ADVANCED CYBER SECURITY CENTER

Responding to the new SEC Incident Reporting Regulations

Cyber Risk Governance Briefing Summary

March 2024

TRUSTED NETWORKS.
ADVANCING CYBER STRATEGIES.

ADVANCED CYBER SECURITY CENTER

ACSC Cyber Risk Governance Program

A unique collaboration of CISOs, CIOs, Risk Officers and Legal Counsels, identifying and managing digital risk, and effectively communicating risk to boards of directors and senior management.

Our legal advisors

Colin Zick
Foley Hoag

Avi Gesser
Debevoise & Plimpton

What is the issue?

In July 2023, the SEC released new rules on "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure." The rules stated aim is to require companies within the SEC's jurisdiction to give investors more consistent and comparable information about the financial impact of cybersecurity risks on their business and operations. The rules purport to do so by making organizations more accountable and transparent in incident management and documentation.

- A finding of a material cyber event now requires an 8-K filing.
- These risks must also be included in an annual 10-K filing.

We will keep moving towards more reporting, not less. If it's not reporting to a government regulator, it will be reporting obligations that get baked into your contracts.

- Colin Zick

Why is it important?

The regulations broaden the range of incidents reported, triggering a 4-day notification requirement and produce a ripple effect across sectors, expanding their impact.

- Third parties linked to organizations within the SEC purview. Every organization should review its SEC-related risk profile based on vendor and partner relationships.
- Other regulatory bodies, including DoD requirements for defense contractors, already have or are adopting similar requirements.

Reference Materials

Leveraging Board Governance for Cybersecurity

Contact Us
(617) 485-1112
wguenther@acscenter.org

ADVANCED CYBER SECURITY CENTER

What's the impact to date?

Firms are likely to err on the side of reporting to protect themselves, and this will influence whether or not they deem incidents to be material.

- Materiality – the SEC does not specially define materiality for cyber incidents, but applies existing authority that disclosure should include any information a reasonable investor would view as having significantly altered the 'total mix' of information made available for an investment decision
- Standards do not yet exist, filings to date provide little specific information.
- We anticipate that the SEC will further define expectations and requirements over time.

Key takeaway: Regulators will inevitably bring more scrutiny to process and documentation than they will to a specific decision on materiality. Disclosure must be driven by an internal materiality analysis that sits inside an organization's larger risk picture.

As a result, organizations are revisiting incident response processes and structures, standards for documentation and decision-making on materiality, and reporting.

Questions: With concerns about information that should be disclosed, are the new regulations undermining existing industry collaborations, including threat sharing? Will boards actually receive less information to avoid unnecessary disclosures?

Generally, these filings have been underwhelming, as they reveal less than has been reported in the trade press.

- Colin Zick

It would not surprise me if the SEC says that some of the current cyber incident disclosures are not sufficient for what they had anticipated.

- Avi Gesser

Two 8-K filings -- from UnitedHealthcare Group and Microsoft -- provide points of comparison on the depth and breadth of information included in their reports.

UnitedHealthcare - *link to filing*

8-K filed on 1/22/2024:

- Contains a **single paragraph** about unauthorized access to Change Healthcare IT systems
- Reported impacted systems had been isolated
- At the time of filing, claimed **no finding of materiality "so far"**
- Little update since then, even as we hear reports of a $100M daily impact on national healthcare and pharmacy operations

Microsoft - *link to filing*

8-K filed on 1/17/2024

- A much **more robust and informative** filing, story revealed in layers
- Key accounts compromised starting in 2023
- Accounts belonged to senior staff, all with cybersecurity roles
- At the time of filing, Microsoft also claimed **no finding of materiality "so far"**

ADVANCED CYBER SECURITY CENTER

We update our incident response plan annually with respect to boards, so we have a number of mechanisms to escalate information when we need to report or when incidents happen.

- Member CISO

How are ACSC members responding?

Five Steps You Can Take to Get -- and Stay -- Prepared

ACSC members are updating and testing the following actions:

1. **Ensure materiality is properly understood and defined** through consistent assessment and analysis.
2. **Clarify and capture the processes and decisions** that drive and inform final executive (e.g. CFO) finding.
3. **Strengthen documentation standards,** including for incidents that don't meet reporting requirements.
4. **Have a plan: engage the board strategically** to reinforce the appropriate committee roles during and after a reported incident.
5. **Test the plan: launch a new round of incident simulations and senior executive and board reporting** to test regulatory compliance.

ADVANCED CYBER SECURITY CENTER

Getting into the Detail

Understanding and Defining Materiality

There seems to be a fundamental disagreement between SEC and the market as to what is material for a cyber event. The market isn't reacting to these supposedly 'material' disclosures -- stock prices aren't moving.

- Avi Gesser

There are multiple reasons to disclose under SEC rules, even before a formalized finding of materiality.

- Reputational advantage of getting ahead of bad news
- Might be appropriate where incident clearly has risk of becoming material (i.e. Microsoft 8-K)
- Financial impact dictated by scale -- e.g. United Healthcare reported a loss of $100M a day
- Some impact -- operational, reputational, effect on third party partners -- is harder to measure
- Ultimately, the filings of materiality are definitive and can't be undone later in the process.

A Challenge: "How is your guidance affected if you're in a situation where it's not necessarily material to you, but others are facing the same vulnerability or threat actor? If they're disclosing, does that dictate your need to disclose as well?" - Member Counsel

Microsoft originally disclosed that there were 40 companies impacted. If 20 of those file 8-Ks, that puts the burden on the other 20 companies to explain why they didn't disclose.

- Avi Gesser

Balancing Internal Priorities and Dynamics

The 8-K filing puts a stake in the ground but can still feel like a subjective exercise. Organizations must produce their own multifaceted materiality analysis on what ultimately might have an operational or financial impact, an important part of the disclosure. The SEC, however, doesn't require you to explain what it is that is driving your materiality analysis.

- Businesses are not required to explain how these risks might have material impact
- Disclosures provide only one datapoint available to regulators (and public)
- In some cases, a failure to disclose creates additional burdens

Contact Us
(617) 485-1112
wguenther@acscenter.org

ADVANCED CYBER SECURITY CENTER

Member Case Studies: Responding to the New Guidance

Two ACSC global firms shared their experience.

#1 Continually Assess, Update, and Test

- Enhanced existing disclosure processes to include an SEC materiality assessment group which reports to the disclosure review committee
- Created new documentation to define roles, requirements, and authority for the materiality determination, as well as FBI guidance for seeking extensions
- Tested new processes through workshop with the assessment group
- Standardized and documented process for assessing “related incidents”

#2 Continuous Learning

- The challenge of securing a set of entities with disparate risk profiles
- Leverages entity-based risk profiles and then a global risk categorization scheme
- Building on existing processes, including the IR module in ServiceNow

It’s better to think through these things when you’re not under a four-day clock. You’ll learn a lot and you just get way better prepared for an actual decision.

- Member Counsel

“The biggest challenge is having a third party that discloses, raising a lot of questions about how that impacts us.”

- Member CISO

Final Thoughts on Working with the Board

- Educate them early on the external and internal disclosure standards
- Agree on reporting scope and cadence in advance

About the ACSC

The Boston-based ACSC advances member cyber defense strategies through regional, national and global practice-sharing networks of industry leaders and provides professional opportunities for rising talent.

Contact Us
(617) 485-1112
wguenther@acscenter.org