A CISOs Guide to the SEC's Cybersecurity Regulation:

Everything you need to know

Balbix®

On July 26, 2023, 29,980 senior business leaders of the 5,996 public companies in the US got a new headache. CEOs, CFOs, CISOs, CIOs, and the senior leadership teams at US public companies must now make room for the SEC's final rule S7-09-22, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.

The goal of SEC cybersecurity law is to ensure that all public companies disclose information in a manner that is as mature and effective as the most cyber-mature company.

And since stakeholders—investors and customers—are increasingly concerned about how organizations manage their cybersecurity risks, a clear mandate on disclosure can boost trust and transparency. Therefore, these disclosures aren't just a form of mere compliance requirement but a business-critical function.

Timeline for the SEC Cybersecurity Rule

Overview of requirements

	SEC Disclosure Requirements for Public Companies
Cyber Incident Reporting • Form 8-K Item 1.05 • Form 6-K	Companies must report material cybersecurity incidents in Form 8-K within four business days of materiality determination, including the nature, scope, and timing of the incident and the material impact or reasonability likely material impact on the Company. Exceptions for public safety and national security situations. Materiality determination should be based on federal securities law materiality, including quantitative and qualitative factors. If 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.
Cyber Risk Management and Strategy • Regulation S-K Item 106(b)	Company must describe process for assessing, identifying and managing material risks from cyber threats. And describe where there any risks from Sherry security threats may have materially affected (or are likely to materially affect) Business strategy, results of operations, or financial condition.
Cyber Governance • Regulation S-K Item 106(c) • Form 20-F	Company must describe governance of cyber security risks as it relates to: • The board' oversight of cyber security risk, Including identification of any board committee is responsible for oversight and the process by which they are informed about cyber risks. • Management's role and expertise in assessing the managing material cyber security risk and implementing cyber security policies, procedures and strategies.

The SEC's new regulations mandate that organizations disclose material cybersecurity incidents within four business days. Annual disclosures must include cybersecurity risk management, strategy, and governance details. The rules apply universally, covering both domestic and foreign private issuers.

CHALLENGES POSED FOR BUSINESS LEADERS

The introduction of these new regulations presents a multi-faceted challenge for business leaders. First, there's the issue of understanding what a 'material' cybersecurity incident means, a term surrounded by subjectivity. Next, the four-day window for disclosure puts significant pressure on organizations to quickly gather facts & disclose the scope of impact, which is particularly difficult in an enterprise environment with thousands of assets, applications, systems, and tools.

NEED FOR CHANGES TO ADAPT TO THE NEW REQUIREMENTS

Adapting to the new SEC requirements requires a twofold approach that may not come naturally nor can be turned on like a switch. First, organizations must have the flexibility to tweak existing data collection processes. Perhaps more importantly, a cultural shift is required. What does that look like? It may involve setting up specialized disclosure teams, conducting regular cybersecurity audits, and even changing organizations reporting structure.

A GAP ANALYSIS

A gap analysis, based on extensive discussions with senior cybersecurity and business leaders, reveals a disparity between current organizational capabilities and the requirements of the new SEC regulations. Many organizations struggle with foundational aspects like asset inventory and inconsistent cyber risk management processes. Even cybersecurity-savvy Fortune 100 companies haven't fully mastered the landscape. A comprehensive, real-time overview of cyber risk that bridges IT-level risks with business implications remains a challenge for many. The intricate nature of materiality determination further complicates this landscape.

The Concept of Materiality in Cybersecurity

COMPLEXITIES OF DETERMINING MATERIALITY

Materiality is subjective: determining what constitutes a 'material' cybersecurity incident is the most challenging aspect of the new SEC regulations. Materiality is more than the number of records compromised or the immediate financial impact. The concept also encompasses long-term repercussions like reputational damage, loss of competitive advantage, and potential legal liabilities. For almost all organizations, determining materiality requires a multi-disciplinary approach.

HOW SHOULD COMPANIES DEFINE MATERIALITY?

