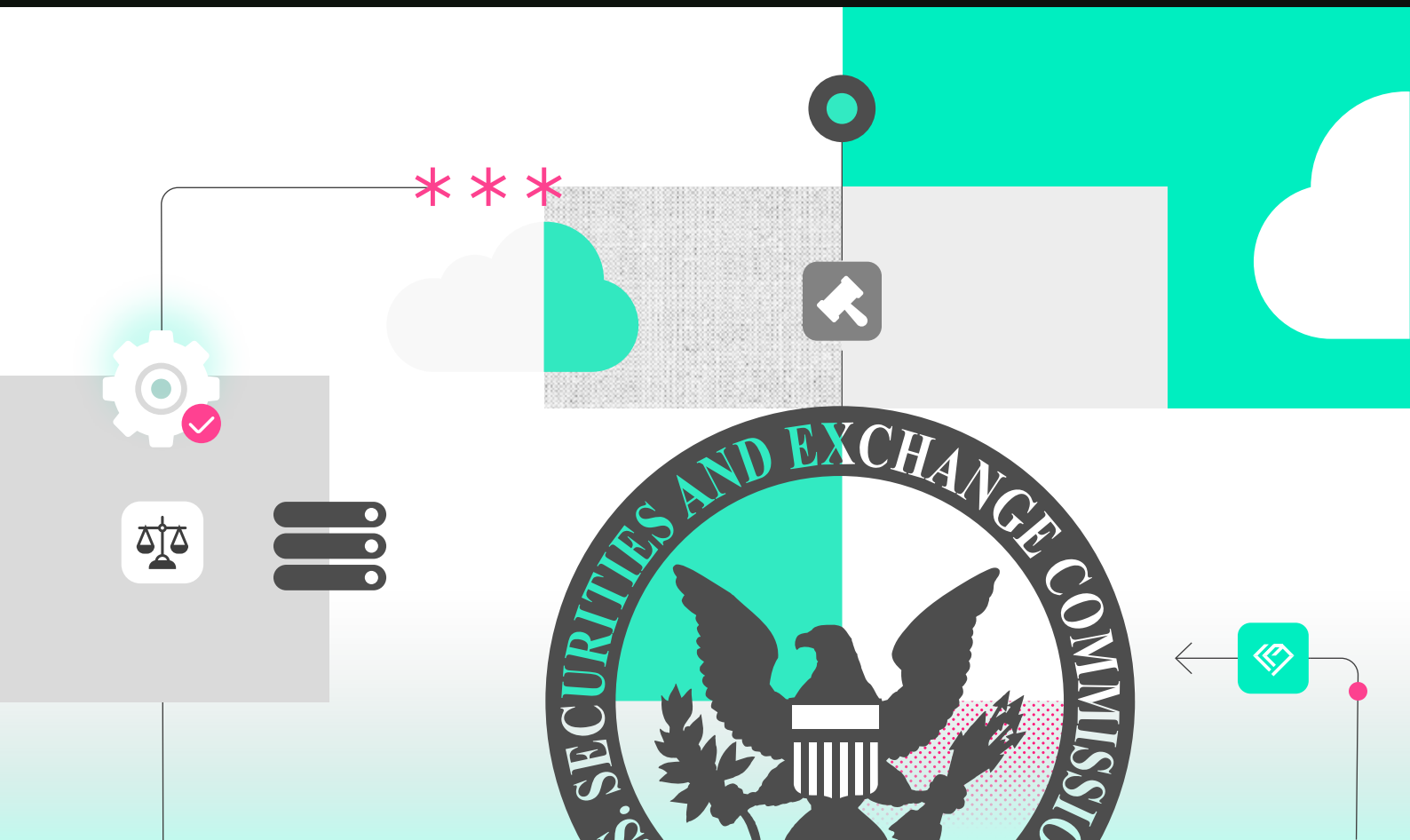
The New SEC Cybersecurity Rule: The Good, the Bad, and the Maddening Frustrations and Contradictions

Concerned but surprisingly optimistic, CISOs discuss practical tactics to abide by the rules – and, incidentally, to better protect their companies.

