CAP Group

SEC Cybersecurity Disclosure Rules

ADOPTION FRAMEWORK

August 2023

SEC Issues Final Cybersecurity Disclosure Rules

On July 26, 2023, the SEC issued its final rules that require registrants to provide enhanced and standardized disclosures regarding "cybersecurity risk management, strategy, governance, and incidents." The final rule addresses concerns over investor access to timely and consistent information related to cybersecurity risk driven by the continuing increase in the level and complexity of the threat environment. The pervasive use of digital technologies in operations, the expanding potential of artificial intelligence, the realities of hybrid work, the rise in the use of crypto assets, and the increasing threat of ransomware and stolen data – all combine to escalate cybersecurity risk and its related impact to registrants and investors.

SEC Final Rules

The final rules can be generalized into three key areas, with summary outlines for each as follows:

Cyber Governance

Describe the company's governance of cybersecurity risks as it relates to:

- The board's oversight of cybersecurity risk, including identification of any board committee or subcommittee responsible for oversight and the process by which they are informed about cyber risks.
- Management's role and expertise in assessing and managing material cybersecurity risk and implementing cybersecurity policies, procedures and strategies.
- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such person or members in such detail as necessary to fully describe the nature of the expertise.

Cyber Risk Management

Describe the process, if any, for assessing, identifying, and managing material risks from cybersecurity threats, including:

Whether cybersecurity is part of the overall risk management program.

Whether consultants, auditors or other third parties are engaged, and processes to oversee and identify risks from use of third-parties.

Whether and how any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect the registrant's business strategy, results of operations, or financial condition.

Cyber Incident Disclosure

Report "material" cybersecurity incidents on a Form 8-K within four business days of materiality determination. Note: Materiality determination should be based on federal securities law materiality, including consideration of quantitative and qualitative factors.

Describe the nature, scope, and timing of the incident and the material impact or reasonably likely material impact on the registrant. To the extent required information is not determined or is unavailable at the time of the filing, the 8-K should include disclosure of this fact, and the 8-K should be later amended when the information is determined or becomes available.

