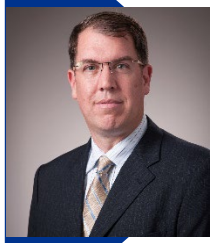
KPMG

SEC Proposed Cybersecurity Disclosures

July 2022

With you today

Tyler Williamson
Director Advisory
Technology Risk Management
Atlanta
E: twilliamson@kpmg.com
P: 863-860-8366



Dr. Aaron Kemp
Director Advisory,
Technology Risk Management
Atlanta
E: aaronkemp@kpmg.com
P: 404-221-2358

Agenda

A. Background
B. Key Terms
C. Guidance
D. Role of IA
E. Questions
F. Case Studies
G. Perspectives

Background

- **Cybersecurity risks have increased significantly over the last few years:**
  - Digitalization of organizations operations
  - Increased remote work (COVID-19)
  - Ability of cyber criminals to monetize security incidents (ransomware, stolen data, crypto)
  - Increasing reliance on third party providers
- **In 2019, CEOs rated cybersecurity as the biggest threat to business growth and the international economy**
- **Cost to companies due to cybersecurity incidents is rising exponentially:**
  - Costs due to business interruption, decreases in production, and delays in product launches
  - Payments to meet ransom and other extortion demands
  - Increased cybersecurity protection costs
  - Damage to the company's competitiveness, stock price, and long-term shareholder value
- **There are currently no disclosure requirements in regulation S-K or S-X that refer to cybersecurity incidents**
- **SEC believes investors would benefit from timely and consistent disclosure about material cybersecurity incidents**

Key Terms

Information Systems

— Information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of the registrant's information to maintain or support the registrant's operations.

Cybersecurity Threat

— Any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

Cybersecurity Incident

— An unauthorized occurrence on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity or availability of a registrant's information systems or any information residing therein.

Proposed New Rules

Given the current environment, the SEC has determined new standards for reporting should be applicable. It must be noted that these standards are in the comment phase at this moment and are not policy!

- Reporting cybersecurity incidents on a Form 8-K
- Disclosing cybersecurity incidents in periodic reports
- Disclosing cybersecurity policies and procedures
- Disclosing management's role in cybersecurity governance
- Disclosing cybersecurity oversight by the board of directors and the director's expertise

Proposed Rules – Cybersecurity Incidents

Reporting cybersecurity incidents on a Form 8-K

— Proposal would introduce Item 1.05 to specifically require disclosure of specified information about a material cybersecurity incident within four business days of the organization determining the incident was material (not within four days of the incident occurring).

Disclosing cybersecurity incidents in periodic reports

— Amendments to Forms 10-K and 10-Q would require periodic updates on material incidents by disclosing material changes, additions or updates of incidents previously disclosed on Form 8-K, as well as disclosure of previously undisclosed immaterial incidents when material in the aggregate.

Proposed Rules – Risk Management, Strategy, and Governance

Disclosing cybersecurity policies and procedures

— Proposal would require disclosures about policies and procedures on cybersecurity risk management and strategy in Form 10-K.

Disclosing management's role in cybersecurity governance

— Proposal would require description of management's role in assessing and managing cybersecurity-related risks and in implementing cybersecurity policies, procedures and strategies, including the designation of cybersecurity expertise within management in Form 10-K.

Disclosing cybersecurity oversight by the board of directors and the director's expertise

— Proposal would require disclosure of the board's oversight of cybersecurity risk and board member cybersecurity expertise (if any) in annual reports and certain proxy filings.

CPE Question 1

Which of the proposed SEC rules will be most difficult for you organization to meet?

1. Reporting cybersecurity incidents on a Form 8-K (4 business days)
2. Disclosing cybersecurity incidents in periodic reports
3. Disclosing cybersecurity policies and procedures
4. Disclosing management's role in cybersecurity governance
5. Disclosing cybersecurity oversight by the board of directors and the director's expertise

Materiality

A key challenge for companies will be to identify incidents that are in fact reportable events. To that effect, the SEC offers limited guidance and no quantitative thresholds for reporting. The following guidance will need to be evaluated by the organization and acted on if determined to be appropriate

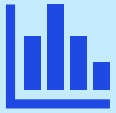
Incidents must be reported within four business days after materiality has been determined

Materiality

Incidents are material if:

There is a substantial likelihood that a reasonable shareholder would consider it important

It would have significantly altered the total mix of information made available



An organization needs to thoroughly and objectively evaluate the total mix of information, considering all relevant facts and circumstances surrounding the cybersecurity incident (including both quantitative and qualitative factors) to determine whether an incident is material

Examples of Incidents Requiring Disclosure

- An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset
- An unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems
- An incident in which an unauthorized party accessed, altered, or has stolen sensitive business information, personally identifiable information, intellectual property
- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data
- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered

These examples are not inclusive of all cyber incidents which may need to be disclosed and are for illustrative purposes only.

