wallarm

INFOGRAPHIC

New SEC Cybersecurity Incident Disclosure Rules

Who's Impacted, What's New, and What Do You Need to Do by When?

The final rule from the Securities and Exchange Commission (SEC) on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure was published on August 05, 2023.

Depending on the size of your organization, this gives you about 3 to 6 months before cyber incidents need to be disclosed in new 8-K forms.

You also need to confirm your compliance plans in an updated 10-K before the new disclosure requirements take effect on December 15, 2023.

Who in the Organization Needs to Prepare?

- **CEO / CFO** who need to sign & certify company's 10-K, attesting to the integrity, completeness and accuracy of information related to the cyber risk management program.
- **Board of Directors** who need to get effective, ongoing reporting needed to understand key cyber risks and what management is doing to mitigate those risks, and develop the expertise to effectively oversee this area.
- **CIO / CISO** who need to develop the systems and processes to support timely disclosure without introducing additional risk to the company.
- **Legal** who need to develop policies and procedures for determining materiality, when & how to federal law enforcement, and draft disclosures which are compliant but do not compromise cybersecurity programs.
- **Audit** who need to confirm that disclosures are complete, accurate and sound.

Key Changes in New Rule.

- Required disclosure of "material" cybersecurity incidents within 4 days
- Updated form 8-K for incident disclosure
- Requirements for foreign private issuers to disclose incidents as well

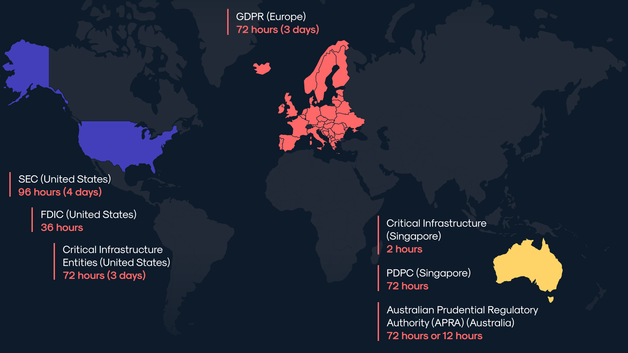
What Companies Are Impacted?

All approximately 12,000 SEC registrants: public companies, mutual funds, investment advisors, transfer agencies, broker dealers.

Includes all companies registered to trade on US stock exchanges

- US-based public companies
- Non-US companies filing Forms 6-K and 20-F

How Does It Compare?



When Do These Changes Take Effect?

The clock is already ticking, with the final rule slated to take effect in early September 2023.

Mar-2022
Proposed Rule Published

Jun-2023
Comment Period Closed

26-Jun-2023
Press Release for Final Rule

04-Aug-2023
Published in Federal Registrar

05-Sep-2023
Final Rule in Effect

02-Nov-2023
New 8-K Required

15-Dec-2023
Updated 10-K Required

31-Jan-2024
"Small Company" New 8-K Required

How to Define "Material Incident"?

1. Preparation
2. Identification
3. Containment
4. Recovery
5. Lessons Learned

Does It Include API Incidents? YES!

- **DDoS attacks** (ex.: Anonymous Sudan) - Potential revenue impact might need to be reported
- **Infrastructure attacks** (ex.: Ivanti EPMM) - Disruption of operations might be reportable
- **PII breach** (ex.: Experian) - Breach clean-up expenses (and fines)
- **Leaked Secrets** (ex.: CircleCI) - Disruption of operations & possible loss of IP
- **Ransomware** (ex.: MOVEit) - Disruption of operations & cost of remediation (and cost of ransom, if applicable)

The Final Rule Also Covers

- **Cybersecurity Risk Management**. Companies must annually disclose their processes for assessing, identifying, and managing material cybersecurity risks in sufficient detail for a reasonable investor to understand those processes.
- **Cybersecurity Governance**. Companies must annually disclose the board's oversight and management's role in assessing and managing material cybersecurity risks, and the process of how they are kept informed.

Why Are These New Rules Needed?

"To enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and material cybersecurity incidents by public companies."

"Because cybersecurity threats and incidents pose an ongoing and escalating risk to public companies, investors, and market participants."

How to Approach Disclosure?

1. Identify and Document the Incident
2. Evaluate the Incident for Materiality
3. Draft the Disclosure
4. Review Incidents for Materiality in Aggregate

To learn more, watch this panel discussion:
CISOs and the New SEC Regulation Panel Discussion (30 mins)

(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107
www.wallarm.com