SKYHAWK SECURITY

A Simple Checklist to Start Compliance Initiatives

SEC Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Introduction

The U.S. Securities and Exchange Commission's ("SEC") new rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (the "Cybersecurity Rules") came into effect on effect on December 15, 2023[1].

These new rules apply to public companies, or more specifically: corporations, limited liability companies, and partnerships that are subject to the regulations and disclosure requirements of the Securities Exchange Act of 1934, and to business development companies subject to the Investment Company Act of 1940 (collectively, "registrants" or "public companies"). This document helps security leaders understand and collaborate with other C-level executives on these new rules and the RACI on page X helps clarify roles and responsibilities.

On January 8, 2024, LoanDepot disclosed a cyberattack that shut down their systems[2]. The organization suffered a ransomware attack which impacted their business. The first reports or a material cyber incident were from Clorox on August 14, 2023[3].

Why the change?

The need for updating the reporting guidelines became evident in recent years as more and more publicly traded companies were affected by cyberattacks. These could seriously impact a business and could influence an investor's decision to invest or not. However, most of the information regarding breaches is not available in a timely and reliable fashion to make an investment decision, like whether or not to sell the stock they own.

82%

of breaches involved data stored in the cloud.[4]

The SEC lists four key factors as to why it updated these guidelines.

First, the dependency on electronic systems for operating modern businesses and the potential adverse impact of large-scale attacks on such systems. Technology is prevalent in business, from small businesses with just a few employees, all the way to organizations with thousands of employees globally. Technology is a staple in all businesses. A recent survey of businesses showed that 99% say they are using at least one digital technology in their day-to-day operations[5].

Second, the rise in the number and severity of cyber incidents driven by modern work trends (work from home), reliance on third-party service providers and proliferation of cybercrime activities. With people working from home, security teams are no longer in complete control of security policies and practices. Additionally, when a breach involves multiple environments, it becomes more complex. It can take up to 291 days to identify and contain breaches across mulitple environments[6].

1. https://www.sec.gov/news/press-release/2023-139
2. https://www.scmagazine.com/news/loandepot-discloses-cyberattack-shut-down-systems-in-sec-filing
3. https://www.csoonline.com/article/653983/companies-are-already-feeling-the-pressure-from-upcoming-us-sec-cyber-rules.html
4. https://www.ibm.com/downloads/cas/E3G5JMBP
5. https://www.businessdit.com/technology-in-business-statistics/
6. https://www.ibm.com/downloads/cas/E3G5JMBP

Third, the increased costs and adverse consequences of cybersecurity incidents to companies. If a company is breached, there are significant costs incurred. A ransom could be millions of dollars. In fact, the largest known ransom paid was $40 million[7]. Although that is by far the highest amount, the average cost of a data breach is still in the millions, averaging around $4.45M in 2023[8].

Finally, the SEC also wished to update its reporting guidelines to align with other governing bodies such a CISA Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") that requires companies which are part of the critical infrastructure sectors to report cyber incidents to CISA within 72 hours of discovery, and report ransom payments within 24 hours.

The new guidelines take a more holistic approach to registrants' cybersecurity apparatus on their business. It now requires both incident reporting and ongoing, annual reporting of the sturcture of cybersecurity risk management program. This enables investors to see how an organization manages and responds to security threats and enables investors to make more informed investment decisions.

Material

Prior to the rule update, SEC reporting obligations were voluntary and allowed responded corporations greater discretion, especially when determining whether a cybersecurity incident was "material" to the business. In the view of the SEC a "material" cybersecurity incident is one where there is a substantial likelihood that a reasonable investor would attach importance in determining whether to buy or sell the securities registered.

Each coroproation must devleop their own standards for materiality and apply them consistently in their evaluation of incidents. The SEC does not detail how the materiality of an incident should be evaluated. Examples of incident impacts which cloud be material include business interruption, lost revenue, ransom payments, remediation costs, liabilities to affected parties, cybersecurity protection costs, lost assets, litigation risks, and reputational damage. Companies should probably take all these - and more - into consideration when assessing the potential materiality of an incident. In addition, in another section of the document[9], the SEC highlights the importance of identifying "key systems and information, such as those the company considers its 'crown jewels'". Any impact on these could be considered material.

The changes

The new guidelines affect both scheduled and unscheduled reports.