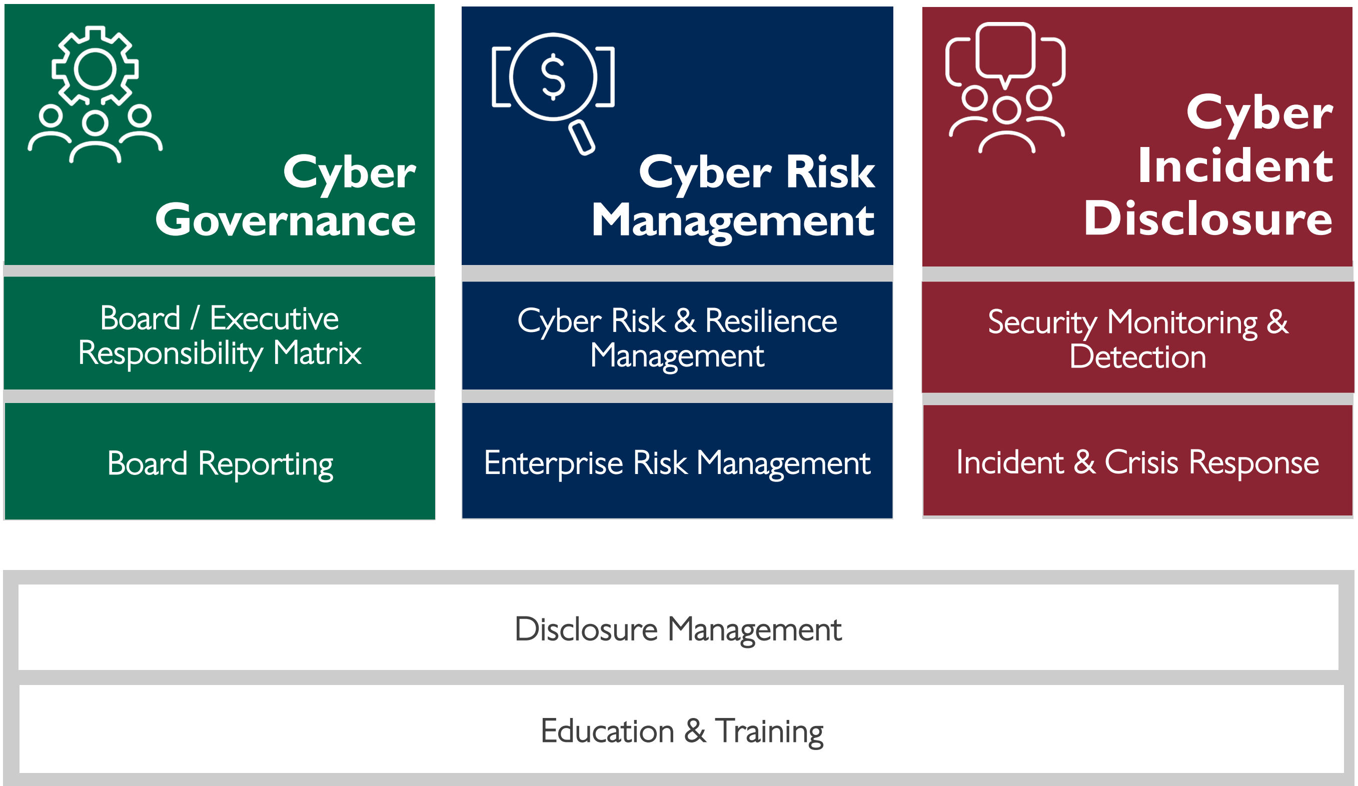
Key Impacted Capabilities

The SEC's final rules were released in July 2023 and significant action is likely required by December 2023. The rules incorporate the SEC's drive for companies to give investors **current, consistent, and "decision-useful" information** about how they manage cyber risk.

On the surface, the annual disclosure of required information may not seem difficult, but the practical realities involved in such revelations may be **significant**. Once published, the risk management strategy and processes will be highly scrutinized – and such disclosures are permanently in the public sphere. Informal processes, ambiguous terminology, or non-specific role definitions could quickly draw undesired attention from investors, competitors, or an array of potential plaintiffs.

Given this backdrop, we offer the following **key capabilities** that are the **most affected** and potentially require review or maturation prior to public disclosure. It is important to note that this is not intended to be an all-inclusive or a prescriptive guide to cyber risk management – that would consume many volumes. Rather, it is intended to be a targeted subset of the most time-critical areas for review.

Finally, it is important to recognize that these 3 areas represent an enterprise-wide perspective for managing cyber risk. Together and individually, these rely on deep, foundational underpinnings of the totality of the enterprise's capabilities and systems.. It is vital that the director and officer community understand these with sufficient fidelity to effectively monitor and manage cyber risk.



Cyber Governance

Board / Executive Responsibility Matrix

Board Reporting

Cyber Risk Management

Cyber Risk & Resilience Management

Enterprise Risk Management

Cyber Incident Disclosure

Security Monitoring & Detection

Incident & Crisis Response

Disclosure Management

Education & Training

Cyber Governance

Board / Executive Responsibility Matrix

The new rules specify the disclosure of the responsibilities of the board, any board-level committees, as well as management-level committees or positions that have key responsibilities regarding the management of cyber risk. The rules do not contain any prescriptive guidance on the number or form of such responsibilities; however, the following represent a common model that we leverage for this framework.

- **Full Board**: the full board is ultimately responsible for overseeing enterprise risk so a specifically documented schedule, attendees, and agendas will be vital. In addition, processes for handling exceptions and unplanned meetings should be included.
- **Board Committee**: given the quantity of information and the specialty of the expertise involved in managing cyber risk, many boards delegate cyber oversight to a committee for oversight. This committee often consists of directors with first-hand technology or cyber expertise and is a key contact for the Executive-Level Cyber Committee. A clear articulation of the members, scope and charter will provide context for the committee. In addition, routine schedules and a broad characterization of the meetings, agendas, and types of information provided should be included.
- **Executive-Level Cyber Committee**: separate from board committees, it is common to have a management-level committee that oversees digital risk at-large. Normally focused on cyber risk, cybersecurity, and privacy, this committee makes recommendations to the board on risk tolerance considerations and endorses budgets and other resources required by the CISO to execute approved strategies for mitigating cyber risk. Normally a cross-functional team involving IT, security, risk, audit, legal, and business operations, this team will also be the senior-most group responsible for policy and standard approval and granting of exceptions. A reasonable outline of this group, charter, members, and cadence should be included.

