panaseer

SEC cyber rules: 3 reasons why cyber governance is king

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.

01

New SEC regulations: what, when, who, and why?

The Securities and Exchange Commission (SEC) in the USA has hardened its stance on the risk that cyber threats pose to investors in companies. It has enacted new regulations that mean publicly listed companies need to disclose three things:

- Material cyber security incidents, to be reported in a timely fashion.
- How the company approaches cyber risk management and strategy, detailing processes, and also whether threats are likely to impact strategy, operational results or finances.
- Board oversight and management's role in cyber governance.

There are just 3 impactful rule changes – Item 1.05 on 8-K, and items 106(b) and 106(c) in Regulation S-K, respectively.

Any annual report from 15 December 2023 will need to include the new disclosures on form 10-K (or 20-F for foreign private issuers). Incident disclosure rules came into force on December 18, 2023, with **smaller reporting companies** having until 15 June 2024 as the deadline for the new rules.

None of this should come as a shock. In fact, the SEC could legitimately argue that it has requested that organizations do this forever, as cyber risk is just one aspect of risk reporting that the SEC has been concerned with since its inception. The 1933 Securities Act, enacted during the Great Depression in response to the stock market crash of 1929, was firmly based upon the principle of disclosure, which is the eighth word in the act itself!

> ***AN ACT To provide full and fair disclosure of the character of securities sold in interstate and foreign commerce and through the mails, and to prevent frauds in the sale thereof, and for other purposes.***

The commission itself was established in 1934 via the Securities Exchange Act, and ensured publicly traded companies had to disclose material facts, including risks, annually.

As a reminder, the US Securities and Exchange Commission (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 definition of the word, summed up as "protection against threats". Fundamentally, the SEC sees its mission to drive security as well as securities.

The recent history of the SEC's cyber rules

In October 2011, the SEC Division of Corporation Finance **published disclosure guidance specifically for cybersecurity**. This guidance (not rule or regulation) is relatively short and provides "views regarding disclosure obligations relating to cybersecurity risks and cyber incidents".

In 2018, the Commission itself **issued guidance** 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**.

Those rules were modified – which we'll dig into – and **adopted in June 2023**.

As a result, security leaders and teams are experiencing yet more pressure. Security, particularly security governance, is a topic that is becoming red hot. Everyone has more security tools, yet breaches are still happening, suggesting a failure in governance.

The word governance is often used but has many different nuances depending which definition you pick. Wikipedia defines governance as the "process of making **and enforcing** decisions within an organization". I personally think this is clearer than the more pointed definition of cybersecurity governance, which **CISA defines** as "a comprehensive cybersecurity strategy that integrates with organizational operations and prevents the interruption of activities due to cyber threats or attacks."

Is it governance? Or a strategy? That question leads me to prefer the generic definition: governance is how you make decisions, and how you make sure those decisions are being followed. And that is why I assert that the biggest challenges in cybersecurity are of governance, specifically making sure decisions are being followed. We'll come back to this, frequently.

(As an aside, the SEC has been asking for disclosure of climate impact risks, which has been similarly badly implemented, and has now **adopted rules for climate-related disclosures**. Expect more disclosure requirements from the SEC).

What's different from the proposals?

The new regulations differ from the earlier proposals and guidelines. The proposals from 2022 set out four major areas of disclosure:

Timely (exceptional) and periodic reporting about material incidents.

- Periodic disclosure of its policies and procedures to identify and manage cyber risk.
- Periodic disclosure of management's role in implementing cybersecurity policy and procedures (or governance).
- Periodic disclosure of the board of directors' cybersecurity expertise (if any, the proposal text noted slightly wryly)

Comments were requested, and many were received, resulting in changes to both periodic disclosure and incident disclosure, however one major change saw the dropping of the requirement to disclose the board's cybersecurity expertise.

The final rules **can be found here**, and is frankly a good read as it does examine the ins and outs of the changes from the proposal, explore comments, and provide balanced rationale for how the rules were honed and finalized.

