panaseer

SEC Cybersecurity Disclosure Proposals: Get ready for public inspection of your cyber strategy

Contents

ABOUT THE AUTHOR

Nick Lines
Product Evangelist

Nick champions Panaseer's unique value and ensures we're helping solve the biggest challenges in cybersecurity. He's worked for multinational systems integrators and consultancies in roles including developer, technical sales, and offering management, and previously spent a decade at Microsoft.

Introduction

The US Securities and Exchange Commission (SEC) has signalled a major shift in its thinking on cybersecurity risk. To better protect investors, it has proposed new regulations that will bring more consistency to the way organizations disclose security policies, procedures and expertise.

In this whitepaper we look at the impact of new regulation proposals and how organizations need to respond.

A hardening approach to cybersecurity disclosure

The SEC says its mission "is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The SEC strives to promote a market environment that is worthy of the public's trust."

Trust can only be built on a foundation of security, using the traditional, non-financial instrument definition of the word, summed up as "protection against threats." Fundamentally, then, the SEC sees its mission to drive security as well as securities.

The threat landscape against which organizations must secure themselves has changed rapidly in the past decade, and the SEC has evolved guidance governing all publicly-traded organizations to recognize this. That guidance, however, is not being followed consistently, hence the need to propose enforcement through regulation.

In October 2011, the SEC Division of Corporation Finance **published disclosure guidance specifically for cybersecurity**[1]. This guidance is relatively short and provides "views regarding disclosure obligations relating to cybersecurity risks and cyber incidents." It also notes it is guidance, not a "rule, regulation or statement of the commission."

In 2018, the **Commission itself issued guidance**[2] clarifying expectations on disclosure, noting that cyber risks should be disclosed as with other material risks to an organization, and reminding organizations of their existing obligations around disclosures. It's striking that the introductory sentence is, "Cybersecurity risks pose grave threats to investors, our capital markets, and our country." Threats such as ransomware are explicitly mentioned.

Skipping forward, in March 2022 the SEC proposed **Rules on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure by Public Companies**[3].

1 Security and Exchange Commission Division of Corporation Finance (2011), *CF Disclosure Guidance: Topic No. 2*

2 US Securities and Exchange Commission (2018), *SEC Adopts Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures*

3 US Securities and Exchange Commission (2022), *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*

> ***"Over the years, our disclosure regime has evolved to reflect evolving risks and investor needs. Today, cybersecurity is an emerging risk with which public issuers increasingly must contend. Investors want to know more about how issuers are managing those growing risks. A lot of issuers already provide cybersecurity disclosure to investors. I think companies and investors alike would benefit if this information were required in a consistent, comparable, and decision-useful manner. I am pleased to support this proposal because, if adopted, it would strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting."***
> **SEC Chair Gary Gensler**

The SEC clearly feels that the interpretive Committee guidance from 2018, building on the 2011 advice, is not being consistently followed. It's now seeking to regulate as the guidance hasn't given the protection they feel investors deserve. And with so many incidents since 2011 with such variable disclosure, it's hard to argue with that.

Whereas previous guidance focused on disclosure of risks and incidents, these proposed amendments to rules will put the spotlight firmly on an organization's overall approach to cybersecurity, mandating:

- Timely (exceptional) and periodic reporting about material incidents.
- Periodic disclosure of its policies and procedures to identify and manage cyber risk.
- Disclosure of management's role in implementing cybersecurity policy and procedures (or governance).
- Disclosure of the board of directors' cybersecurity expertise (if any, it notes slightly wryly).

Each of these topics deserves a more thorough examination of the proposals and discussion of their impact. The **proposed rule document**[4] is well structured and easy to read, and weighs in at just over 100 pages, however the details of regulatory changes cover just under 30 pages. It's important to note that the regulations are principle based, much like other recent regulation from around the world, notably the EU's GDPR and **Digital Operational Resilience Act (DORA)**[5].

These proposed amendments to rules will put the spotlight firmly on an organization's overall approach to cybersecurity.

4 US Securities and Exchange Commission (2022), *Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*
5 Panaseer (2023), *DORA: What security leaders need to know about the Digital Operational Resilience Act*

SEC Cybersecurity Disclosure Proposals

01

Timely reporting of cybersecurity incidents - Form 8-K

An 8-K is a report of *unscheduled* material events or changes at an organization that could be of importance to shareholders or the SEC. Previous guidance suggested companies should use these following a cyber incident.

The proposed amendment would require disclosure within four days after an organization has determined that it has experienced a material cybersecurity incident.

