Deloitte.

Cybersecurity

View from an External Auditor

February 18, 2022

Objectives

Overview

- Identify the current state of cybersecurity, its policies, and governance.
- Identify cybersecurity risk considerations.

Cybersecurity in practice

- Discuss real-world cybersecurity incidents and explore how cyber threats can impact business operations.
- Identify resources to help improve cybersecurity practices and better manage cyber risk.

Cybersecurity: Current state and what more can be done

Cybersecurity: Current state and what more can be done

PCAOB issued the following observations in their speech from May 2019:

Good Practices

- Establish a network of specialized professionals to address emerging risks.
- PCAOB has seen audit quality increase and the improved application of professional judgment when audit firms use **subject matter experts** (SMEs) to address new and emerging risks as well as complex and challenging areas, such as technology and new accounting standards.

For example, some audit firms have established a group of cybersecurity experts to serve as specialists if a company they are auditing has experienced a cybersecurity incident.

General Observations

- Cybersecurity risk - In approximately *10 percent* of the audits we inspected, the company had experienced a cybersecurity incident during the audit period, many of which related to malware and email phishing scams. Not every incident we observed had a financial statement impact. Nevertheless, auditors generally considered the cybersecurity incident in their risk assessments and modified their audit procedures, as needed, to address the potential impact on relevant controls and the data generated by the company's information technology systems.

As part of the risk assessment process, it is important for auditors to take steps to become aware of cybersecurity incidents at the companies they audit.

Source: Kathleen Hamm, PCAOB, Cybersecurity: Where We Are; What More Can be Done? A Call for Auditors to Lean In, May 2 2019

Cybersecurity: Current state and what more can be done

"…auditors should consider cybersecurity as part of their audit risk assessment"

"If the auditor identifies a risk related to cybersecurity… auditor should then design and execute procedures to address those risks"

Understand the why when assessing the potential entry points and attack surfaces

"… auditor should also understand the methods used by the company to prevent and detect cyber-incidents that could have a material effect on the financial statements…"

"… areas of focus should include the company's processes to assess and address material cyber-incidents once identified. Understanding how the company ensures timely evaluation and reporting up the management ladder of material cyber-incidents. It also includes how the company ensures appropriate escalation to the board and timely consideration of disclosure obligations to investors and others."

Think broadly

"…. an auditor should be clear-eyed about the risk that attackers can operate under the guise of legitimate users."

Source: Kathleen Hamm, PCAOB, Cybersecurity: Where We Are; What More Can be Done? A Call for Auditors to Lean In, May 2 2019

Cybersecurity and securities laws

The SEC issued the following observations in their speech from January 2022:

Team Cyber

- SEC's Division of Examinations (EXAMS) has issued Risk Alerts and statements regarding cybersecurity topics and delivered a report in 2020 on Cybersecurity and Resiliency Observations. This work helps SEC registrants and the public prepare for and manage some of these cyber risks.

Policy

- **Three parts of cybersecurity policy at the SEC**:
  - cyber hygiene and preparedness
  - cyber incident reporting to the government
  - in certain circumstances, disclosure to the public
- **Policy relates to the following entities**:
  - SEC registrants in the financial sector, such as broker-dealers, investment companies, registered investment advisers, and other market intermediaries
  - Public companies
  - Service providers that work with SEC financial sector registrants but are not necessarily registered with the SEC themselves
  - The SEC itself

The SEC has a key role as the regulator of capital markets. One of their goals is to maintain orderly markets.

"Cybersecurity is a team sport" – Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA)

Source: SEC, Gary Gensler, Cybersecurity and Securities Laws, January 24 2022

KNOWLEDGE CHECK

01

What option below is NOT part of cybersecurity policies at the SEC?

A. Cyber hygiene and preparedness

B. Cyber incident reporting to the government

C. Disclosure to the public

D. International data transfer

Cybersecurity and external audit

Cybersecurity and external audit

- The external auditor considers cybersecurity in two key contexts: **(1)** the audits of financial statements and, if applicable, ICFR; and **(2)** other disclosures.
- Financial information is a subset of the broad universe of information used by entities to support business operations; accordingly, cybersecurity risk is a broad business risk to be managed.
- Cyber incidents are increasing in frequency and complexity; therefore, cybersecurity controls, including GITCs, are increased areas of focus.
- Management and auditors focus on the controls and systems that are the closest to financial information (i.e., systems and applications that house and process financial transactions). Auditors should consider cybersecurity risk as it relates to these systems.