By Evan Schuman,
Contributing Writer for *Dark Reading* and *CSO Online*



The SEC cybersecurity rules that went into effect in December 2023 will absolutely plunge CISOs and boards into a lot more cybersecurity discussions and a massive number of additional filings. But a fundamental concrete answer remains: To what end? Will it result in more secure companies or simply generate lots of paperwork? Will it truly make board members take security more seriously? Will it deliver meaningful information to investors and potential investors or simply deliver to them words that have no actionable information?

Enterprise CISOs and other security and legal experts are mixed on the answers, but the hope is that the new rule will definitely shine far more light on companies' security monitoring controls and threat landscapes. In cybersecurity, more light is almost always good. Almost always.

The emphasis on "almost" speaks to the other group impacted by the new rules: cybercriminals, nation-states, and others with ill intent. That is just one of the many delicate balancing act dances that the new rule forces on CISOs. How can the filings be specific enough to help the investing public while simultaneously being vague enough to not help bad guys do their bad deeds?

Even **former Uber CISO Joe Sullivan**, who was charged and convicted of failing to appropriately report a material cybersecurity incident to the SEC, applauds the new SEC rule, saying that although it's not perfect, it's better than what existed before.

> We can nitpick the details as much as we want, but this is the right way to do it. I seem to be the person who's criticizing the SEC less than everyone else because I think we should praise them for trying to make rules.

Joe Sullivan
former Uber CISO

As reported in TechCrunch, Joe said: "We can nitpick the details as much as we want, but this is the right way to do it. I seem to be the person who's criticizing the SEC less than everyone else because I think we should praise them for trying to make rules

Let's start by identifying some of the top myths about the new rule and what the rule actually mandates.

False Belief: It requires reporting a security incident within four days

Truth: The rule absolutely does not require that. The SEC requires the company to report a security incident within four days of determining that the incident is to be considered material for SEC purposes. Even more to the point, the SEC does not specify any time limit for how long the company can take to determine that an incident is material.

That said, the absence of a time limit to make that material determination doesn't mean that a company can sit on the information about a security incident forever. If the SEC eventually finds out about and chooses to accuse the company of deliberately hiding information from their investors and potential investors, the SEC can and will act.

The process of determining that a security incident is real takes some time, but the decision for whether it is significant enough to be considered material, that could take quite a bit longer. Just be prepared to defend everything in a courtroom later on. There are oceans of things that are not certain in a security investigation, but only one fact that is absolutely definite. That definite fact is that everything will eventually surface. As Murphy's Law establishes, the more embarrassing the details, the more quickly it will come out.

False Belief: The rule is solely about data breaches

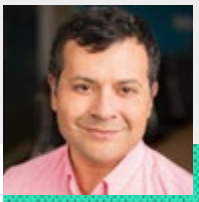
Truth: The rule envisions all security incidents, including ransomware, DDoS attacks, sabotage and anything else that threatens the security and assets of the company.

There are a couple of reasons for this. First, "security incident" is a better term for addressing anything that might impact the investing public. Secondly, the term data breach means very different things to lawyers and compliance specialists compared with CISOs and other security professionals.

To a security professional, a breach is what the name implies: a breach of security. If someone or something gets into a restricted area without authorization (whether by brute-forcing credentials, using stolen credentials, or through some other means such as accessing a vulnerable storage bucket), that's a breach of security and, therefore, is a security breach.

But to lawyers and compliance people, a breach only exists if protected and/or sensitive information is exfiltrated. That's what almost all compliance rules care about. That means that if an attacker gets into a sensitive area – such as payroll or the area where secret blueprints are stored – but doesn't exfiltrate anything, they don't consider it a data breach or even a security breach.

> Every CISO needs to go look at their continuous monitoring controls. Do you have the right incident response — people, process, and technology — to quickly connect the dots and help the management team understand what happened, remediate the breach, and decide if an incident is material?