The word material is important here. It brings in a subjectivity to the regulation, with information being material if "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would have significantly altered the 'total mix' of information made available."

The Supreme Court noted that there would be "doubts as to the critical nature" of information, but that "it is appropriate that these doubts be resolved in the favor of those the statute is designed to protect", namely investors. The proposal gives examples of what would need to be disclosed.

It includes:

- If someone's compromised an asset.
- A violation of policies and procedures.
- An interruption of normal service on operational technology.
- Unauthorized access to information.
- Lost (or stolen) personal or sensitive business information, trade secrets, or intellectual property.
- Extortion or ransomware demands.

That's pretty exhaustive and it's difficult to find what doesn't require disclosing!

All in all, you will not find yourself breaking rules by over-disclosing. And you may find that the transparency earns you plaudits from your investors, too, as **analysis by the HBR in 2020**[6] noted that stock prices can actually rise following disclosures. Of course, that should be treated with a note of caution as disclosing serious data breaches can have lasting impacts on stock price. Attempting to cover up, though, has worse effects, as we saw with the recent **prosecution of Uber's**[7] former **CISO**[8].

6 Harvard Business Review (2020), *A Cyberattack Doesn't Have to Sink Your Stock Price*
7 The Wall Street Journal (2018), *Uber to Pay $148 Million Penalty to Settle 2016 Data Breach*
8 Dark Reading (2023), *Judge Spares Former Uber CISO Jail Time Over 2016 Data Breach Charges*

What should be disclosed?

Best practice is coalescing around the factual: state what happened, state what protections were in place, state what you will learn and change going forward. There's no need to give detail on the precise tooling you use, however you are trying to educate your investors about the risk and impact of any incident and give them confidence.

The next point worthy of consideration is the duty for an organization to disclose within four days of "determining it has experienced a material cybersecurity incident."

As a principle this is easy to say. But it raises important questions:

- If a security operations center (SOC) discovers an indicator of compromise (IOC), does that start the clock ticking?
- Who makes the call on materiality? Is it operations (1LOD), monitoring and reporting (2LOD) or audit (3LOD)?
- How does the SOC determine context to support the decision on materiality?
- At what point does an immaterial incident become material? And who makes such a decision?
- For a ransomware incident, even if recovery is possible without paying any ransom or disruption to business, does it need to be disclosed?

That is by no means an exhaustive list, but it does illustrate some process considerations that need to be taken, and that multiple teams will need to be involved. And that does not include investor relations, press relations or legal review either. During an incident the pressure will be on everywhere, so preparation is paramount.

Especially given the timeframes demanded by the SEC. Four days may seem a short window, however when the average dwell time (time between assumed initial intrusion and detection of an intrusion) for a ransomware attack is nine days, according to the **Mandiant M-Trends 2023 report**[9], defenders need to move fast.

The SEC does recognize that a delay in reporting may seem to be justified to support ongoing investigations, or law enforcement, but concludes that: "On balance, it is our current view that the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay." In other words, if there's a material incident that's still ongoing, you disclose it: no excuses.

To support rapid response, defenders will need to understand the context of any suspected attack, which means they need to understand the role and importance that the potentially compromised asset plays in the organization's business. A SOC may not have this information to hand, however it's critical when responding and when determining materiality.

There's no need to detail the precise tooling you use, however you're trying to educate investors about the risk and impact of any incident.

9 Madiant (2023), *M-Trends 2023*

02

Periodic reporting of cybersecurity incidents - Forms 10-Q and 10-K

This requirement can be summarized by stating organizations need to revisit and wrap up the incident that caused the filing of the 8-K form. If an incident that was considered immaterial, and therefore not reported, has evolved to become material, this too needs disclosure on the appropriate periodic report, and arguably should have triggered an 8-K filing too.

The periodic filing should include what impact the incident had on operations and finances, any future impacts, whether the incident is fully remediated or is still ongoing, and what changes have been made to policies and procedures as a result of the incident.

Again, visibility of assets and context, along with derived insights, are critical. Being able to evidence historical status and remediation progress using trusted data and metrics will also provide assurance to investors and the SEC, and the insights that come from business context and history should be used to inform the evolution of policy and the focus of operational priorities.

Disclosure of cyber risk management and strategy

In the proposals for disclosing risk management and strategy, the SEC observes that most registrants that disclosed a cyber incident in 2021 did not describe their cyber risk oversight policies and procedures. It proposes that better disclosure would allow investors to make better decisions. Given the observation, it's hard to argue with the proposal.

