ASK THE EXPERTS

SEC Cyber Security Regs: The Materiality Minefield

November 14, 2023

CohnReznick

EPIC

Agenda

- Introductions:
  - Meet the Experts
- Laying the Foundation:
  - Overview of the New Rules
- Ask the Experts/Discussion:
  - The Materiality Minefield
- Tips & Takeaways
- Q&A

MEET THE EXPERTS

MODERATOR:
Kelly Geary, Esq., CIPP/US, ACP, CCP
EPIC National Practice Leader
Professional, Executive and Cyber Solutions

CYBERSECURITY EXPERT:
Scott Corzine
Managing Director, Cybersecurity, Technology Risk and Privacy
CohnReznick

CYBERSECURITY REGULATIONS EXPERT:
Richard Borden, Esq.
Partner, Privacy & Data Security Group
Frankfurt Kurnit Klein + Selz, PC

CohnReznick EPIC

Laying the Foundation

The New Rules

On **July 26, 2023**, the SEC adopted new rules to enhance and standardize **disclosures** regarding **cybersecurity risk** management, strategy, governance, and incidents by **public companies.**

Effective Date: December 18, 2023

CohnReznick EPIC

Two Key Disclosures

<u>Annual Disclosure:</u> Cybersecurity risk management, strategy, and governance. Must disclose:

The processes for assessing, identifying, and managing **material cybersecurity risks**

The **board of directors' oversight of cybersecurity risks** (including identifying any board committee or subcommittee responsible for such oversight) and management's role in assessing and managing **material cybersecurity risks**.

<u>Incident Disclosure</u>: Material cybersecurity incidents within ***4 business days*** of determining that a cybersecurity incident is **material. Must disclose:**

The **material** aspects of the nature, scope, and timing of the incident; and
The **material impact** or reasonably **likely material impact** on the Company, specifically the financial and operational condition.

CohnReznick EPIC

When does the 4-Day Clock Start Ticking?

The **4-day clock** to filing a Form 8-K starts ticking when the Company determines that the ***incident is material***.

The Company must make the materiality determination ***"without unreasonable delay".***

ASK THE EXPERTS!

How big of a net has been cast?

Who do these rules apply to – directly and indirectly?

CohnReznick EPIC

MATERIALITY

A fact is “material” if there is a “substantial likelihood that a reasonable investor would consider it important” or if it would have “significantly altered the *total mix* of information made available.”

NOTE: The SEC explicitly **declined** to adopt a cybersecurity-specific definition of materiality.

- **Disclosure Committees: Who** should determine, or be involved in determining, materiality?
- What **factors** should be considered when evaluating materiality? What factors make materiality determination difficult for organizations?
- How do we determine materiality in the context of a **rapidly** evolving cyber incident?
- What are the risks associated with **premature** determinations of materiality and disclosure? What are the risks of **delayed** determinations?
- How can **effective** corporate governance improve organizations' ability to meet their disclosure obligations?
- What will be the impact of the new rule on **risk-transfer** mechanisms: contractual and insurance based?

TIPS & TAKEAWAYS

- Public companies need to supplement their Disclosure Controls so that during a breach, the Disclosure Committee is properly informed, **in a language they understand**, of the implications of the findings of an investigation - in real time.
- Consider the impact on **Risk Transfer Mechanisms** – contractual and insurance-based (D&O and Cyber).
- Consider the impact of the available **limit of liability** of a Cyber Policy on the determination of **materiality**.
- Regulations are becoming increasingly prescriptive and **enforcement** risks more aggressive.
- Boards should play an amplified role in **cybersecurity risk management** by ensuring they can exercise their duty of program supervision.
- Incident Response teams need someone who **understands securities laws** to help translate the findings into information that will allow the Disclosure Committee to make the appropriate materiality determination.

CONTACT THE EXPERTS

Kelly Geary, Esq., CIPP/US, ACP, CCP
Managing Principal, National Practice Leader
EPIC Professional, Executive and Cyber Solutions
917-468-1459
kelly.geary@epicbrokers.com

Scott Corzine
Managing Director, Cybersecurity, Technology Risk and Privacy
CohnReznick
703-744-8541
Scott.Corzine@CohnReznick.com

Richard Borden, Esq.
Partner, Privacy & Data Security Group
Frankfurt Kurnit Klein + Selz, PC
Rborden@fkks.com