Management's cybersecurity program and controls

The root cause of certain cyber breaches can be attributed to ineffective GITCs. GITCs are important to financial reporting and to managing cyber risk.

Cyber threat considerations – BEC scams

The SEC issued an investigative report on October 16, 2018, that cautioned companies to consider cyber threats when they are implementing their internal accounting controls.

The report focuses on the internal accounting controls of nine issuers in a range of sectors "that were victims of one of two variants of schemes involving spoofed or compromised electronic communications from persons purporting to be company executives or vendors," commonly referred to as business e-mail compromise (BEC) scams.

What is a **BEC scam**?

BEC scam occurs when attackers use compromised or fraudulent e-mail addresses to target specific employees within organizations and ask them to participate in what appear to be legitimate transactions or to make changes to key payment or vendor information.

How does a BEC scam occur?

Using publicly available information. Six types of BEC scams are prevalent:

- Changed vendor payment details
- Changed employee payroll details
- Email Replication
- Fraudulent email request
- Executive/attorney impersonation
- Data theft

A pervasive theme in BEC scams is that an individual employee gives the hacker access to an e-mail account, generally by clicking a link in an e-mail or by downloading a file through a phishing attack. A BEC scam can also occur when an employee completes a requested action based on a fraudulent or spoofed e-mail.

How can BEC scams be identified and avoided?

Both General IT Controls and Business Process Controls should be considered:

- Multi Factor Authentication — IT access
- Virtual private network
- Authorization verification controls
- Review of vendor or employee master file changes
- Change confirmation

What controls may help prevent or detect BECs?

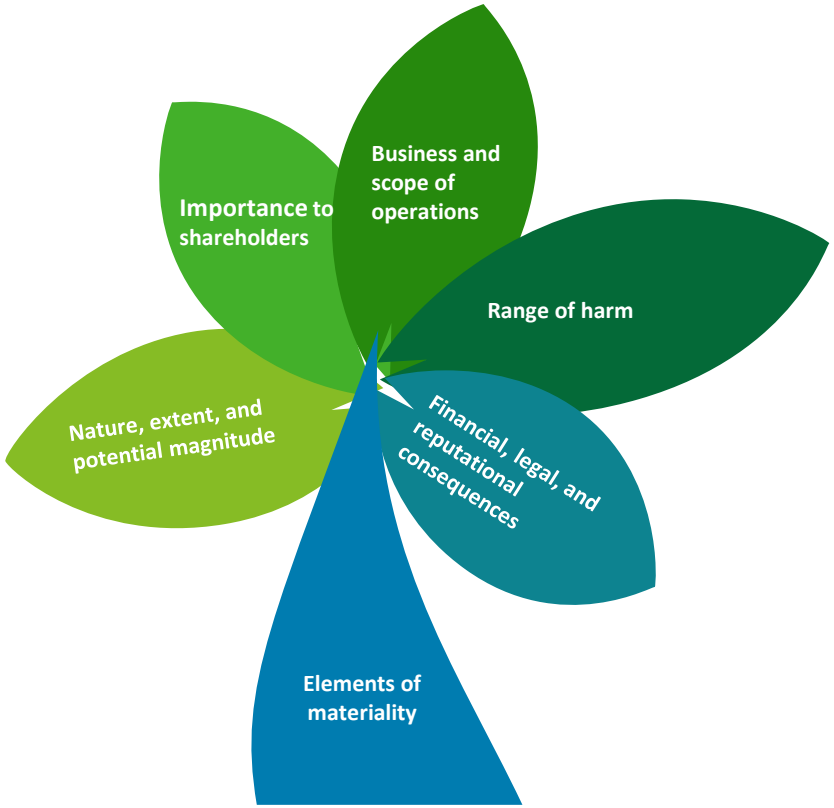
Key take-aways

- Cybersecurity landscape continues to evolve, and as more economic activities take place through digital technology and electronic communications
- BEC examples described above underscore the importance of devising and maintaining a system of internal accounting controls to address this kind of cyber-related fraud
- Training and user security awareness are key

Source: SEC, Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls, October 16 2018

Cybersecurity disclosures and materiality

SEC guidance emphasizes that companies should consider the materiality of cybersecurity risks and incidents when preparing disclosures.