It also notes that third-party risks, or supply chain risks, were responsible for a third of security disclosures, and therefore deserve special handling.

In the introduction, the SEC posits that organizations "may" have cybersecurity policies, procedures, approaches, and tactics but does not mandate them. The new regulations do however mandate that their existence, and some details, are disclosed. The preamble also appears to strongly encourage sharing of how the risk of impact from cybersecurity incidents are identified and managed, with a focus on financial impacts.

Third-party risks, or supply chain risks, were responsible for a third of security disclosures, and therefore deserve special handling.

The proposals themselves are straightforward, and for clarity they are included below. The registrant would be required to provide, if applicable, details of whether:

1. ***The registrant has a cybersecurity risk assessment program and if so, provide a description of such program.***

What approach does the organization take to assessing risk? The description is an opportunity to explain why the organization should be seen as a safe investment and to differentiate itself. Given the number of high-profile cyber incidents, investors will want to feel reassured. An absence of this would do the opposite.

2. ***The registrant engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program.***

Dependent on the organization size, this may be table stakes. Referring to third-party frameworks (NIST, CIS, Mitre ATT&CK, …) would help prove the efficacy of the risk assessment and mitigation as well as a full understanding of their security posture using trusted data and metrics. Note this is risk assessment, not penetration testing.

3. ***The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider (including, but not limited to, those providers that have access to the registrant's customer and employee data), including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers.***

As noted, third-party service provider incidents are seen as a root cause of a third of recent disclosures. Understanding the size and management of that risk is critical for investment decisions in the SEC's view. Being able to inspect or have the third party attest to their own security posture management and security KPIs using trusted data and metrics may come to be seen as best practice.

4. The registrant undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents.

This requirement only mandates that the registrant undertake the activities: a further description here by the registrant would pay dividends.

Starting from a description of how a single view of a trusted asset inventory is achieved, the registrant could then describe its approach to basic cyber hygiene, which according to Microsoft **protects against 98% of attacks**[10]. This would certainly help reassure investors. However, ensuring the accuracy of the inventory, and proving control status across all asset types, is a non-trivial challenge.

Further describing how the NIST CSF is implemented across the five pillars (Identify, Protect, Detect, Respond and Recover) at a high level would be a good way of demonstrating how cyber risk is actively monitored, or through use of other frameworks. Best practice would include continuous, automated monitoring of security controls with detailed and accurate asset information to ensure evaluation of risk and appropriate prioritization occurs.

Details of tooling should not be exposed, however the process and approach may be a good reassurance additionally supported with a high-level understanding of security posture management utilizing trusted data and metrics.

5. The registrant has business continuity, contingency, and recovery plans in the event of a cybersecurity incident.

Demonstrating how tabletop cyber exercises are conducted, and simulating recovery from common threats – especially ransomware – may again win investor confidence.

6. Previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies.

An interesting question to ask is whether this is just incidents that have happened to the organization or wider incidents? Showing an evolution of risk appetite, threat understanding and commensurate updates across policies, procedures, technology and governance is again an important way to win confidence.

It would be concerning to not have an answer here. Demonstration that security posture has improved since incidents, ideally using trusted data and metrics, shows cyber maturity and is likely to further reassure investors.

7. Cybersecurity related risk and incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition and if so, how; and Cybersecurity risks are considered as part of the registrant's business strategy, financial planning, and capital allocation and if so, how.

We see this as the SEC providing the opportunity for organizations to demonstrate their understanding of the impact of cyber risk on their financial operations. Being able to quantify cyber risk through understanding context, likelihood and impact using data and metrics would greatly help reassure investors here too.

10 Microsoft (2022), *Microsoft Digital Defense Report 2022*

03

Disclosure of cyber governance

The propositions split into two areas here: the board's oversight of, and management's involvement in, managing cyber risk.

Board requirements

Board-level disclosures are straightforward and give an opportunity for organizations to demonstrate the maturity of their cyber governance. The regulation requires disclosure on:

> ***1. Is the board, a board member or a sub-committee responsible for oversight of cyber risk?***

Interestingly, the SEC's regulations are focused on responsibility for security rather than accountability. Indeed the proposal does not discuss accountability, which is at odds with other regulations and guidance from US and EU organizations.

> ***2. The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic.***

A more detailed question around processes. Best practice may be regular discussions of agreed cybersecurity metrics and KPIs, and evolution of those KPIs over time as maturity increases. Adherence to policy and SLAs, as disclosed in the previous section, backed by trusted data and metrics would be an effective way to demonstrate board competence and oversight.

