Brown & Brown

PROPERTY & CASUALTY

SEC Cybersecurity Rule: A Closer Look

Authored by Sal Ansari and Coles Cotter

> **Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors**
>
> **-Gary Gensler, SEC Chair**

New SEC rules released on July 26, 2023, require publicly listed companies to disclose material cybersecurity incidents they experience, and the material information regarding their cybersecurity risk management, strategy and governance annually. The new disclosure requirements take effect starting on or after December 15, 2023. The SEC's objective is to standardize cybersecurity risk reporting to enable investor confidence and enhance executive/board level oversight of the cyber risk management function

Cybersecurity Incident Disclosures

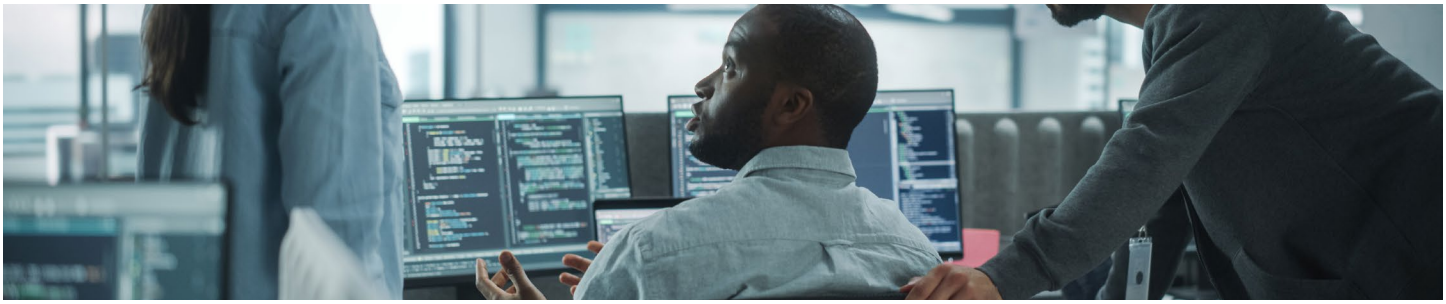
Material cybersecurity incidents should be disclosed within a period of four business days from the date materiality was determined.

Cybersecurity Risk Management, Strategy & Governance Disclosures

These periodic disclosures outline methodologies for evaluation, identifying and mitigating cybersecurity risks.

Included in Disclosure(s)

- Description of incident's material financial, operational or other impact
- Description of incident's nature, scope and timing
- Description of any missing requirements in the event that information is not yet available for disclosure
- Description of processes for evaluating, recognizing and mitigating significant risks
- Description of how these processes have been integrated into a risk management framework
- Details of realized risks arising from prior material cybersecurity incidents, including impacts
- Description of processes for the cybersecurity program's engagement with third-party consultants and auditors
- Description of processes for management/board



Key Challenges

- Understanding the definitions of cybersecurity incident and materiality
- Timely filing of SEC 8-K Cyber Incident Disclosures

Actions to Prepare and Comply

- Establish cyber risk quantification capability to support materiality assessments
- Conduct sample materiality assessments for mock incidents (i.e., tabletop exercise)
- Review disclosure controls and procedures
- Conduct an internal SEC readiness assessment

Overview

New SEC rules released on July 26, 2023, require publicly listed companies to disclose material cybersecurity incidents they experience, and provide material information regarding their cybersecurity risk management, strategy and governance annually.

All publicly listed companies are required to disclose details regarding a significant cybersecurity incident through the submission of Form 8-K within four business days from the moment they ascertain its materiality. This disclosure timeline may be extended up to 30-60 days, but only in cases where the U.S. attorney general determines that such disclosure could pose a significant threat to national security or public safety.

Entities must outline their methodologies for evaluating, identifying and mitigating cybersecurity risks, including insights into the board's supervision and the involvement of management. The new disclosure requirements take effect starting on or after December 15, 2023. Smaller Reporting Companies (SRCs) must comply by June 15, 2024. The SEC's objective is to standardize cybersecurity risk reporting to enable investor confidence and enhance executive/board level oversight of the cyber risk management function.

Cybersecurity Incident Disclosures

The SEC rules require that material cybersecurity incidents be disclosed within four business days from the date materiality was determined. The concept of materiality is consistent with securities case law: information is deemed material if "there is a substantial likelihood that a reasonable shareholder would consider it important." For cybersecurity incidents, materiality will often involve cyber risk quantification to estimate potential financial loss. This estimation can then be used to determine materiality based on a "percentage of revenue" approach at the discretion of the organization.

In situations where an incident presents a significant risk to national security or public safety, as determined by the U.S. attorney general, a disclosure delay of up to 30 days is allowed. Additional delays can also be granted on a case-by-case basis at the discretion of the attorney general or the Commission.

There is no requirement that materiality determinations be made by the full board, a board committee or specific officers. The registrant can follow normal internal disclosure controls and procedures to demonstrate good faith compliance.

Our Perspective

From a cyber insurance perspective, when conducting materiality assessments, entities should weigh the nature of compromised data and the organizational impact in evaluating a cybersecurity incident on financial and operational health. This includes information privacy, proprietary data loss, cyber extortion, revenue loss, regulatory exposure, the cost of replacement of hardware and more. Companies should establish internal protocols for determining materiality.

Cybersecurity Risk Management, Strategy & Governance Disclosures

Our Perspective

The new rules aim to enhance transparency and accountability in how companies manage cybersecurity risks through clear articulation of the organizations' related processes. Management must be prepared to address board inquiries about cyber risk management, impact assessment, materiality and response times. Additionally, companies will need to have mature cyber risk quantification capabilities to appropriately determine materiality. Another element of the new disclosure rules addresses third-party risk. Companies may be required to disclose a material cybersecurity incident that occurred on a third-party system. This focus on third-party risk management from the SEC should impact how organizations manage their third-party engagements and increase due diligence in the areas of third-party risk.