The summary of changes from previous proposals is:

- 8K Rule 105: clarity on timelines, suggestions on materiality decision-making, exceptions for national security and public safety reasons
- 106(b): revised to create clarity on what is, and isn't, expected to be disclosed, and be less granular with less chance of being seen as prescriptive
- 106(c): as with 106(b), less granularity is required than the original proposals, and less details on frequency and overall oversight
- Dropping of disclosure of board cyber expertise

Many others have provided insights and guidance into their interpretation, notably the big 4, and other security vendors. PWC have a simple, **no-nonsense view of what functions are required to support disclosure**:

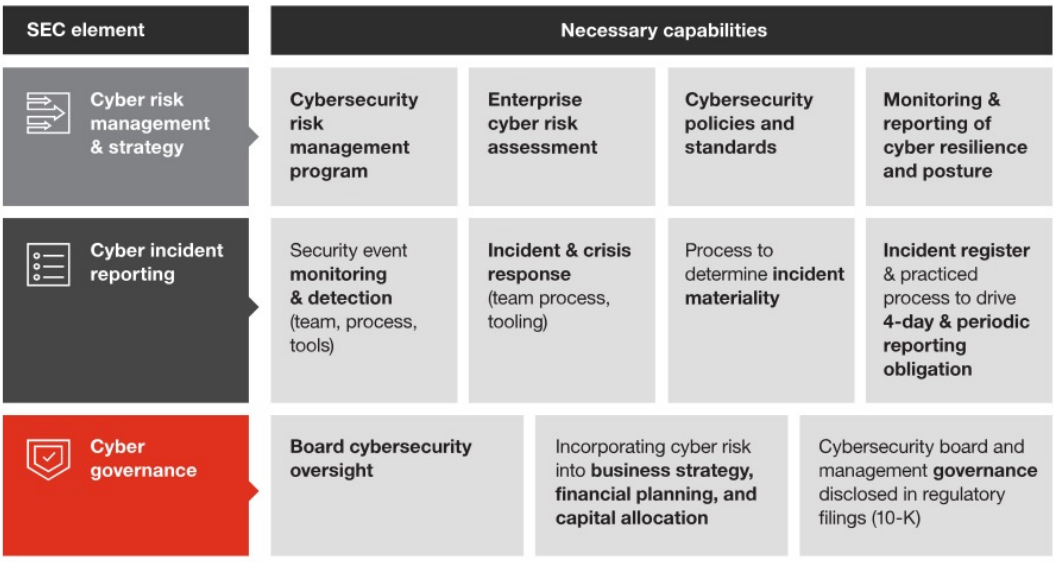


Image PWC

Others provide similar viewpoints and clarity.

02 The new rules

8-K 1.05: Timely incident disclosure

This aspect of the new disclosure requirements seems to have received the lion's share of comment and the most coverage both in proposed and final forms.

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. One must be filed within four days of discovery of such an event – this is the timeline for any 8-K triggering event, not just cyber incidents. Previous guidance from the SEC suggested companies should file an 8-K following a cyber incident, but the guidance was not being followed consistently. Consequently, we now have rule 1.05 in the 8-K.

If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe 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.

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 SEC has reaffirmed its alignment with this decision and is not seeking to define materiality in a specific way for cyber incidents, in the same way it is not changing timelines.

It's important to note that incident disclosure, and indeed decisions on materiality, will not fall to the CISO. However the CISO should expect to be intimately involved in the processes that lead to a decision on whether to disclose an incident. on this, telling CISOs: "Do not assess the materiality of a cybersecurity risk or threat" and "Do not overshare". The Big 4 are all unified behind this approach, too.

The clock starts ticking quickly when it comes to disclosure: instruction 1 for 1.05 states:

This is actually an improvement on the proposal for organizations, it previously stated "as soon as reasonably practical" which is subtly different from "without unreasonable delay".

This raises questions:

- If a security operations center (SOC) discovers an indicator of compromise (IOC), does that start the clock ticking? Because if so, that's challenging!
- 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?

There is no guidance on who makes the materiality call, however the final rule rationale does make a suggestion:

> ***Item 1.05 does not specify whether the materiality determination should be performed by the board, a board committee, or one or more officers. The company may establish a policy tasking one or more persons to make the materiality determination. Companies should seek to provide those tasked with the materiality determination information sufficient to make disclosure decisions.***

There are further instructions giving guidance that you cannot delay filing your 8-K due to having incomplete information. Instead, you should disclose that you do not yet have the information needed.