Mario Duarte
Former VP of security for Snowflake

False Belief: Given that publicly-held companies have always had to report every material incident, there is nothing new here

Truth:This is true but it lacks the proper context. Yes, the fact is that anything material needs to be reported is nothing new. But the rule now requires breaking out cybersecurity incidents into a separate form.

"This will lead to far more internal attention. This is no longer a line buried in hundreds of thousands of lines in a 10K," said SailPoint CISO Rex Booth in *Dark Reading*.

The "attention" part is crucial. By requiring companies to report all material security incidents, that forces the company to routinely review security incidents to determine if any rise to the level of being material. Typically, that will mean the creation of a committee consisting of the CISO, the CIO, the CFO, General Counsel, Investor Relations and sometimes the COO and other executives.

The fact that all of those players will now have to set aside time every week or whatever frequency the company decides is a big deal. For many companies, that is a massive increase in how those execs think about cybersecurity. That alone is a powerful step to getting companies to take cybersecurity more seriously.

Secondly, to make the decision for whether an incident is material, committee members must deeply think about how security can impact operations. Again, having them think about that on a regular schedule is also a powerful step.

Partially False Belief: The SEC rule only impacts publicly-held companies

Boards are getting more security savvy. What kind of metrics should they be demanding? What is the threat landscape? What technical security controls are in place? How are the risks identified across the company? How is the risk measured?

Selim Aissi
former CISO for Ellie Mae

The essence of the belief is technically true, in that the SEC's jurisdiction only covers publicly-held businesses. But that doesn't factor in the massive influence of the SEC in the United States. And given how many of the Fortune 500 are multinationals, it is also unrealistic to assume that this won't cause any changes outside the U.S.

When public companies are routinely making these disclosures, it is absolutely going to change the perspectives of their privately-held competitors. Customers – regardless of whether they are businesses or consumers – often do not care whether the supplier/vendor is private or not. Once customers get used to seeing those disclosures, they will start to expect and insist on them from everyone in their supply chain. Private firms may not have to answer to Wall Street, but they do have to answer to their customers – as well as private investors. Once the data disclosure floodgates open, no one is likely to be immune to the change.

The Legal Catch-22

- If someone above the CISO changes a filing and makes it fraudulent, the CISO could be legally exposed even if they had nothing to do with the fraud.
- If the CISO knows of a fraud and says nothing to the SEC, the CISO could get into trouble.
- That means the CISO must take concrete due diligence steps to determine if the filing is indeed legitimate.

Board Risk Tolerance

What the CISO and other executives need to hear from the board is a risk tolerance level. The problem is that almost all boards – when asked – say they want to have a low risk tolerance. That's great, except that many don't typically act that way. Board members will often vote to have a low-risk approach but then push back on security budget increases and deny the CISO the resources to implement the controls required to lower risks to an acceptable level.

Selim Aissi was previously the CISO for Blackhawk Network and Ellie Mae, the VP of Global Information Security for Visa, and the chief security strategist & architect for Intel. Aissi also oversaw safety-critical embedded software for Applied Dynamics, General Motors, and General Dynamics. He currently serves as a board member and technology advisor.

Aissi argues that boards must understand cybersecurity better so that they can both ask better questions and understand the implications of the answers better.

"Boards are getting more security savvy. What kind of metrics should they be demanding? What is the threat landscape? What technical security controls are in place? How are the risks identified across the company? How is the risk measured?" Aissi said.

It is also critical to have a very concrete plan to deal with risk issues, so that the board and the CISO – and all other executives – know what the rules are. The SEC says that every company's leadership must decide on their own how they will handle security. That means that boards must explicitly do that and put it into writing.

"You need to create a playbook with the rest of the management team about how to deal with the SEC. These need to be very clear playbooks, defining what a material incident is, what is the IR process after an incident is detected, etc." and it needs to be tested regularly, Aissi said. "No one is talking about the 10-K. It is very significant. It is a risk management document that gives everyone the opportunity to agree on what the security strategy looks like."

Governance Focus Is Critical

Charles Blauner, the former Global Head of Information Security for Citi and the former CISO for Deutsche Bank and JP Morgan, agrees.