Role of Internal Audit

- **Aid in developing and implementing policies and procedures to meet disclosure requirements**
- **Assist with organizational readiness performing audits to identify gaps for leadership**
- **Assist in developing robust policies and procedures to identify, assess, and manage cybersecurity risks**
  - New guidance requires organizations to share policies and procedures to provide transparency to investors about the organizations strategies and actions to manage cybersecurity risks
  - Cybersecurity strategy can have a significant impact on business strategy, financial outlook, and financial planning
- **Determine if organizations are implementing cybersecurity policies and procedures as designed**
- **Assist in developing criteria to determine if a cybersecurity incident is material**
- **Assist in developing cybersecurity training programs**

Organization Disclosure Examples:

— **While this list is not inclusive the below examples provide some examples of what information will need to be provided by the organization**

If there is a cybersecurity risk assessment program and if so, provide a description of such program	**If the organization engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program**	**The policies and procedures which oversee and identify the cybersecurity risks associated with its use of any third-party service provider including how cybersecurity considerations affect the selection and oversight of these providers**	**If the organization undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents and has business continuity, contingency, and recovery plans in the event of a cybersecurity incident**	**Previous cybersecurity incidents have informed changes in the organization's governance, policies and procedures, or technologies and how incidents have affected operations or financial conditions**	**Cybersecurity risks are considered as part of the organization's business strategy, financial planning, and capital allocation and if so, how**

Roles of Leadership

Organizations must disclose their Cybersecurity Governance and:

Board Responsibilities	Cybersecurity Awareness	Cybersecurity Priority	Cybersecurity Leadership	Cybersecurity Status
Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks	The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic	Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight	Whether the registrant has a designated chief information security officer	The processes by which leadership committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents

CPE Question 2

What is an example of a incident that would need to be reported 4 business days under the proposed SEC guidance?

1. A shortage of computer hardware to upgrade corporate laptops
2. An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset
3. A four hour outage due to a hurricane at a peripheral site
4. None of the above

KPMG

Questions?

Case study 1 – Large retailer

- Who?
  - Suspected to be Russia/Ukrainian hackers that also breached another retailer
- Type of attack?
  - Malware to collect emails and payment card information
- How did the breach occur?
  - Hackers entered through a Vendor using a name and password
    - Hackers worked during normal business hours moving laterally and vertically until the found the information they were looking for
    - Hackers used a variant of BlackPOS malware
- Reaction?
  - 52 million email addresses stolen
  - 40 million payment cards stolen
  - Biggest retail credit card breach in U.S. history

Case study 2 – Software company

- Who?
  - Linked to Russia's Foreign Intelligence Service (SVR)
- Type of attack?
  - Advanced Persistent Threat (APT) leading to Malware attacks
- How did the breach occur?
  - Attack was on the control system and changes were made to updates that were then sent to 33,000+ customers
    - Hackers were able to install a back door in the software updates
    - Once installed the backdoor allowed more malware to be installed
    - Allowed hackers to spy on companies and organizations
- Reaction?
  - Thousands of clients forced to take systems offline for patching and remediation
  - Scope of spying and breadth of malware is still unknown
  - Homeland Security has said it could be years before government networks are secure again

Case study 3 – Gas and utilities company

- Who?
  - Linked to Russian hacking gang DarkSide
- Type of attack?
  - Ransomware
- How did the breach occur?
  - Attack was linked to a single password that was stolen
    - Allowed access to a legacy VPN
    - Did not have multifactor authentication in place
- Reaction?
  - Company was forced to shut down parts of their infrastructure
  - Knocked billing systems offline
  - Paid 75 bitcoin (worth more than $4 million at the time) to get ransomware key
- **Attack was one of the largest disruptions of US critical infrastructure**

CPE Question 3

Under the proposed SEC guidance you would not be required top report an material incident until you had completely resolved the situation?

1. True
2. False

KPMG

Perspectives

Thank you

kpmg.com/socialmedia