Four days is a short window, especially when you consider that 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**, defenders need to move fast.

There is an exception. Rule 1.05(c), which requires a high bar to pass as it requires written notification by the Attorney General confirming that:

> ***If the United States Attorney General determines that disclosure required by paragraph (a) of this Item 1.05 poses a substantial risk to national security or public safety, and notifies the Commission of such determination in writing, the registrant may delay providing the disclosure required by this Item 1.05 for a time period specified by the Attorney General.***

This is a non-trivial exception to have granted as it involves the Attorney General of the United States issuing such an exception. The time period of the delay is, ultimately, down to the Attorney General, but starts at up to 30 days, may be extended by up to a further 30 days, then up to 60 days, and any further delays will be considered by the Commission if requested.

What shouldn't be included?

The proposals gave examples of the sort of information to be considered to disclose but these caused quite an outcry as the proposals may well have given an advantage to an adversary. This has been significantly changed, and the following instruction is now provided:

> ***4. A registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident.***

This instruction is helpful, simple, straightforward and does relieve significant load from IT and Security teams. Less is definitely more in this case.

In summary:

- Your SOC is critical to identifying incidents, material or not. They need information at their fingertips to enable this;
- Processes need to be in place for determining materiality quickly, and the bar set for materiality is low. Having effective communication based on common understanding, and common data, is critical;
- Disclosure of cyber incidents is treated the same as other incidents, but will need exercising and refining regularly. Cyber needs to have a voice at the Enterprise Risk Management table, and bring the right data and insight;
- Details of assets, processes and technology do not need to be disclosed. They do, however, need to be well considered and backed by attestable data;

Disclosure examples

Whilst it's not as burdensome as the proposals, cyber incident disclosure is now up and running. To date in 2024 there have been 19 mentions of "Material cybersecurity" within 8-K forms filed, across 14 organizations, 2 of which mentioned that "material cybersecurity" might impact them in the future and so are not disclosures under rule 1.05. The other 17, across 14 organizations, were Rule 1.05 disclosures. All of this is open to anyone via **EDGAR search**.

A few are generic, perhaps disclosed due to the low bar being set for materiality. For example, the **Federal Home Loan Bank of New York** discovered an attempt to obtain money through a compromise of a fourth party (vendor of a third party vendor) which was detected and closed down. This seems a straightforward incident that was discovered, handled and closed off. As an investor, this would give me confidence that processes and technology are in place to monitor, flag and handle such incidents.

Others are more concerning:. Microsoft, for example, **filed in January** to disclose that emails for senior leadership, cyber security, legal and other roles had been accessed, and that access was disabled on 13 January. They further stated that "at the time of filing, this incident has not had a material impact".

They **further disclosed** in March that the attacker had used information gathered in the attack to gain or try to gain access to systems including source code, and that they are still investigating, and that further "unauthorized access may occur."

This is obviously not the we'll see last of this particular incident. Whether there will be further 8-K notices for this is unknown, but it should certainly be included in the 10-K Cybersecurity section for the annual report. That will be a busy section. Interestingly, this does not seem to have had an impact on Microsoft's share price.

Some journalists are obviously busy watching for 8-K filings as this has been picked up in a few outlets, including the **Wall Street Journal**. Given the interest in all things cyber from the White House down, this trend seems likely to continue.

We expect to see generic disclosures, such as "we found an abnormal event" and "as a result, we executed our processes upon discovery of the event", finishing with "we do not expect this to be materially impacting on our business".

Whether these are accepted by the SEC, and investors, and what happens if the disclosures turn out to be understating the risk, is yet to be seen. The fact that the SEC have brought fraud charges against a CISO and organization for statements *prior to these new rules* may be indicative of the SEC's attitude towards what they see as playing a little fast and loose with disclosure, and indeed public, statements.

S-K 106(b) and 106(c): Annual cyber disclosures

The SEC has always required risks to be disclosed, however as noted previously the depth and completeness of disclosures around cyber risk have been variable. Given the threat posed by digital operations that every organization relies on, the SEC felt things had to change, and with good reason.