Ongoing reporting:
Registrants must disclose their internal cybersecurity risk management practices in their annual reports (regulation s-k item 106(b)) , including detailed descriptions of the following:

- Processes used by the Board of Directors to oversee cybersecurity risks, such as appointment of board committees and standardized reporting on cybersecurity risks to the Board and/or appropriate Board committee.
- Management's role in assessing and managing material risks from cybersecurity threats, including designation of specific positions such as CISOs and/or committees, the processes used to stay informed of cybersecurity incidents and monitor their prevention, detection, mitigation, and remediation; and reporting obligations to the Board of Directors and/or a Board committee.
- Security assessments. Registrants are required to describe their processes (if any) for assessing, identifying, and managing material risks from cybersecurity threats. Further, registrants must undertake an assessment of whether any risks from cybersecurity threats, including risks from previous incidents, have materially affected them or are reasonably likely to materially affect them in the future. The assessments should be appropriately documented to accommodate any regulatory inquiries.

7. https://www.varonis.com/blog/ransomware-statistics#:~:text=In%202021%2C%20the%20largest%20ransomware,(NetApp%2C%202022)
8. https://www.ibm.com/reports/data-breach
9. https://www.sec.gov/files/rules/final/2023/33-11216.pdf

Unscheduled reporting:
In case of an incident resulting in a material impact, the corporation must file an 8-K (Item 1.05), or 6-K for foreign organizations, report of unscheduled material events or corporate changes, including the material aspects of its nature, scope, timing, and impact (or reasonably likely material impact) on the registrant[10]. An incident is defined as: "An unauthorized occurrence, or a series of related unauthorized occurrences, 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.".

With regards to timeline of reporting:

- Registrants must determine if a cybersecurity incident is material "without unreasonable delay" after discovery of the incident.
- Material cybersecurity incidents must be disclosed (Form 8-K or Form 6-K for foreign organizations) no later than four business days after the determination of materiality.
- If relevant information is not yet available, registrants must include a statement to this effect and, within four business days after it becomes available, file an amendment that contains this information.

A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, but should include information about the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.

Registrants may request a delay in disclosure of cybersecurity incidents if there is an active law enforcement investigation regarding the incident or the U.S. Attorney General that disclosure impacts national security or public safety and notifies the SEC in writing[11].

What Should Registrants Do Now?

Given that companies should start including information about their cybersecurity preparedness in their annual reports, they should first establish internal processes to identify and mitigate cybersecurity threats (including incident response and business continuity plans). Then, they need to establish the criteria they will use to determine whether an incident is material. This should be done in an orderly manner, taking into consideration financial, legal, operational and other considerations. Lastly, they should identify and determine who will be the person (or committee) in charge of post-incident decision to report.

Do-now checklist

Task	Completed
Create a SEC Cybersecurity Task Force to lead a cross functional team to identify the process for reporting an issue. It should include legal, IT, SOC, risk, and finance teams. Add others as necessary.	
Create tiger teams to tackle specific issues:	
1 CISO meets with CFO/GC to discuss cybersecurity support for assessment of the materiality of cybersecurity incidents. Outcomes- defined impact thresholds for escalation, minimum data set for escalation of an incident.	
2 CISO coordinates with GC to determine longevity of incident data storage to support and contain scope of longitudinal analysis of incident data to support aggregated incident detection and escalation	
3 CISO revises incident response plan to include collection, compilation and communication of incident data when any given incident triggers escalation for materiality assessment or when analysis reveals an aggregate incident which triggers aggregate impact thresholds	
4 CISO/GC/CFO plan and implement tabletop exercises to practice complete process from incident detection through to materiality assessment.	

10 https://www.sec.gov/files/rules/final/2023/33-11216.pdf
11 https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements

Figure A: Gartner® Quick Answer: New SEC Cybersecurity Rules – What CISOs Should and Shouldn't Do: Example RACI Chart[12]

Investors need timely, standardized, comparable and easy to locate disclosures regarding cybersecurity incidents, governance, risk management and strategy practices materially affecting registrants' businesses. The purpose of the cybersecurity disclosure rules is to inform investors, not to influence whether and how companies manage their cybersecurity risk.

Responsible: Those responsible for undertaking the work and completion of the task and for the successful end-to-end execution of that task on behalf of the Accountable individual. Every action must have at least one person responsible for its delivery.

Accountable: Is the "owner" of the work and ultimately accountable to senior management for the effective execution of the security process, but may not be involved in execution. This person must have the authority vested in them to ensure the task is completed. Every action must have no more or less than one person allocated as accountable for its execution.