Nature, extent, and potential magnitude

The 2018 guidance notes that the magnitude of cybersecurity risks or incidents depends on, among other things, their nature, extent, and potential magnitude

Importance to shareholders

Consistent with the standard of materiality articulated by the Supreme Court, the 2018 guidance holds that a fact is material if there is a substantial likelihood a reasonable shareholder would consider it important

Business and scope of operations

The 2018 guidance notes that the materiality of cybersecurity risks and incidents is related to a company's business and scope of operations

Range of harm

The 2018 guidance emphasizes that the materiality of cybersecurity risks and incidents depends on the range of harm that such incidents could cause, and urges companies to consider the indicated probability that an event will occur

Financial, legal, and reputational consequences

The Commission expects companies to disclose cybersecurity risks and incidents that have financial, legal, or reputational consequences

Ransomware typical root causes

Phishing emails were sent to company users, who unknowingly clicked on links that downloaded malicious software and introduced a ransomware attack. The users clicked on the link due to lack of end-user security awareness.

The company has **servers on an older operating system** with inherent vulnerabilities that were exploited by bad actors to gain access.

Operating system **domain administrator account passwords** were not properly secured, which allowed the bad actors to obtain administrator credentials. For example, a service account password was not changed from the vendor default or was stored in plain text. Another example is an account having inappropriate domain administrator access.

The company did not apply **vendor patches/updates** in a timely manner, therefore their servers/systems were susceptible to known vulnerabilities that were exploited by bad actors to gain access.

The **firewall** was not configured appropriately to restrict external users from gaining access to the company network.

The company's **antivirus** control did not perform at an appropriate level of precision to protect their technology from threats (viruses, malware, ransomware, etc.).

The bad actors obtained valid user credentials through **phishing** (or another mechanism). Since the company did not have multi-factor authentication in place, there was no second level of authentication to prevent the bad actors from gaining access to the company's network/systems.

KNOWLEDGE CHECK

02

All of the following are examples of cybersecurity attacks, EXCEPT?

A. Phishing

B. BEC Scam

C. Phone call from Scammer

D. DDoS

Ransomware events

Ransomware case

Ransomware case – ABC Company

- In 2020, ABC Company detected a ransomware attack that accessed and encrypted a portion of the company's systems. The attackers downloaded certain data files. Upon detection of the attack, the company launched an investigation, notified law enforcement, and engaged legal counsel and other incident response professionals. Throughout the investigation, the company implemented a series of containment and remediation measures to address the situation and reinforce the security of its systems. The company worked with several cybersecurity firms to immediately respond to the threat, defend the company's systems, conduct remediation, and help assess the overall impact of the attack.

- Based on the assessment of the attack, the company does not believe the incident will have a material impact on its business, operations or financial results. Nonetheless, the company expects that the event included unauthorized access to personal data of customers and employees, which may result in potential claims from customers, employees, shareholders, or regulatory agencies.

- Although the company believes that no other systems of the company's entities have been impacted by this incident, there can be no assurance that other systems were not adversely affected.

Note: The above case is a fictious case and ABC company does not exist

Recent cyber events

Log4J Vulnerability

- A remote code execution vulnerability was identified in Apache Log4j.
- The vulnerability can be exploited remotely without authentication.

Service Provider Breach

- A service provider was the target of a ransomware attack, which took their cloud-based systems offline and impacted lots of customers.
- Systems were offline for several weeks.

KNOWLEDGE CHECK

03

What does PII stand for?

A. Postal Identity Information

B. Personal Identifiable Information

C. Public Identify Information

D. Private Identity Intelligence

Resources

Cybersecurity resources

- **Center for Audit Quality**
  - https://www.thecaq.org/cybersecurity-risk-management-oversight-tool-board-members/
  - https://www.thecaq.org/understanding-cybersecurity-and-external-audit/
  - https://www.thecaq.org/emerging-technologies-risk-and-the-auditors-focus-a-resource-for-auditors-audit-committees-and-management/
- **COSO guidance on managing cyber risks in a digital age**
  - https://www.coso.org/Documents/COSO-Deloitte-Managing-Cyber-Risk-in-a-Digital-Age.pdf
- **Center for Board Effectiveness Thought Leadership → Cyber Risk**
  - https://deloittenet.deloitte.com/cm/boardeffectiveness/pages/thought-leadership.aspx
- **Heads Up on SEC Interpretive Guidance on Cybersecurity Disclosures**
  - https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/ASC/HU/2018/us-aers-hu-in-the-spirit-of-full-cybersecurity-disclosure.pdf
- **AICPA Cyber Exam**
  - https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity/soc-2-vs-cyber-whitepaper-web-final.pdf
  - https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative.html
- **National Association of Corporate Directors (NACD)**
  - https://www.nacdonline.org/
  - https://www.nacdonline.org/insights/publications.cfm?ItemNumber=10687

Questions?

Deloitte.

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.