***. The exercise should also go through validation by an independent party such as legal counsel. This process becomes much easier when incident reports are centralized in a common platform that all teams involved in the process can access for collaboration.

Cybersecurity Risk Management, Strategy, and Governance Disclosure Questions to Consider

To aid your preparation, ***we have compiled a list of questions you should ask to evaluate your company's readiness for the SEC Cybersecurity Disclosure proposed rules***. These are just to get you thinking, and we are sure you will have many additional questions once you partner with your internal stakeholders on this topic.

1. Has the company identified a cybersecurity expert on the board of directors? Who is the person, and what are their qualifications for this subject matter expert (SME) role?
2. What processes are in place to provide status updates to the board's cybersecurity SME, and how is this information used to influence the organization's cybersecurity governance?

We have compiled a list of questions you should ask to evaluate your company's readiness for the SEC Cybersecurity Disclosure proposed rules.

3. Who in the organization owns responsibility for cybersecurity, and what is their relationship to risk management?
4. Does the company have an incident response team with policies and procedures outlining their responsibilities? Do they contain clear guidelines for escalating and notifying company leadership when incidents occur?
5. How are cybersecurity incidents tracked, compiled, and communicated to risk management? Who performs follow up on the incidents to ensure the issues are resolved?
6. Is anyone in the company performing an enterprise-level cybersecurity risk assessment? Have controls been designed, implemented, and tested?
7. Are there specific cybersecurity policies and procedures that include evaluating for materiality and drafting disclosures? How are these communicated to the organization? How often are these reviewed and revised?
8. Do the policies and procedures address the company's approach to planning for cyberattacks, preventing attacks, detecting those that do happen, and mitigating the damage from an attack?
9. Is the company using technology to track incidents, including financial impact, that can be used to evaluate incidents in aggregate?
10. Has internal audit evaluated the company's cybersecurity risk management or cyber incident management programs?
11. Is the financial reporting team aware of the proposed rules and working with the cybersecurity team and risk management to prepare for potential new disclosures?
12. Have cybersecurity disclosures been included voluntarily in past financial reports?
13. Has the company been through a practice run of the process using a mock incident to test internal procedures, including documenting the incident, evaluating for materiality, drafting the disclosure, and reviewing incidents in aggregate?
14. If an incident were discovered today, could your company comply with the proposed rule with the disclosure produced within four days?

The four cybersecurity incident disclosure steps and readiness assessment questions above will help you determine if additional work is needed to meet compliance with the SEC's proposed rules.

Preparing for Compliance

The SEC is likely to adopt rules related to disclosing cyber security incidents soon. To make the best use of time before the rules go live, start planning for compliance now. ***The four cybersecurity incident disclosure steps and readiness assessment questions above will help you determine if additional work is needed to meet compliance with the SEC's proposed rules***. Start asking questions today to ensure senior management at your company is aware of this topic and taking action to improve the company's ability to discover and get the right information and key stakeholders involved. Meeting the SEC's requirements will benefit from a collaborative approach supported by integrated risk management software to ensure the disclosure is accurate, complete, and transparent — and pulled together in time.

John Wheeler
Senior Advisor, Risk and Technology
AuditBoard

Richard Marcus
Head of Information Security
AuditBoard

AuditBoard transforms how audit, risk, and compliance professionals manage today's dynamic risk landscape with a modern, connected platform that engages the front lines, surfaces the risks that matter, and drives better strategic decision-making.