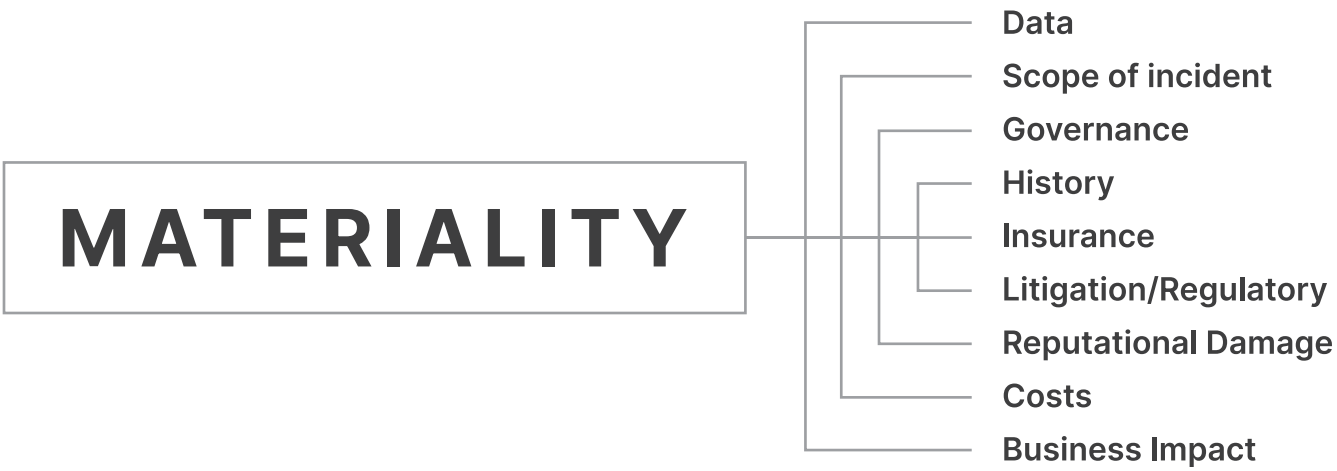
Materiality is a key concept in the new rules set by the SEC regarding when publicly traded companies must report serious cyberattacks. The SEC has given companies the discretion to determine whether a cyber incident is material, as long as the definition aligns with established case law and legislation from the 1930s. The rationale is that information is considered material if a reasonable person deems it important when making an investment decision or if it would significantly alter publicly available company information. Any doubts about materiality should favor the investor. This approach ensures that companies remain transparent with their stakeholders about significant cyber incidents that could impact their financial health.

WHO SHOULD BE INVOLVED IN DETERMINING MATERIALITY?

Determining materiality requires the involvement of multiple stakeholders. Executives accountable for cybersecurity must document their process and thinking when assessing materiality. The SEC emphasizes that a materiality determination should be made "as soon as reasonably practicable after discovering an incident. Companies must also disclose their criteria to determine materiality in their annual reports. For CISOs, the new rules highlight the importance of their role in the decision-making process, suggesting that they should have a seat at the table with business managers and directors, especially given the need for these directors to be aware of details that might influence materiality determinations.

IMPORTANCE OF CONSIDERING BOTH QUANTITATIVE AND QUALITATIVE FACTORS

When determining materiality, focusing solely on quantitative metrics like the number of records compromised or the financial losses incurred might be tempting. This approach, however, is far too narrow. Qualitative factors like reputational damage, loss of customer trust, and potential legal liabilities can often be far more damaging in the long run. Therefore, a balanced approach that considers quantitative and qualitative factors is essential.



Reporting Cybersecurity Incidents

8-K AND 10-K REPORTING

The SEC has introduced two reporting categories to keep us informed. The "current" category covers material incidents in 8-K filings, while the "periodic" category provides mandatory cybersecurity risk management, strategy, and governance disclosures in 10-K filings. The SEC's four-day window for reporting material cybersecurity incidents starts from the day the incident is deemed material—not from the day it is detected.

IMPORTANCE OF UNDERSTANDING INTERNAL ESCALATION AND EXTERNAL REPORTING PROCESSES

Effective incident reporting is a multi-step process that begins with internal escalation. A cybersecurity incident must be escalated through predefined organizational channels as soon as it is detected. This process is crucial for quick decision-making and response. Then, once internal escalation is complete, teams can begin external reporting to comply with SEC regulations.

DOCUMENTATION AND DISCLOSURE

While maintaining comprehensive documentation is a regulatory requirement, it has always been considered a best practice. Documentation should include records for how the incident was detected, steps taken to contain it, and how the materiality assessment was conducted. This documentation will be crucial for any potential legal proceedings and for preparing the mandatory SEC disclosures.

