Cybersecurity Best Practices for Recent SEC Ruling & PCAOB Focus Areas for IT

IT Risk & Compliance

IIA – Atlanta | June 28, 2024

forvis mazars

Stephanie Jarvis, CPA, CISA, ISO 27001 Senior Lead Auditor

Director / IT Risk & Compliance

- Focus areas
  - PCAOB Audits
  - Cybersecurity
  - ISO 27001 Compliance

Zach Shelton, CISA, CDPSE

Principal / IT Risk & Compliance

- Focus areas
  - PCAOB Audits
  - Cybersecurity
  - Internal IT Audit
  - IT SOX

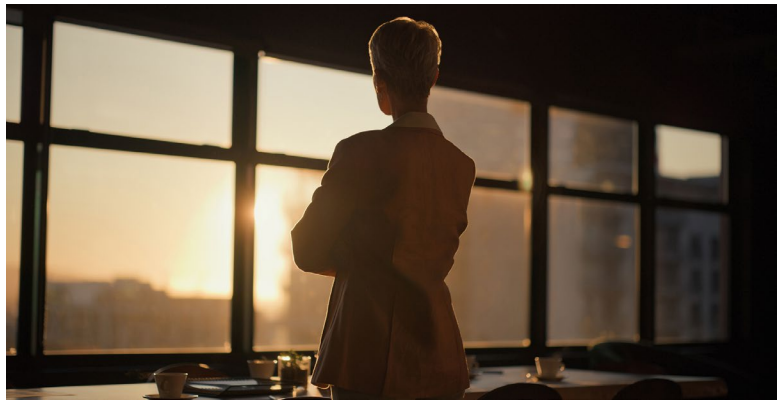
IIA Atlanta
Learning Objectives

01

Revisit the 2023 SEC Cyber Disclosure Ruling Requirements

02

Discuss Best Practices for Management Response Procedures to the Cybersecurity Disclosure Ruling



03

Dive into recent PCAOB focus areas for IT

Agenda

- 01 - Overview of the 2023 SEC Cybersecurity Disclosure Ruling
  - Recent SEC Cease & Desist Order
  - How has the new cybersecurity ruling impacted management's day to day?
- 02 - Preparing for Cybersecurity Considerations in Audit
- 03 - PCAOB Focus Areas for IT
- Q&A Session

01

Overview of the 2023 SEC Cybersecurity Disclosure Ruling

Reminder – SEC New Final Rule

"Cybersecurity Risk Management, Strategy, Governance, & Incident Disclosure"

The SEC cyber disclosure rule, released July 2023, requires publicly traded companies to disclose a breach within **four** business days of determining the breach was **material** to the company with exception if the US Attorney General determines immediate disclosure would pose a substantial risk to national security.

Companies must **outline** their cyber strategies, **address** how the organization handles and addresses threats, and **provide** the details of their cyber risk management and governance programs annually in their 8-Ks and 10K.

In addition, it requires publicly traded companies to reveal what board-level involvement there is in cybersecurity or what cyber expertise is held by members of the board. A recent study by Gartner shows by 2026, **70% of boards** will have a cyber expert . FORVIS foresees this percentage continuing to grow, hopefully leading to an improved level of cyber expertise throughout executive levels

Keen, Emma. "Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024." gartner.com, March 28, 2023

forvis mazars

Polling Question 1

Companies must outline their cyber strategies, address how the organization handles and addresses threats, and provide the details of their cybersecurity risk management and governance programs annually in their 8-Ks and 10-K.

A) True

B) False

Reminder – SEC New Final Rule

"Cybersecurity Risk Management, Strategy, Governance, & Incident Disclosure"

Required disclosures regarding (new Reg S-K Item 106):

- Processes to assess, identify, manage material cybersecurity risks
- Management's role in assessing & managing material cybersecurity risks
- Board's oversight of cybersecurity risks
- Required for fiscal years ending on or after December 15, 2023

New 8-K requirement (new Item 1.05):

- Disclose material cybersecurity events & related impact
- To be filed within 4 business days after determination that an event will have or is reasonably likely to have a material impact
- Required after December 18, 2023 (for SRCs required after June 15, 2024)
  - *SEC guidance on May 21, 2024 – If disclosing an incident for which materiality has not been evaluated yet, or has been determined to not be material, use a different Form 8-K, e.g., Item 8.01*

What is a material cybersecurity incident?