Board Reporting

The SEC rules specifically seek to explain how the board is informed of a registrant’s cyber risk situation. Based on a responsibility matrix as shown here, there are some broad expectations in terms of frequency and content of information provided upward – as well as directions and approvals downward – that should be outlined.

- **Full Board**: it is common for the board to receive key updates on a quarterly basis, often including both the Board Committee and the Executive-Level committees. Key updates regarding operating metrics – at a high level – as well as changes in risk situation and cybersecurity posture are normally reviewed.
- **Board Committee**: the board-level committee normally receives updates to the full committee (or a subset) on a monthly basis with sufficient detail on operating metrics, risk position, and security posture to provide transparency and support alignment between the board and management committees.
- **Executive-Level Cyber Committee**: this group normally meets monthly and is briefed by a cross-functional team including at least business operations, technology, security, risk, audit, and legal.

Cyber Risk Management

Cyber Risk & Resilience Management

The final rules clarified the expectations for disclosure – focusing on the overall process of cyber risk management across the enterprise. This topic is extremely broad and will have several sub-focus areas for consideration.

- **Risk Tolerance**: the board needs to define – in unambiguous terms – its tolerance for cyber risk and ensure that management defines clear strategies for delivering results in alignment with that expectation. While not mandated to be released in-detail, this baseline understanding is foundational to managing risk and resilience and for providing context in determining the materiality of incidents.
- **Risk Measurement**: the board and executive teams need to formalize the method for measuring cyber risk. There is significant variability in the approach used, with some choosing qualitative assessments of maturity as a proxy for overall cyber risk, while others use more sophisticated probabilistic models to estimate cyber risk in financial terms. Regardless of the approach, this as a key alignment and coordination mechanism between the board and executive leadership and this should be clearly defined and communicated.
- **Resilience Management**: given the increasing likelihood of adverse cyber incidents, it is imperative that all cybersecurity strategies include recovery and resilience plans. Contingency plans and capabilities need to be in-place and tested to allow operations to recovery quickly, minimizing disruption to operations.
- **Cybersecurity Strategy**: many have adopted industry standard frameworks in the formulation of the cybersecurity strategy (eg, NIST) and this will simplify communication of the strategy in the disclosures. Such a common lexicon will also enable precise communication across the organization, as well as with key vendors, regulators, and auditors.
- **Cyber Insurance**: a number of organizations have obtained cybersecurity insurance as a method of transferring some of the financial uncertainty to a third party. In addition, many find the pre-vetting of suppliers and the ability to gain support in a crisis to be extremely valuable.

Enterprise Risk Management

Existing ERM capabilities may need to be extended and expanded to more uniformly incorporate cyber risks as part of the overall portfolio. Cyber risks differ from others in that they are highly variable – and unpredictable - in both probabilities and impacts. This variability results from the reality of cyber risk – it is a manifestation of human-to-human conflict (bad actor offense against your defense). Though difficult to estimate, these risks need to be included in the enterprise risk register alongside other traditional risks.

Cyber Incident Disclosures

Security Monitoring & Detection

Though this area is clearly operational and the responsibility of management, it is important to recognize that this capability is material to the timely identification of incidents that may ultimately be deemed material. Though the board does not need to be informed of the operational minutiae, it will be vital that they understand what is "normal" in terms of security activities and high-level performance metrics. This will ensure transparency and alignment and provide directors with insights sufficient to support investments recommended by management.

Incident & Crisis Response

As cyber events are classified as incidents, it will be vital that the board and management have a clear, shared definition of the characteristics that define what constitutes a 'material' incident that should be disclosed. Note that the SEC did not prescribe a new definition of materiality for cyber incidents. They instead stated that determination should be based on federal securities law materiality, including consideration of quantitative and qualitative factors. Given the time criticality of required disclosures of material incidents, there are several key areas to consider.