REPORTING RELATED INCIDENTS

The new SEC regulations require organizations to report related cybersecurity incidents collectively. What does this mean? Here's an example: if an organization is targeted in a phishing campaign and suffers a data breach, both incidents must be reported together, providing a comprehensive view of the cybersecurity incident.

STRATEGIC DISCLOSURE WITHOUT ALERTING ATTACKERS

When reporting cybersecurity incidents, a balance must be maintained between transparency and security. Disclosing too much technical detail can inadvertently provide attackers with insights into your organization's vulnerabilities and boost the effectiveness of their tactics. To avoid tipping off attackers, companies should focus on reporting on the nature and potential impact of the breach without specific technicalities or intrusion methods. Collaborating closely with cybersecurity experts during the disclosure process can help craft statements that inform stakeholders without giving away sensitive information. Avoid providing details about specific exploited vulnerabilities and systems compromised.

Cyber Risk Management Plans

COMMUNICATING CYBER RISK TO INVESTORS

The SEC's proposed regulations underscore the need for public companies to standardize their approach to disclosing their cybersecurity risk management strategies. Companies should incorporate cyber risk communication in annual Form 10K submissions for this initiative.

BEFORE

- Business risk
- Legal risk
- Ownership risk

AFTER

- Business risk
- Legal risk
- Ownership risk
- Cyber risk

A well-structured 10K submission should highlight:

Cybersecurity Risk and Governance: This section should provide insights into the company's understanding of its cyber risk landscape. It should detail the measures to mitigate these risks and the governance structures overseeing these processes.

Dynamic Cyber Risk Assessment: Companies should emphasize the tools and methodologies they employ for continuous and dynamic cyber risk assessment. This demonstrates a proactive approach and assures investors of the company's commitment to avoiding potential threats.

Board Involvement: Highlighting the board's active involvement in cybersecurity oversight can instill confidence in investors—proving that cybersecurity is not just an IT issue but a top-tier business concern that commands attention from the highest levels of the company.

Integration with Business Strategy: It's crucial to demonstrate how cybersecurity risks are integrated into the broader business strategy, risk management processes, and financial oversight. This sets the bar for how a company views cybersecurity not as an isolated challenge but as an integral part of its overall business operations.

ENHANCED DISCLOSURES

The new regulations also mandate enhanced disclosures about cybersecurity risks in annual reports. Enhanced disclosures include a description of the risks and the measures taken to mitigate them.

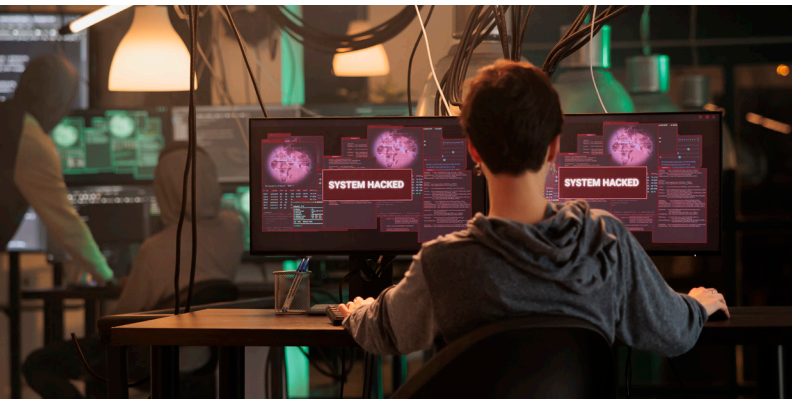
RECORD-KEEPING REQUIREMENTS

Advisers and funds must maintain detailed records of all cybersecurity incidents and the steps taken to address them. In the event of legal proceedings or regulatory audits, these records could be crucial.

The Role of CISOs, CIOs, and CFOs in SEC Disclosures

As the CEO or CFO is ready to sign and certify the company's 10-K, one more question they must ponder is the confidence level about the completeness and accuracy of the company's cyber risk management program disclosure. From a legal perspective, they must stand behind the criteria used to determine whether or not an incident or risk item qualifies as material.

CISOs or CIOs are probably worrying about striking the right balance in the details of their disclosure so they can meet the SEC's requirements without giving away confidential information about the company's cyber program. Plus, they're likely debating with senior leaders and the legal department about determining the materiality of incidents and risk items.