In securities law, **materiality** is generally understood to be when there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would significantly altered the total mix of information made available.

The SEC notes that an accidental occurrence is an unauthorized occurrence, even if there is no confirmed malicious activity. For example, if a customer's data is accidentally exposed, allowing unauthorized access, the data breach would constitute a cybersecurity incident that would require a materiality analysis to determine if disclosure is required.

Companies should be assessing both qualitative and quantitative factors when assessing materiality."

PCAOB Spotlight Staff Priorities for 2024 Inspections

Cybersecurity

PCAOB Spotlight – Staff Priorities for 2024 Inspections & Interactions with Audit Committees

The risk of cybersecurity attacks for public companies and broker-dealers is always present and increases for those who have not understood their vulnerabilities and are unprepared to identify and react to cyber incidents when they do occur.

For audits selected for review, PCAOB will request that auditors discuss how cybersecurity risk is considered and incorporated, if applicable, into the planned audit response.

For audits selected for review where a cyber incident has been identified, PCAOB will review how the firm evaluated the public company's response, including how the firm may have modified its planned audit response.

We will also review the incident disclosure made in compliance with the U.S. Securities and Exchange Commission rules requiring, among other things, public companies to disclose material cybersecurity incidents they experience and the audit firm's related audit response, if appropriate.

SEC Cease & Desist Order as of 6/18/24
Cybersecurity

R.R. Donnelley & Sons Co. (sec.gov)

1. This matter concerns violations by RRD of the Exchange Act's disclosure controls and procedures and internal accounting control provisions relating to its **cybersecurity practices** between **November 2021 and January 2022 (the "Relevant Period").** Throughout the Relevant Period, RRD **failed to design effective disclosure controls and procedures** as defined in the Exchange Act rules related to the disclosure of cybersecurity risks and incidents. RRD also **failed to devise and maintain a system of cybersecurity-related internal accounting controls sufficient to provide reasonable assurances that access to RRD's assets** – its information technology systems and networks, which contained sensitive business and client data – was permitted only with management's authorization.
   - Due to RRD's business of storing and transmitting large amounts of data, including sensitive data, information technology and cybersecurity are critically important to RRD. As a result of these internal accounting controls deficiencies, RRD failed to **execute a timely response to a ransomware network intrusion** that occurred between **November 29, 2021 and December 23, 2021**, which culminated in encryption of computers, exfiltration of data, and business service disruptions.
2. Based on the foregoing conduct, and the conduct described herein below**, RRD violated Exchange Act Section 13(b)(2)(B) and Rule 13a-15(a).**

The Ruling's Impact on Management

"How has the new cybersecurity ruling impacted management's day to day?"

- Increased External Audit Procedures
- Enhanced Cybersecurity& Incident Management Policies & Procedures
- Documented Analysis on Materiality Evaluation and Conclusion
- Adoption of tools supporting expedited response time for incidents to allow for timely detection, classification, and disclosure
- Increased training needs for management and control owners
- Additional Third-Party System Vendor Management Practices

"Only four days to disclose a breach"

forvis mazars

Polling Question 2

Within how many days does a publicly traded company have to disclose a breach when determined material to the company?