In the proposed regulations from March 2022, the SEC observes that most registrants that disclosed a cyber incident in 2021 did not describe their cyber risk oversight policies and procedures in any filing. It proposed that better disclosure would allow investors to make better informed decisions. Given the observation around lack of disclosure of policy when incidents are being reported, it's hard to argue with the proposal. These have largely been implemented by the new rules, although not quite to the extent suggested by the proposal.

In the introduction to the proposed regulations, the SEC posited that organizations "may" have cybersecurity policies, procedures, approaches, and tactics but, crucially, the SEC does not mandate what they are. 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.

Let's split into what the two rules cover:

106(b) – Risk management and strategy

The finalized rule is short, with no further instructions provided. It is straightforward and easy to read, but remains subjective. There are two parts: processes, and current threats.

Part 1:

> ***Describe the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:***
>
> ***(i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes;***
>
> ***(ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and***
>
> ***(iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.***

So, processes to assess, identify, and manage risks from cyber threats, again qualified with the word "material", must be disclosed.

This is very open ended, and subject to interpretation as to how much process should be disclosed. What is critical though is that whatever the processes are, they must be disclosed.

From reviewing 10-K filings since the deadline passed, the level of detail is varied, with some filing a paragraph or two, and some filling pages.

One extreme on the lower range has the phrase "We do not presently maintain any formal processes for assessing, identifying and managing material risks from cybersecurity threats", which I have to admit surprised me. This is a filing from a smaller company, which strictly speaking did not need to include the section.

Others mention their approach to risk assessments. One extremely large global organization that has had significant data losses historically and recently discloses that an annual assessment is carried out that "includes assessments of their security program's control domains", rolling into "an enterprise risk scorecard reviewed on an annual basis".

Annually is not very often. One would hope for monthly as a minimum, and ideally such a scorecard should be reviewed continuously. As an investor, what would I think of that? As a user of their service, what would I think? As a subject of data held by them, what do I think? Personally, I'm unimpressed. But I'm also thankful that they have told me their approach.

NIST alone has been mentioned in 10-K filings 1188 times for the first three months in 2024, compared with 128 times in the whole of 2023 (98 times in Q1 2023), 94 times in 2022, 64 times in 2021, and 48 times in 2020.

In total, there were 7997 10-K filings in 2023, with 5660 being filed in Q1, suggesting that 70% of all filings are in Q1. Using that as a basis of extrapolation predicts that there will be nearly 1700 reports mentioning NIST in 2024, compared to 128 throughout 2023. A 13x uplift.

That's quite an uplift. Even if taking just Q1 figures, that's a 12x increase between 2023 and 2024.

Looking at a company that has recently been in the spotlight, SolarWinds filed their 10-K already this year. In it, they state:

> ***We use, among other frameworks, the NIST Cybersecurity Framework and CIS Critical Security Controls as guides to help us identify, assess, and manage cybersecurity risks relevant to our business. Although we refer to such frameworks in developing our cybersecurity risk management approaches, our use of them as guides is not intended to suggest that we meet any particular technical standards, specifications, or requirements set forth therein.***

Given the current **SEC initiated lawsuits** against them, I expect to see this language become boilerplate as one of the complaints raised by the lawsuits is that their public statements around use of NIST CSF. The SEC points out that SolarWind's public Security Statement, on their website, claimed "SolarWinds follows the NIST Cybersecurity Framework with layered security controls to help identify, prevent, detect and respond to security incidents."

Compare and contrast with the new language in the 10-K of 2024. Expect to see caveats appearing as more organizations get to grips with the implications of what they put in their 10-K filings for cyber security.

The SEC **advises investors** that "Laws and regulations prohibit companies from making materially false or misleading statements in their 10-Ks".

Equifax, for example, has carefully structured their 10-K cyber section to say: “Our unified security and privacy controls framework is based upon the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF) and Privacy Framework (NIST PF)”.

Would a reasonable investor understand that based on does not mean full adherence to and compliance with NIST CSF and PF? I don't know, and I wouldn’t like to be the test case.

