TheChertoffGroup
Enabling A More Secure World.

SEC GUIDANCE

How to Meet New Public Company Cybersecurity Disclosure Requirements

What Happened

On July 26, the U.S. Securities & Exchange Commission (SEC) adopted its Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. The final rule is a significant expansion of disclosure requirements for "material" cybersecurity incidents.

Current reporting about material cybersecurity incidents:
Key requirements include:

- Determination must be made "without unreasonable delay."
- 8-K filing must occur four business after determination days absent U.S. Attorney General determination that disclosure would pose substantial public safety/national security risk.
- 8-K Amendments with material new information.

Periodic disclosure of a registrant's cybersecurity risk management, strategy, and governance in annual reports.
Key public disclosure items include:

- **Processes for assessing, identifying, and managing material risks from cybersecurity threats,** including how cyber risks are integrated into overall risk management system; use of cybersecurity assessors, consultants and auditors; identification and oversight of third-party service provider risks and whether cybersecurity threats have materially affected business strategy, results of operations, or financial condition.
- **Board of directors' oversight of risks from cybersecurity threats, including board committee** or subcommittees responsible for cybersecurity oversight and related processes.
- **Management's role in assessing and managing the registrant's material risks from cybersecurity threats,** including which management positions or committees are responsible for measuring and managing cybersecurity risk, plus related processes and relevant expertise.

Deadlines for Compliance

- Annual reports for fiscal years ending on or after **December 15, 2023** must include risk management/ governance disclosures;
- Incident disclosure requirements must be implemented by **December 18, 2023**.

Failure to adequately implement these requirements can result in SEC enforcement actions directed both at the company as well as its officers and directors.

Our experts can help you meet these new requirements by providing advice to the Board, based on authoritative guidance and decades of expertise, on best practices for overseeing cyber risk.

1. Treat cybersecurity as an enterprise risk: understand the company's business profile and high value assets. Ensure an understanding of potential cybersecurity-related legal risks (in cooperation with the General Counsel and outside counsel).
2. **Update incident response and crisis management plans** for the new SEC requirements and exercise internal processes for responding to a cybersecurity incident.
3. Build **resiliency** through **response-oriented engineering:** implement asset visibility and logging strategies to streamline the process for understanding and thereby containing incidents when they do occur.
4. Review the company's **governance framework** both for management and the board.
   - Deliver education and awareness of changing cybersecurity threats and best practices for management and board members.
   - Ensure management uses an enterprise-wide cyber risk management framework with adequate staff and budget; include discussions on how cyber risk is being identified, managed and measured with transparency, accuracy and precision.
5. Consider how **effectiveness** will be evaluated. Validating that cybersecurity measures are operationally effective in defending against likely threat activity is key to ensuring accuracy and timeliness of the reporting referenced in the final rule.

Contact us for a more detailed assessment of how to meet these requirements at info@chertoffgroup.com.

The Chertoff Group

1399 New York Avenue NW
Suite 1100
Washington D.C., 20005
202.552.5280

chertoffgroup.com

The Chertoff Group is a specialized advisory firm that helps organizations achieve their business and security objectives in a complex risk environment. Our highly qualified and experienced team includes a diverse mix of commercial and public sector security backgrounds. We serve global Fortune 500 clients across multiple sectors, as well as small to medium-sized businesses with specialized needs. Effectiveness, durability and stakeholder alignment are common themes, and our work is grounded in principles of anticipating what is next, demonstrating best practice and value.

Our team helps organizations manage cyber, physical and geopolitical risks; navigate evolving regulatory and compliance requirements; and discover opportunities to win business and create value.

Headquartered in Washington, D.C.
Contact info@chertoffgroup.com for more information.