Key Challenges

Understanding the Definitions of Cybersecurity Incident & Materiality

Determining materiality will be complex, involving subjective assessments and balancing quantitative and qualitative factors. The rule's lack of disclosure limits will require entities to make judgment calls that have legal and reputational implications. Navigating these challenges effectively will be crucial to avoiding legal actions, penalties or damage to trust and reputation.

The Short Four-Day Timeline

The four-day window will present significant challenges. Meeting this tight deadline will constrict time for a comprehensive incident identification and assessment, given resource constraints, data collection complexities and the varied nature of incidents. Cyber risk quantification pre-incident will be an important part of the cyber risk management function in addition to legal and compliance preparation, coordination with third parties, continuous monitoring and well-defined incident response plans.

Actions to Prepare and Comply

Review & Prepare

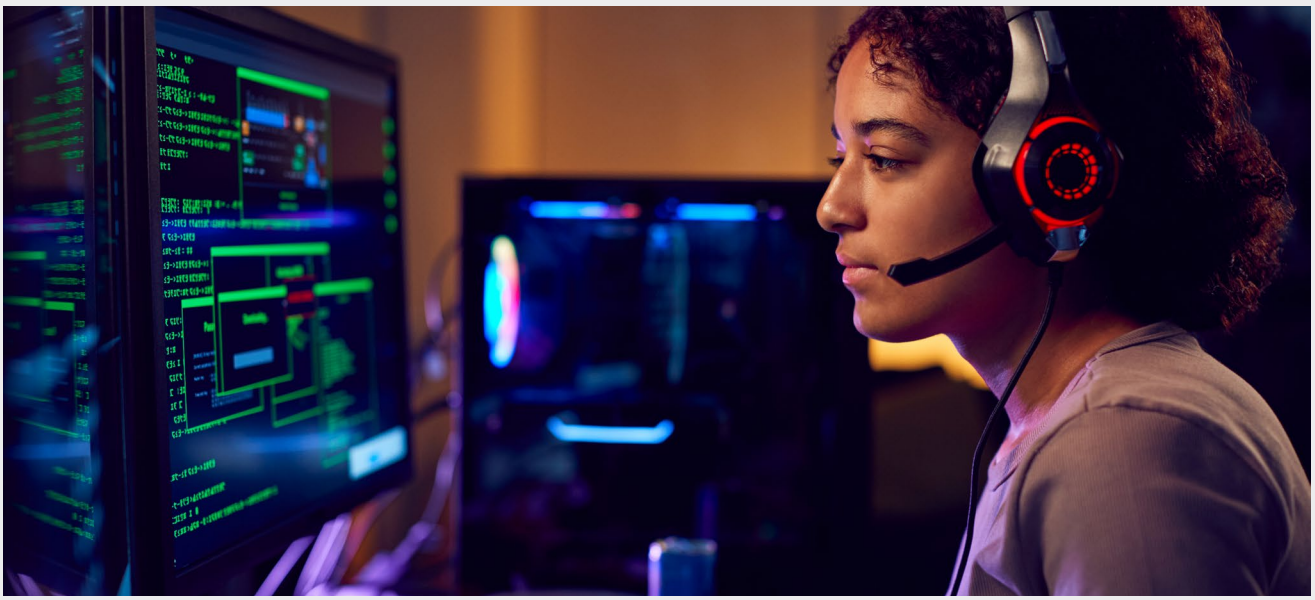
- Cross-functional engagement and external security counsel
  - » Involve key stakeholders, including general counsel, chief accounting officer, CFO, CISO and board members
  - » Seek guidance from external security consultant/ council
- Review disclosure controls and procedures
  - » Assess and revise disclosure controls and procedures for accurate and timely reporting of material cybersecurity incidents
- Materiality assessment and incident documentation
  - » Establish a process for conducting materiality assessment of cybersecurity incidents
  - » Establish cyber risk quantification capabilities to support materiality assessments
  - » Define and document the parties involved and establish controls for timely information gathering
- Stakeholder coordination and orchestration
  - » Develop organization-wide, cross-functional disclosure capabilities for timely reporting
  - » Combine legal guidance with cybersecurity knowledge
  - » Establish accountability for compliance and disclosure

Enhance & Operate

- Cyber incident response and reporting enhancement
  - » Define materiality criteria and integrate them into incident response processes
  - » Continuously meet disclosure obligations and learn from past incidents to improve resilience
- Enhance cybersecurity governance framework
  - » Educate the board and management to strengthen cybersecurity governance
  - » Identify a board committee or subcommittee responsible for cybersecurity oversight

Assess & Evaluate

- Board and management oversight assessment
  - » Evaluate how the board and management oversee cybersecurity risks
  - » Consider updates to policies and procedures if necessary
- Cybersecurity risk management evaluation
  - » Evaluate existing cybersecurity risk management systems and processes
  - » Determine if updates are needed to align with new disclosure requirements
- SEC readiness assessment
  - » Conduct an SEC readiness assessment to identify potential risks and compliance issues
  - » Develop a foundation for evolving response capabilities



To maintain compliance and establish a robust cybersecurity program, it is crucial to have effective cybersecurity governance and control capabilities alongside comprehensive risk transfer (i.e., cyber insurance) solutions. The Cyber Risk Quantification capability will be a key ingredient to materiality assessments as part of the SEC 8-K incident disclosures. Brown & Brown Risk Solutions is well positioned to help guide customers through these unique risk transfer and quantification challenges.

How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.

Brown & Brown

Find Your Solution at BBrown.com