Consulted: Is asked for advice or input that informs the execution of the action or task to ensure success.

Informed: Is informed about the execution of the security process from time to time. May or may not have any influence on its execution.

Responsible and accountable: Is responsible for doing the work required to execute the security process or activity end-to-end and is accountable for its success and failure.

ROLE (RACI)

All roles are informed (I) of all requirement by default

	This RACI table is a partial, non-prescriptive example of how responsibilities should be defined and allocated to appropriate roles within the corporation.	**BoD**	**CEO**	**COO**	**CFO**	**GC**	**CISO***
R E Q U I R E M E N T	Determination of incident materiality		C		C	A	
	Determination of risk materiality		C		C	A	
	Description of processes for identifying, assessing and managing material risks from cybersecurity threats (if processes exist)		C	C	C	C	R/A
	Determination as to whether cybersecurity processes are incorporated into overall risk management processes or systems			C	C		R/A
	Description of which cybersecurity processes, if any, are supported by assessors, consultants, auditors, or other third parties			C			R/A
	Description of cybersecurity processes for the oversight of third party risks from cybersecurity threats				C		R/A
	Determine whether any risks from cybersecurity threats have or are reasonably likely to materially affect the organization		C	C	C	A	C
	Description of board/subcommittee's oversight of risks from cybersecurity threats	C				A	
	Description of processes on how board/subcommittee is informed of material risks from cybersecurity threats	C	C		C	A	
	Description of management's role in assessing and managing material risks from cybersecurity threats		R/A	C	C	C	C
	Description as to whether individuals or committees are assessing and managing material risks from cybersecurity threats and their relevant expertise				C	A	C
	Description of processes on how individuals or committees are informed and can monitor the prevention, detection, mitigation and remediation of cybersecurity incidents					A	
	Determination as to whether individuals or committees report material risks from cybersecurity threats to the board/subcommittees					A	
	Collection and aggregation of incident information (includes information from third parties when available)						R/A
	Inline XBRL Tagging - 8-Ks *(required one year beyond initial compliance with the disclosure requirements)*				C	A	
	Inline XBRL Tagging - 10-Ks *(required one year beyond initial compliance with the disclosure requirements)*				C	A	
	Disclosure Filing of 8-Ks - Item 1.05 Material Cybersecurity Incidents (including amended 8-Ks)		R/A^	R/A^	R/A^	R/A^	
	Disclosure Filing of 10-Ks - Item 106 Cybersecurity		R/A^	R/A^	R/A^	R/A^	

NOTE THIS DOES NOT APPLY TO FOREIGN PRIVATE ISSUERS (FPIs)

*Owner of the Cybersecurity Program

^The SEC can hold responsible & accountable any officers of the corporation

Gartner®

12 Gartner, Quick Answer: New SEC Cybersecurity Rules - What CISOs Should and Shouldn't Do by Andrew Walls, Lisa Newbauer, Deepti Gopal, Leigh McMullen, William Candrick, Published January 11, 2024

Legal Disclaimer

This document provided by Skyhawk (CNP) Security Ltd. and/or its affiliates ("Skyhawk Security"), is intended for marketing, eduational, and informational purposes only. Skyhawk Security does not provide legal or investemnt advice, nor does it advise, recommend, solicit, or endorse any security, financial instrumetn, or investment deicision. Adherence to the recommendations herein does not guarantee complete and full compliance. this document is not intended as a comprehensive action plan, the information herein may not be complete and/or up-to-date and Skhaw Security expressly disclaims any responsibility for its use, nor for any damages or losses of any kind that may arise from reliance on it. As such, this document should not be construed or used as a specific guide to action, but instead as a preliminary, education step towards understanding and meeting SEC Cybersecuirty regulatory obligations.

Gartner Disclaimer

About Skyhawk Security

Skyhawk Security is the originator of Cloud Threat Detection and Response (CDR), helping hundreds of users map and remediate sophisticated threats to cloud infrastructure in minutes. Led by a team of cybersecurity and cloud professionals who built the original CSPM category, Skyhawk Security evolves cloud security posture management far beyond scanning and static configuration analysis. Instead, using advanced generative AI and ML sequencing of context-based behaviors, Skyhawk provides CDR within a 'Runtime Hub' to quickly detect and remediate malicious activities across multiple cloud platforms **as they happen**. Skyhawk Security is a spin-off of Radware® (NASDAQ:RDWR).

Contact us today to learn more at skyhawk.security

SKYHAWK SECURITY