"Having a well-documented governance process is very important. What the SEC has said is that you have to tell us how you do governance. You should be very clear about what your risk identification and lifecycle process looks like," Blauner said. 'Who has the right to approve risk acceptances? What is the process by which you and the board set risk tolerances?'"

Blauner added that CISOs must take a proactive approach to security. The problem is that due diligence means very different things to different people and certainly with different companies.

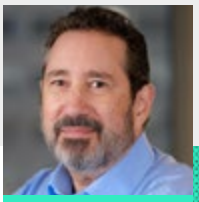
"There is no good definition of what due diligence is. There is no clear definition of material. Negligence is not defined so we have no idea what the bar is," Blauner said. "You can't judge a good security program by whether you have had a breach because any company can have a breach."

The wording of the SEC rules are deliberately designed to be vague. The premise is that the nature of companies under the SEC jurisdiction vary wildly in terms of size, vertical, nature of products/services and their level of risk. Therefore, they want to give executives the flexibility to structure a cybersecurity program that makes sense for that company's situation. The problem is that many CISOs see the rules as far too vague, making it almost impossible to know what the SEC wants.

Blauner is one of the CISOs who says that the SEC went too far in its lack of specifics. "They have to be flexible to some degree, but they were far too vague. Today in the U.S., it will be infinitely debatable, and the huge problem for CISOs is that they have proven to be the ones to be prosecuted. CISOs never ever make notification decisions. This puts CISOs in an impossible position. By title, they are the accountable person, but they are never the actual decision maker. CISOs are often at odds with the general counsel."

The SEC recently took action against a CISO who the SEC accused of misleading investors in an SEC submission.

> Having a well-documented governance process is very important. What the SEC has said is that you have to tell us how you do governance. You should be very clear about what your risk identification and lifecycle process looks like. 'Who has the right to approve risk acceptances? What is the process by which you and the board set risk tolerances?'



Charles Blauner
Former Global Head of Information Security for Citi

The SEC used the CISO's own words from internal communications to argue that the CISO knew that the disclosures written by others were incomplete. But that is not necessarily fair because executives have a different standard about what they say to an employee in an email, text, or Slack message compared with what they say in a public filing to the SEC.

Blauner said that CISOs must take notice and become far more careful and circumspect of what they say to anyone in writing about the company's security situation. "No more joking. You can't make an off-color joke about the security status of your firm. You can't vent. I would suggest overcommunicating, over-documenting and finding a good therapist."

New Rule Almost As Nebulous As SOX, PCI

Another cybersecurity expert is **Mario Duarte, the former VP of security for Snowflake.**

Duarte maintains that the SEC rules for cybersecurity are "a little nebulous. Not as detailed or as technical or as specific as I would like." He compared it to the early days of Sarbanes-Oxley (SOX) and PCI. He also agreed that flexibility is needed, but that the SEC has gone too far. "The SEC was uber nebulous as opposed to just being flexible. In the absence of one federal law to govern all these things, the SEC appears to be using a blunt instrument."

The SEC recently took action against a CISO who the SEC accused of misleading investors in an SEC submission.

The SEC used the CISO's own words from internal communications to argue that the CISO knew that the disclosures were incomplete. But that is not necessarily fair because executives have a different standard about what they say to an employee in an email, text, or Slack message compared with what they say in a public filing to the SEC.

Blauner said that CISOs must take notice and become far more careful and circumspect of what they say to anyone about the company's security situation. "No more joking. You can't make an off-color joke about the security status of your firm. You can't vent. I would suggest over-communicating and over-documenting."

Need for Effective Incident Response

Duarte also stressed that most enterprises need to be better at gaining immediate visibility into any ongoing attacks. One of the top reasons for this is that the speed and scale of cloud threats have mushroomed in size over the last five years.

The attack surface has dramatically increased due to the many cloud applications and resources – both shadow and authorized – spun up every day by DevOps teams in support of the business. Enterprises are also enabling a vast array of supply chain partners and other third party suppliers to access their cloud infrastructures — and the true security posture of those third-party environments is often hidden from the CISO's teams.