- **Incident Classification**: It is imperative that the board and executive leadership have a well-understood, pre-defined methodology for classifying cyber incidents, especially those that are ultimately identified as 'material'. It is unlikely that a single pre-defined set of criteria will address every incident and determination of materiality, but the general parameters for evaluation should be defined and agreed in advance including such considerations as number of assets affected, duration of interruption, financial loss, etc. More important, the process should be well-defined, as well as the clear definition of roles and authorities/accountabilities in evaluating incidents.
- **Incident Response**: Once identified as material, an incident will need to be managed by a well-structured and efficient process for managing the remediation and recovery of the incident. One key change is the importance of engaging the board with management in declaration of material incidents on a timely basis to support 8-k disclosures.
- **Crisis Response**: Pre-defined roles and crisis response plans should be defined and tested, including templates for communications, updated contact information for company personnel, key third-parties, and law enforcement.
- **Drills, Testing**: Rapid determination and disclosure will require efficient execution and coordination. To ensure all members of the director and officer team are clear on processes and roles, drills should be conducted on a routine basis, along with after-action reviews to identify areas of improvement.

Finally, it is important to clearly define which leaders are leading each of these capabilities. In the heat of an incident, the CISO will be interrupting the attack and recovering operations with the technology team. A separate leader will need to handle crisis response and communications, and likely another leader will need to handle the creation and approval of the 8-k disclosure. The importance of this specialization will become obvious with practice drills and iterations.

Common Capabilities

In addition to requirement-specific capabilities, it is important to note that there are common capabilities that will be required to enable all the new SEC rules.

Disclosure Management

The new rules for cybersecurity disclosure consist of two general types – (1) routine annual disclosure of cyber risk strategies and capabilities, and (2) incident-specific disclosures. Both will have significant implications for registrants.

- **Initial Release – FY23:** At the outset, registrants will have an initial challenge in drafting disclosure-ready documents that describe the risk management and governance practices that are in-place. While most will have gained confidence in their practices in the last several years, the reality of public disclosure of these in an SEC filing will likely necessitate a thorough re-examination and potentially a revision prior to release.
- **Ad hoc Incident Disclosures**: Incidents are, by definition, unexpected and are impossible to predict. The new SEC rules have two requirements for disclosing such incidents: (1) upon determination that such an incident was 'material' and (2) amendments to the original disclosures as incremental new information is discovered. This is a significant impact, and such capability needs to be established now and will need to be included in routine incident drills to ensure capabilities are sufficient for meeting these new short time requirements.

Education & Training

A recurring theme throughout the SEC rulemaking process in 2022-2023 was that of expertise. Though the rules ultimately did not include the disclosure of director biographies, that could arise in the future – and current requirements do seek to understand the expertise of key management members. It is vital that education and training be a continuous activity to ensure that the team has sufficient baseline expertise as well as awareness of shifting trends and issues. Specifically focusing on the SEC rules, some initial training considerations might include:

- **Board Level**: Recent analyses have shown that many boards lack deep cyber expertise[1]. While each board may not need a dedicated cyber expert, it is likely reasonable to expect that each director should have sufficient cyber training to support the oversight of cyber risk. Many boards are providing ongoing training and real-world briefings on trends and issues as part of the regular board cadence. In addition, many are providing formalized training and certification for Committee Members – specifically tailored to cyber risk oversight. As an example, the NACD cyber risk oversight certification is increasingly popular and provides a solid grounding in terminology and concepts.
- **CISO**: Similarly, CISOs are often highly talented technical leaders but with limited board-level experience[2]. Many CISO roles are newly created in the last 5-10 years and the individuals in those roles are still adapting to expanded responsibilities. A number of companies are investing in formal education and certification for CISOs – similar to that provided to board directors. In the case of the CISO, there are key concepts and frameworks that will help accelerate their preparation for effective and efficient interaction with the board. The NACD Accelerate program receives solid reviews for its effectiveness in providing such opportunities for CISOs, including both formal education and certification for aspiring CISOs.

References:

1 – 90% of Boards Are Not Ready For SEC Cyber Regulations – Forbes (Brian Walker - *Feb 6, 2023*)
2 – The SEC Wants Board Cyber Expertise: How Many CISOs Are Board-Ready? – Forbes (Brian Walker - *June 7, 2023*)

CAP Group

The CAP Group is a specialized advisory firm that supports directors and officers in public and private companies who seek pragmatic, strategic cybersecurity advice.

Our advisors are experienced operators from premier organizations, well versed in the complexities of evaluating and mitigating cybersecurity risk.

www.TheCAP.Group

info@thecap.group

214.380.5970