A) Three

B) Four

C) Ten

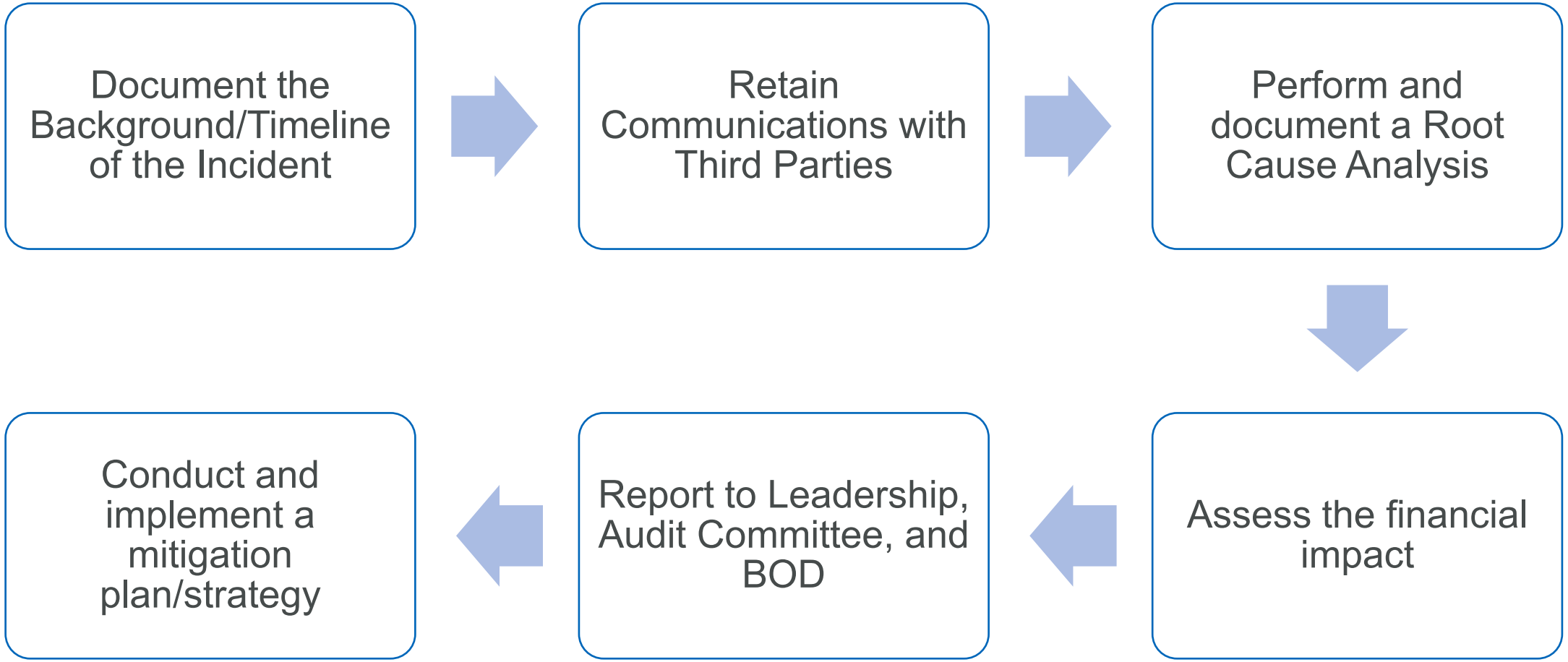
D) Thirty

02

Preparing for Cybersecurity in Audit

Preparing for Cybersecurity in Audit

Steps Management should consider taking for the Audit *when* a cyber incident occurs?



Preparing for Cybersecurity in Audit

Examples of Documentation Auditors should obtain

- Example correspondence to the impacted customers
- Communications with banking regulators
- Public disclosures made by the organization
- Root cause analysis / deliverable
- Analysis on customer accounts and the organizations' financial statements
- Formal reports, presentations, meeting minutes, etc. where a breach/compromise was discussed with governance
- Demonstrate/evidence mitigation strategies taken to prevent the incident from recurring in the future

Polling Question 3

Which of the following documentation examples should management retain when there is a cybersecurity breach?

A) Example of correspondence to the impacted customers

B) Root cause analysis / deliverable

C) Formal reports, meeting minutes where the breach/compromise was discussed with governance

D) Analysis on the customer accounts and the organization's financial statements

E) None of the above

F) All of the above

03

PCAOB Focus Areas for IT

Forvis Mazars' Insight on the PCAOB Examination's Focus on IT

Increased

demonstration of maturity of SEC elements for cyber risk management & strategy, cyber incident reporting, cyber governance

Increased

scrutiny over documentation supporting management's understanding of the completeness and accuracy of their documentation supporting management's IT SOX control series

Increased

analysis over the precision of the control and whether it operates at the right level to mitigate the risk

Increased

documentation supporting management's reliance on third party vendors for outsourced applications/ systems

Increased

scrutiny over control failures and compensating and/or mitigating controls analysis performed to determine whether a control deficiency, significant deficiency, or material weakness exists and impact to downstream financial operations and controls

Increased

emphasis over management tools used in the performance of key-SOX controls

Discussion Question

What IT requests have you felt unprepared or just find *difficult* to provide to Auditors / Regulators?

forvis mazars

Contact

Forvis Mazars

Stephanie Jarvis
Director
stephanie.jarvis@us.forvismazars.com

Zach Shelton
Principal
zach.shelton@us.forvismazars.com