SHARED RESPONSIBILITY FOR REPORTING

Cybersecurity is a shared responsibility that must extend beyond the IT department. While the CISOs may take the lead in managing the organization's cybersecurity posture, the responsibility for reporting cybersecurity incidents should be a collective effort involving legal, compliance, and even the finance department.

CISOs PRIMARY ROLE DURING A BREACH

During a cybersecurity incident, the primary role of the CISO is to lead the incident response efforts. This includes identifying the scope of the breach, containing the incident, and initiating recovery measures. The CISO is also responsible for communicating with other departments to ensure a coordinated response.

It's also important to note that having a CISO on the board can provide valuable insights into cybersecurity risks and challenges. CISOs can ask pertinent questions and ensure that cybersecurity is given the attention it deserves. However, there's a shortage of security professionals who can operate at the executive board level.

WHAT CISOs SHOULD AND SHOULDN'T DO

In the context of the new SEC regulations, CISOs need to distinguish the boundaries of their responsibilities. Here's what they should and should not do.

SHOULD

- Support Materiality Assessment Processes: While CISOs should not directly assess the materiality of incidents, they should provide all necessary support to the officers responsible for SEC reporting. This includes offering relevant data and insights to aid the materiality assessment.
- Update Security Incident Response Processes: CISOs should ensure that their incident response processes are up-to-date in light of the new regulations. This might involve collecting additional data to support materiality assessments, discovering and aggregating related incidents, and ensuring effective communication with the relevant parties.
- Documentation and Process Management: CISOs should ensure that processes for assessing, identifying, and managing cybersecurity threats are well-documented and updated regularly.

SHOULDN'T

- Assess Materiality Alone: CISOs should not directly assess the materiality of any incident or collection of incidents. This responsibility lies with the corporation's officers responsible for SEC reporting.
- Share Sensitive Data About Systems and Software: Regarding SEC disclosures, CISOs should be cautious about oversharing. They should limit incident details and mitigating actions to the minimum defined by corporate officers as required for SEC disclosure.

Practical Steps for Compliance with New SEC Regulations

Merely understanding the new SEC regulations is only half the battle. The real challenge lies in translating this understanding into actionable steps that ensure compliance while safeguarding an organization's assets and reputation.

REVISIT YOUR INCIDENT RESPONSE PLAN

An incident response plan is more than a compliance requirement, it's table stakes for business. Without a well-structured plan, your organization won't be equipped to handle a cybersecurity incident effectively. A robust incident response plan enables quick identification and containment of threats, protects sensitive data, minimizes operational downtime, and mitigates the financial repercussions of a security incident.

UPDATE NOTIFICATION PROCEDURES

In line with the SEC's new regulations, it's crucial to have a clearly defined notification procedure. You must delegate roles and responsibilities for creating, approving, and disseminating notifications to the relevant stakeholders. One good idea is to develop communication templates containing pre-approved language, leaving placeholders for incident-specific details that can be quickly filled in during a crisis.

BALANCE DATA PROTECTION AND DISCLOSURE

Public disclosures, while necessary, may compromise sensitive information. Develop protocols that strike a balance between transparency and data protection. Collaborate closely with your legal team to ensure that disclosures are informative and compliant with legal requirements.

REGULAR REVIEWS AND THIRD-PARTY ASSESSMENTS

Cyber threats continually evolve, and your incident response plan should keep pace. Regularly updating your plan to reflect changes in the threat landscape and compliance requirements should be a priority. Also, consider engaging third-party cybersecurity experts to conduct in-depth assessments of your cybersecurity posture, identifying any vulnerabilities that need immediate attention.

CONDUCT TABLETOP EXERCISES

Tabletop exercises are simulated scenarios that test your organization's incident response capabilities. These exercises should be comprehensive, involving the technical aspects and the business decision-making, communications, and impact assessment processes. These drills are invaluable for preparing your team to meet SEC's new four-day reporting deadline.

Recap/A Look Ahead

The new SEC regulations on cybersecurity disclosures represent a paradigm shift in how organizations approach cybersecurity governance. These regulations have broad implications, affecting how cybersecurity incidents are reported and also how they are managed and governed.

The regulatory landscape is bound to undergo continual transformation. The days of static compliance checklists are numbered; the future calls for a dynamic, adaptive approach to cybersecurity governance.