Finally, beyond the ever-shrinking on-prem environment, there are often tens of thousands of home offices with vastly different – and often unmanaged – technologies, further increasing the attack surface.

That is why trying to get visibility into as much of that enormous threat landscape as possible is crucial.

"Every CISO needs to go look at their continuous monitoring controls. Do you have the right incident response — people, process, and technology — to quickly connect the dots and help the management team understand what happened, remediate the breach, and decide if an incident is material?" Duarte asked.

> We have to pull ourselves up, we have to learn the policy side of it, and we have to learn how to make our voice heard. I think we have to develop leaders who can be real societal leaders who are experts in our profession.

Joe Sullivan
former Uber CISO

The SEC Rule's Many Catch-22s for CISOs

The rule is specific and yet vague, detailed but mind-numbingly amorphous.

Is an incident material for the company? What if an attacker steals the company's decryption keys, but the company has no reason to believe at the time that any encrypted files were stolen? Is the key stealing alone material? Even more likely, what if the scenario is flipped? What if an attacker steals 20 million files containing PII on customers, but all the files are encrypted? Is that a material incident? Is it even reportable at all? Is a CISO allowed to assume that an encrypted file cannot be cracked by an attacker?

It is important to look at the materiality question as two distinct decision points. The first decision, undoubtedly made by committee, is whether the security incident is itself material – in terms of financial impact, reputational impact, regulatory impact, etc.. But once the company has decided that it is material, the CISO then has to decide which of the huge number of details about the incident are themselves material? In other words, what details should be reported to the SEC, and which details are overly technical or overly sensitive or too preliminary?

Given that the materiality question ultimately comes down to the question of whether there is a "substantial likelihood that a reasonable shareholder would consider it important," an argument can be made that just about anything could potentially help some investor out there somewhere -- but an argument could also be made that no details about the security incident are going to prove helpful.

The CISO also must factor in two areas of likely exemption: Is revealing this particular detail going to be more helpful to potential attackers than it is helpful to potential investors? In other words, will revealing this information – such as how they were compromised or how many systems were compromised – hurt the company more than it helps investors?

The second area of exemption: How certain are we about any of these details? The details that a company knows in the hours after discovering a security incident are very likely to significantly change in the subsequent days, weeks and most likely for the next few months. Companies absolutely can update their filings as new forensic information materializes. But why falsely worry investors with details that may be wrong?

CISOs must try and use experience to figure out which details are likely solid and which are more likely to change very shortly. Which is worse? Publishing incorrect information or publishing something that is so devoid of specifics that it becomes pointless?

In One of the SEC's First Filings, Apparel Giant Draws Some Distinctions

One of the first SEC cybersecurity incident filings came from $12 billion apparel giant VF, which owns a wide range of clothing brands including The North Face, and Vans. VF's filing illustrates the tricky nature of these cybersecurity filings.

The security incident appears to be a double extortion attack given that it said "The threat actor disrupted the Company's business operations by encrypting some IT systems, and stole data from the Company, including personal data."

As for the impact, yeah, it looked like the incident itself was clearly material. "Consumers are able to place orders on most of the brand e-commerce sites globally, however, the Company's ability to fulfill orders is currently impacted." In other words, they can take customers' money but they won't be able to send them the product. That is indeed a problem.

But here is where things get interesting: "The incident has had and is reasonably likely to continue to have a material impact on the Company's business operations until recovery efforts are completed. The Company has not yet determined whether the incident is reasonably likely to materially impact the Company's financial condition or results of operations." They are drawing the distinction between a material event and whether it will last long enough to materially impact the quarter.

That means there are three material decisions to be made:

1. Is the security event material?
2. Which details of the event are material?
3. Is this likely to be financially material for the quarter?

There is another factor that sharply influences the materiality decision on a security incident. Although it is true that the committee appointed by the CEO will decide which security incidents to consider reporting to the SEC, as a practical matter, the CISO also has tremendous influence at the beginning of the process.