Onto Part 2 of 105(b):

> ***Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.***

This again has seen widely varying answers. Taking one example from a smaller reporting company:

We have not experienced any material cybersecurity incidents. We have not identified risks from known cybersecurity threats, including as a result of any prior cybersecurity incidents, that have materially affected us, including our operations, business strategy, results of operations, or financial condition.

As a reasonable investor, that would cause me to stop and raise an eyebrow if not two. I do not wish to judge, however I find it odd that any company would state they have not identified any risks from cybersecurity threats.

Others take a more cautious approach and share further details, including going back historically. One, for example, references an incident in 2017 where customer data was lost that may still cause “material adverse effect on cash flow, competitive position, financial condition or results of operation”.

As a reasonable investor, that sounds like a wise disclosure, along with the further disclosure that their business makes them “routinely the target of attempted and other cyber security threats” from third parties and insiders.

They further describe the potential impact of these risks, which ultimately is a loss of stakeholder trust and the commensurate loss in revenue.

Solarwinds, to return to an extreme example, discloses that their cybersecurity incident has resulted in an investigation by the SEC that is materially impacting their business. This is covered in their general risk section and referenced in their cybersecurity disclosure items.

The rules seem simple and seem simple to follow. Ensuring your submission is defensible will take more of the security team’s resources if not carefully managed.

106(c) – Governance

Similarly split into two parts, 106(c)’s parts cover the Board of Directors oversight of cyber governance and management’s role. The disclosure of board member’s expertise is not explicitly asked for, as this proposed rule has been dropped in the finalized rules.

Part 1 is again straightforward, with no subparts and instructions clarifying how foreign private issuers should respond. It appears at first glance less demanding than the March 2022 proposals, however the paragraph largely encompasses the 3 parts proposed in this area.

> ***(1) Describe the board of directors' oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.***

Responses to this again vary between surprisingly light, and the more considered answer which is typically that the board oversees all material risks, before describing how subcommittees govern the process. This seems like best practice, aligning with wider risk management and having specific focus teams on cyber.

I have not witnessed a **Gold/Silver/Bronze approach** documented in any 10Ks yet, however that is more aligned to UK emergency services but appears to be gaining traction. Nor have KRI, KPI or KCI been mentioned, however that may be too low-level a detail.

Moving to part 2 of 106(c):

> ***(2) Describe management's role in assessing and managing the registrant's material risks from cybersecurity threats. In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:***
>
> ***(i) Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;***
>
> ***(ii) The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and***
>
> ***(iii) Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.***

Whilst the requirements to disclose the cyber expertise of the board went away, there is a requirement here to detail the expertise of members of the structure responsible for managing material cybersecurity risks.

These requirements are also slightly different, and less exhaustive, than the proposed rules, notably dropping the explicit question around whether a CISO is in role and where they report to.

Many responses so far have grouped answers to parts 1 and 2 together, which makes logical sense.

There is no consensus yet on what "good" looks like here, however from the 10-Ks that I have reviewed there are a few features that stand out as going above and beyond the minimum:

- Disclosure of approach to security culture.
- How responsibility is clearly shared with business leaders.
- The board's continued education on cyber threats and realities.
- Any use of scorecards to track security initiatives.
- Frequent updates from the CISO to the board and management structures.
- Inclusion of cybersecurity control performance evaluation.

Some cover all of these, some cover none. By examining a few of the big companies you can see who is taking a more thorough approach to disclosure, and indeed some provide more detail in their governance section than they do for their risk and strategy area.

A trend already does seem to be to show the credentials of the CISO and wider security leadership team, with CISSP being mentioned 323 times in 10-K filings for 2024 Q1, as opposed to 3 times in the same period in 2023.

I expect this area to rapidly evolve as people review what others are disclosing and the impact it is having. Some organizations take the opportunity to portray themselves as a safe pair of hands. Others, SolarWinds included, are taking a "more is less" approach to this section, which is somewhat understandable.

Whether disclosures here are picked up by investors and raised on regular calls is as yet unknown. Some have been proactively discussing cybersecurity approaches on their investor earnings and update calls, signaling the importance they place upon it. That openness can only deliver reassurance to investors.