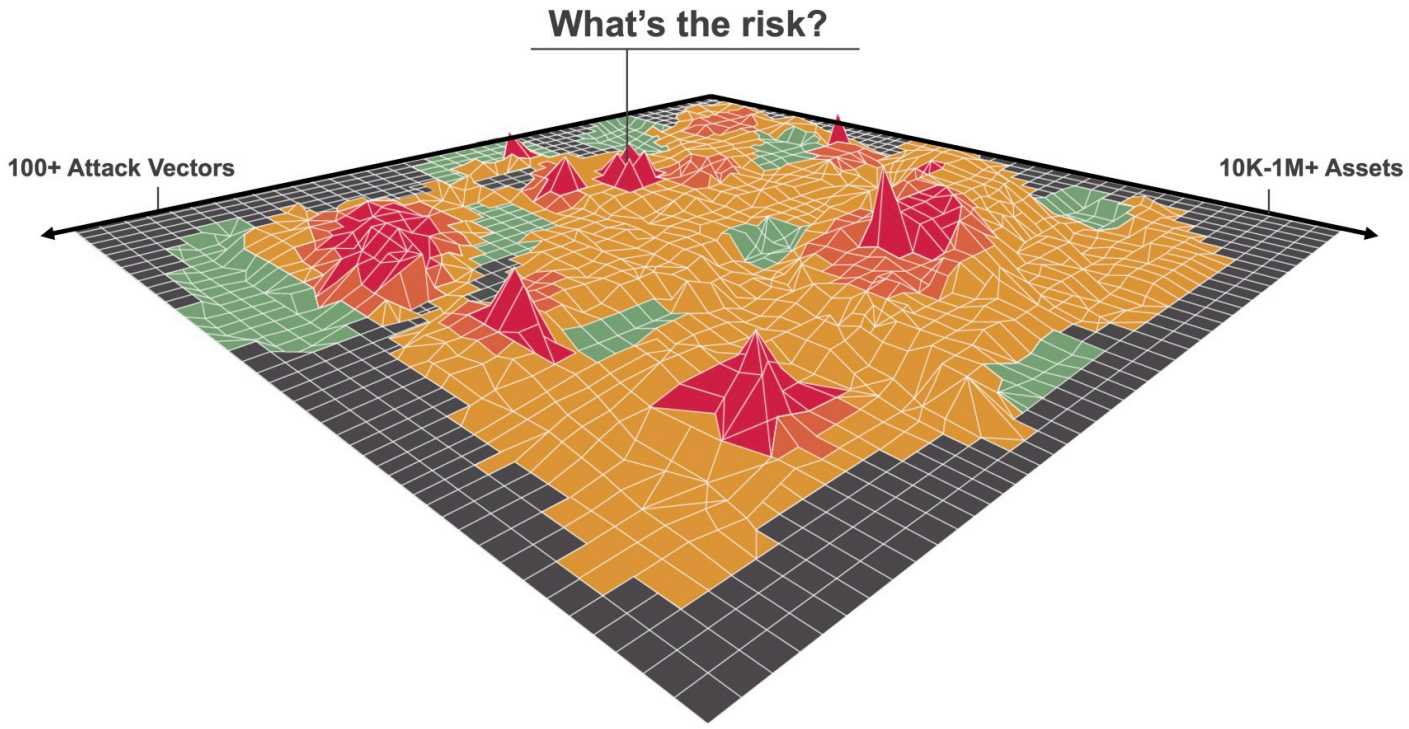
Here's what we can anticipate.

Facing increasingly sophisticated cyber threats, more companies will rely on real-time monitoring and AI-driven analytics in a big way. AI and ML technologies will be at the forefront that can analyze vast data streams to detect potential cybersecurity incidents.

This technological shift may move disclosure practices even further than what we're seeing with the SEC regulations. Instead of reactive announcements after an incident, organizations will lean into proactive disclosures, updating stakeholders on their cybersecurity stance and efforts to address vulnerabilities.

As cyber threats know no borders, the need for a unified global standard for cybersecurity disclosures is growing. We expect to see a push towards creating universally accepted guidelines.

Third-party audits will become more prominent to ensure regulatory adherence. Despite these advancements, the human element will always be crucial. Comprehensive employee training will evolve to emphasize a holistic understanding of the cybersecurity domain and the importance of prompt disclosures.



Balbix®

Want to see how Balbix can help your organization with the new SEC regulations?

Please reach out to us and schedule a meeting.