> ***3. Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.***

The 'and how' clause means this becomes a more insightful answer and is closely related to point 2 above.

Management's requirements

For management levels, the questions are slightly more detailed. The proposals require disclosure of:

> ***1. Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members.***

That this aligns to many frameworks, notably NIST CSF, is not accidental: who is responsible for the security lifecycle, and do they understand it? This complements the disclosure of policy and procedure previously mentioned and shows that responsibility is clearly being managed.

And, as with board members, disclosure of the competence of those responsible is mandated.

> ***2. Whether the registrant has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart, and the relevant expertise of any such persons.***

No comment is necessary here: this is a straight up disclosure that maps to maturity.

> ***3. The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents.***

This neatly ties up another section, notably around incident disclosure, as the inference is that these persons or committees will be accountable for the classification and disclosure of such incidents.

> ***4. Whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk.***

This seems closely related to the previous disclosures covering the board, and the inference is that the board expects to be briefed by those responsible for incident prevention, detection, mitigation and recovery.

As with other disclosure sections, this does seem an opportunity for organizations to differentiate and show maturity by using trusted data and metrics to show security posture.

04 Disclosure of board cybersecurity expertise

When disclosing whether a board member should be considered to have cybersecurity expertise, the following list is suggested as a basis of evaluation:

- Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner.
- Whether the director has obtained a certification or degree in cybersecurity.
- Whether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.

This seems to strongly suggest that having a board member with hands-on experience in the frontlines of cybersecurity is advantageous. Such experiences are hard-won and give a grounding in the realities of cybersecurity. You certainly wouldn't get a former practitioner demanding assurances that an organization is 100% protected, which anecdotally seems to be the demand from some boards to CISOs.

05

What this all means

The SEC has proposed comprehensive disclosure rules around cybersecurity. Its aim is to improve transparency and trust, so investors are better protected and can make informed decisions. As such, the SEC hasn't mandated what organizations should do to secure themselves against cyber threats, but has mandated that organizations tell the public how they manage cyber risk.

These disclosures will place a burden on security leaders to show not only their policies across the totality of security lifecycle, but also how they enforce, measure and improve such policies as the threat landscape evolves.

We would propose that a minimum response should include multiple control technologies, such as vulnerability scanning, multi-factor authentication, endpoint detection and remediation, cloud security posture management and more, alongside an approach to ensure the controls provided by such technologies are in place across all assets and meeting the requirements laid out in your security policies.

Providing such information using trusted data that uses metrics to measure performance will provide more assurance to investors that you're taking cybersecurity seriously and meeting SEC regulations; potentially a differentiator in the market.

Our Security Posture Management platform makes this possible through **Continuous Controls Monitoring (CCM)**. It gives a true measure of your security posture, including the ability to codify your security policies into KPIs and metrics. With this automated, near real-time view of how you're performing against security policies and service level agreements (SLAs), you save time and resources when reporting to the board or disclosing information to the SEC.

Whilst this isn't mandated by the SEC's disclosure rules, we believe by implementing CCM you will both meet the disclosure requirements and gain competitive advantage by demonstrating cyber resilience in your disclosure filings, making you more attractive to potential investors.

Trusted data

As the SEC takes steps to improve trust and transparency, there will inevitably be greater focus on the quality and availability of security data. Security teams that are already overwhelmed with data will need to increase their use of automation, both to reduce the reliance on costly manual processes and to improve confidence in their reporting.

The Panaseer platform solves this problem by creating a single source of truth. We combine data from across your security and business tools, creating a trusted view of your assets and related controls. The platform is transparent and can show exactly how every entry in the inventory got there, what source systems were combined to make it, and why they were combined. Relying on manual processes or a black box to perform this critical task means you can't build trust or drive accountability.

Your asset data is also enriched with business context, such as location, business process, ownership and more. This shows the potential business impact and risk associated with that asset, which helps solve the challenge of whether an issue should be defined as 'material' under the SEC's proposed regulations.

Security is a team sport

The SEC's proposals are part of a broader trend we're seeing from global regulators to create shared accountability around cybersecurity, so it's not just the CISO that's on the hook.

Devolved accountability requires trusted data at its foundation. When data is accurate, the appropriate teams can and will accept their roles. It improves transparency and collaboration from the boardroom to the frontline, ensuring you're in a stronger position to meet the SEC's requirements around management and disclosure of cyber risk.

As the SEC takes steps to improve trust and transparency, there will inevitably be greater focus on the quality and availability of security data.

Automated security posture management

Continuous Controls Monitoring for enterprise security