For annual disclosure, in summary:

- Disclosure is mandatory, the level of detail that you must provide is not. The cyber team will not be responsible for 10-K filings, but they must be consulted and should bring recommendations backed by data
- 10-Ks are open to anyone, from investors to competitors, to journalists, to those with bad intentions. Careful consideration should be undertaken to ensure there is nothing disclosed that would present an opportunity for exploitation
- Previous incidents need reporting in 10-K. A process backed by solid knowledge that is auditable and ultimately attestable needs to be in place to ensure nothing is omitted
- The SEC has a history of litigation. Disclosure needs to be complete, and should be backed by unimpeachable data.

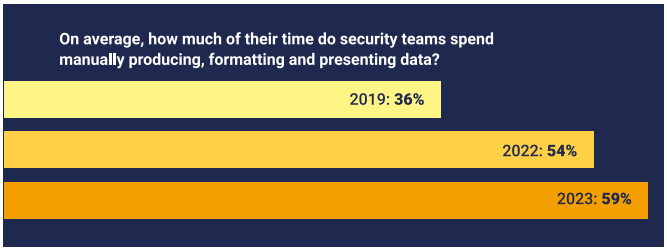
The current realities

SEC reporting, combined with daily news reports covering breaches, are bringing cybersecurity and its governance into the spotlight. This is putting yet more scrutiny on security leaders who, for years, have been the most inspected leaders in organizations.

New cyber regulations have been coming thick and fast, from White House Executive Orders to new DOD requirements, to DORA in the EU: it seems every regulator is expanding their coverage of cyber risk management. A Panaseer survey in 2023 found that 74% of security leaders expected new regulations to have a positive effect on their ability to manage cybersecurity posture. The same survey found 35% of security leaders saying they expected the impact to be significant on their team. In other words, the impact on the team is going to be big, but it's going to be worth it for the outcome.

We believe we are seeing this reality of high impact on teams and improved security posture management play out right now, as security budgets in 2024 appear to be protected despite pressures to reduce spend. Of course, this comes with the need to show value from the investments made.

Both regulatory and budgetary pressures mean there is a real drive for security to demonstrate the efficacy of their programs, leading to yet further internal audit, compounding the external pressures. Unfortunately, this appears to have a negative impact on security teams in particular, who are now spending 3 out of 5 days on manual reporting (**SLPR 2023**).



Furthermore, over half of respondents to the survey who knew how audits were conducted stated they were executed manually.

With the increased visibility, it seems clear that CISOs are hoping to secure more budget, however our survey suggested that they would need an uplift of 40% for CISOs to be "confident" in their ability to mitigate cybersecurity risk.

And perhaps due to the time spent reporting, sapping resource and energy, 52% of respondents would prioritize hiring more staff.

Bring in the new proposals for NIST CSF 2.0, which introduces a new foundational function of "Govern", and it seems changes are coming that bring much needed oversight and governance to the world of cyber security risk management.

There are some hard realities that seem to be challenging the status quo of manual audit, especially of policy enforcement around cyber:

- You can't govern what you don't know.
- You can't govern what you don't measure.
- You can only measure and therefore govern if you trust the data.
- You can only trust the data if you've validated it, and it survives the scrutiny of audit.
- You need security knowledge.
  - Information isn't enough. It needs rules and context to be knowledge.
    - And data isn't enough, it needs purpose to be information.
- You don’t have enough people in your security team to continue to do things as they are.
  - There’s not enough skills in the world to recruit out of this challenge.

As well as this, IT is on a non-stop trend to decentralization. More business leaders procure their own technology but don’t necessarily ensure it meets security policy. Gartner has noted this trend, and believes the answer lies in organizations having wider “cyber judgment” than just more security professionals in IT and Security teams. To me, the answer lies in enabling security to partner with business for business results.

With SEC disclosure rules, your cyber governance, risk management and strategy is out there for all to see. Painting an inaccurate picture is not an option.

03

Cyber governance: a new approach

Incident disclosure

Our clients tell us that, before implementing Panaseer, what typically happened when an incident was discovered was a scramble to determine what the impacted assets were, and where they sat in the organization's critical business processes. CMDBs, which should have answered the question, are silent if they do not know the asset, or rely on manual data which is typically out of date. Whatever they, or other systems said, would need to be manually checked.

