SANS | GIAC CERTIFICATIONS

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

A Rule by the Securities and Exchange Commission

Earlier this year, the Securities and Exchange Commission (SEC) published the final rules in the Federal Register on cybersecurity risk management, strategy, governance, and incident disclosure.

What Does This Mean?

- Publicly traded companies registered with the SEC and bound by the Securities Exchange Act of 1934 reporting requirements must adhere to this new amendment.
- After a cybersecurity incident has been deemed to be a material incident, the company must comply with required disclosure requirements.
- As of the time of publication, the SEC has stated that a materiality determination of the cybersecurity must be made without unreasonable delay.
- Consult our easy-to-follow timeline below to help your organization prepare effectively for the new compliance rules.

Aug 4 2023

August 4, 2023

What: The SEC introduced new cybersecurity regulations.

Why: The purpose of this ruling is to maintain transparency and honesty from publicly traded companies about risks to shareholders while ensuring adequate attention is paid to cybersecurity, preventing financially damaging attacks.

Action: Learn more by reading John Pescatore's blog.

Sept 5 2023

September 5, 2023

What: Final rules go into effect.

Why: These new regulations mandate cybersecurity oversight throughout the C-suite. Moving beyond the CISO to the CEO, CFO, CIO, COO, Chief Legal Counsel, and beyond. These individuals are responsible for staying up to date on evolving threats, supply chain vulnerabilities, and the impact of emerging technologies to ensure the organization meets all regulatory requirements.

Action: Learn what you need to know and gain actionable insights at the SANS Cyber Compliance Countdown event on November 2, 2023.

Dec 15 2023

December 15, 2023

What: Companies must begin providing cybersecurity posture disclosures.

Why: Beginning with annual reports for fiscal years ending on or after December 15, 2023, registrants must describe executive oversight of risks from cybersecurity threats and describe management's role in assessing and managing these risks.

Action: Learn how to navigate to, and complete, the mandatory disclosure forms by following our guide here.

Dec 18 2023

December 18, 2023

What: Mandatory disclosure of cybersecurity incidents goes into effect.

Why: All registrants not identified as smaller reporting companies.

When: Disclosure must be filed within four (4) business days of determining an incident was material in nature.

Action: Test your leadership's crisis management preparedness and response with the SANS Institute's executive cybersecurity simulation exercises.

Conclusion

These updated SEC cybersecurity requirements highlight the importance of establishing a comprehensive security culture within your organization. This culture should encompass both cyber practitioners and all levels of management. Information sharing, effective IT governance, and consistent training for both technical experts and managerial personnel are essential.