At this point, incident response teams became detectives trying to piece together the clues. And all of this would now have to be done against the clock enforced by a regulator with teeth. You now have four days from discovery to its potential disclosure. Tick tock.

Panaseer has calmed the scramble. It has enabled teams to understand the business context of an asset, the processes it is involved in, the applications it runs, where it sits, who owns it, who is responsible for its security, and more. Instantly. With confidence that the knowledge that is providing that insight has been validated and is fully auditable. Even for unknown assets.

This is, in turn, providing insight that is used by the team responsible for determining risk and therefore materiality. And because the knowledge has been continually validated, the team can rely on it.

As CISO, I'm one of the most scrutinised in the company. Thanks to Panaseer I have a low resting heart rate.

Informing risk management and cyber strategy

Panaseer's Continuous Controls Monitoring platform measures, reports and scores the continual truth of your security control status across the assets that make up your digital estate. It doesn't do this by sampling, or questionnaires. It interrogates your tools for their status across all assets. Uses a feature we call Business Logic, it derives the context of the asset: who owns it, who is responsible for it, which business process it is part of. This context enables prioritized decision making.

By using the dashboards it provides, you see the reality of your compliance with your own policies, and can take action to address non-compliance, or Matters Requiring Attention (MRA) even before a point in time audit – whether that be internal or external.

Panaseer delivers the attestable truth of your security controls across your security assets, mapping to NIST CSF and CIS frameworks. By understanding this, you can inform your risk management approach and evolve your security policies to reflect the evolution of your posture and threat landscape.

Our customer know their assets, know the status of controls on their assets, understand their policy compliance and know what to do next to have the most impact on their status against risk appetite or tolerance.

Automating cyber governance

Our customers tell us that one of the biggest transformations they experience is not so much in the measurements, insights and credibility we give them. But more so in their ability to partner with the business to drive wider accountability for cybersecurity throughout the organization. Gartner terms this "cyber judgment", but we believe it's a natural way to ensure that cyber responsibility is decentralized and is correctly implemented throughout an organization.

One organization told us that their attempts to drive security responsibility wider failed due to a lack of data trust. Panaseer doesn't just deliver a database with all your security tools' data in that you can search It delivers a knowledge base on assets augmented with business logic, giving context. We work with you to validate the logic, so you can be sure you can know the reality of your assets, control status and policy adherence, and that it can be trusted and recognized throughout the organization.

A further benefit is that Panaseer delivers the ability for teams across all parts of the business and across all lines to self serve the information they need to do their jobs without relying on manual effort.

Scorecards have been mentioned in a number of 10-K reports already. However, many scorecard efforts are lackluster. They are reported infrequently, rely on significant manual effort to create, and are not driven by control data but rather by sampling or questionnaires. Panaseer delivers a Cybersecurity Controls Scorecard that summarizes your posture, driven by the most important initiatives, each of which has its own score.

Finally, another word from PWC, who have provided this graphic on their SEC disclosure website:

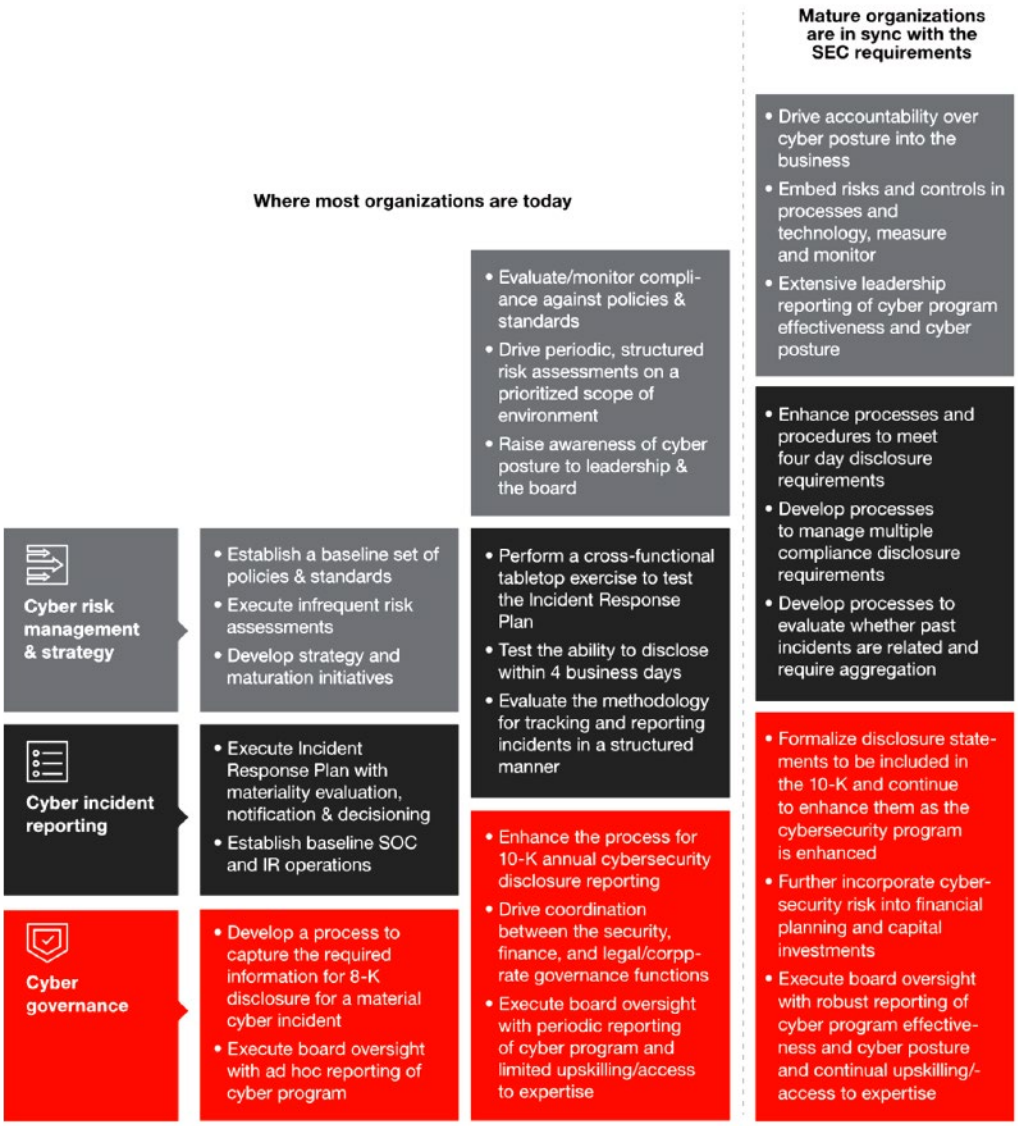


Image PWC

Panaseer CCM supports every part of the journey to maturity highlighted.

Conclusions

The three new SEC disclosure rules are small and innocuous but their impact is already being felt and seen. Companies large and small are filing 8-Ks to disclose cyber incidents, and 10-Ks filed since mid-December are giving good insight into the approach to cybersecurity strategy and governance.

The penalties for inaccurate disclosure are severe, and are being applied to individuals and the organization themselves, so being creative on SEC disclosures is not an option.

The situation that cybersecurity professionals find themselves in is one of extreme inspection. Survival is difficult, but it is possible to thrive by transforming the way cyber engages with business. That relies on data driven decision-making, backed by automation and validation, enabling a widening of cyber judgment and better understanding of the realities and expectations of cyber policy adherence.

There is another, arguably more important, aspect to the new disclosure rules: it gives organizations the opportunity to not only reassure investors that they are managing cyber risk and incidents well, there are clear spaces to differentiate against competition.

When making investment decisions – or supplier decisions, or indeed any decision that would be influenced by your cyber security processes and governance – the SEC filings provide reassurance. Or otherwise. I was exceptionally surprised to see companies quoting in their 10K that they "have not identified any cybersecurity risks", which is akin to **Nelson's oft misquoted line** of "I really do not see the signal" when lifting a telescope to his blind eye.

To see global organizations admit they rely on annual audits also meant I would be reassessing my use of, never mind investment in, their services.

The cybersecurity status quo is changing: do you want to be ahead of the curve, or lagging behind?

Panaseer would be pleased to share further thoughts on how we can help you on your journey.

Automated security posture management

Continuous Controls Monitoring for enterprise security