The typical enterprise has a large number of security events every week. The management committee that decides if any incidents are material will only be able to review a handful. That means the CISO will work with the security operations team and will eliminate the vast majority for consideration – based on their experience, understanding of the business, and best judgment.

The Legal Jeopardy Catch-22 Distinctions

If CISOs are not very careful, they could find themselves in trouble with the SEC even if they did absolutely nothing wrong.

Let's say the company has a security incident and the committee determines that it is material to the company. The CISO and their SecOps team work carefully, honestly, and forthrightly to document all of the details that the SEC must know about the incident.

What happens if someone up the chain, such as the CEO or general counsel, makes significant changes to the filing and hides or obscures critical details – to an extent that the filing seems to be fraudulent? That higher-up executive never runs the revisions by the CISO and simply files it to the SEC.

A few days later, the CISO goes to the SCC website and reads the filing and discovers the changes. Many enterprise CISOs believe that if they did everything right and someone else makes a change, then the CISO has nothing legal to worry about. Unfortunately, that is not the case.

CISO Defenses

- When offered the CISO role, negotiate an agreement to have the right to approve any SEC filings involving a security incident that your team managed.
- Seek company-paid Directors & Officers (D&O) insurance to protect yourself.
- If a CISO disagrees with the final decision, have a mechanism in place for the CISO to file a formal disagreement
- When the CISO files the memo about the incident, the CISO should capture it in various ways, including screen captures.
- If the CISO is not being shown the final document before filing, decide if you want to proactively read the final version. You might not want to.
- If the situation is bad enough, resigning might be better than getting dragged into a legal mess.

This gets complicated. If the CISO is aware of the fraud and the CISO opts to not report it to the SEC, the SEC could eventually come down on that CISO for concealing a fraud and potentially for being an accessory after the fact.

But – and here is where the Catch-22 becomes overwhelming – if CISO reports those changes as being fraudulent and if the SEC ultimately disagrees and concludes that the company was within its discretion to make those changes, then the CISO has no whistleblower protections.

Whistleblower protections only exist if the CISO is right and there actually is fraud. If the CISO is wrong, there are no protections, and the company can retaliate any way the company wants.

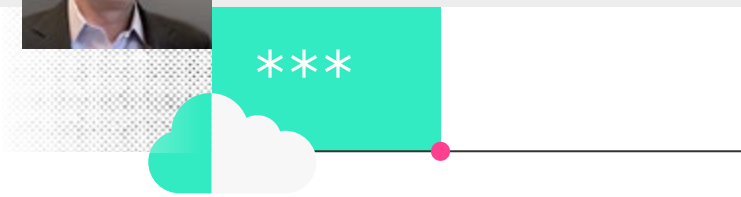
This forces the CISO to conduct reasonable due diligence. That would typically mean meeting with the general counsel to get a legal view of whether the changes are legally appropriate. It might also mean meeting with the head of investor relations to get that executive's view of the SEC interpretations. If the CISO is still not convinced, a meeting with the CFO and ultimately the CEO may be necessary.

If after all of those meetings, the CISO is still convinced that the filing is fraudulent, the next step would be for the CISO to retain private counsel. Eventually, though, the decision has to rest with the CISO.

The tiny ray of good news here is that if the CISO does all of the due diligence mentioned above, there is an excellent chance the SEC will consider the CISO conduct reasonable and not engage in any punitive action.

> It is important to underscore what these rules do not do in order to address a potential misconception. The Commission is not seeking to prescribe particular cybersecurity defenses, practices, technologies, risk management, governance, or strategy. Public companies have the flexibility to decide how to address cybersecurity risks and threats based on their own particular facts and circumstances. Investors have indicated, however, that they need consistent and comparable disclosures in order to evaluate how successfully public companies are doing so.

Erik Gerding
SEC's director of its corporation finance division



CISO Defenses

There are a variety of practical tactics that CISOs can use to better protect themselves

- When offered the CISO role, negotiate an agreement to have the right to approve any SEC filings involving a security incident that your team managed. At the very least, seek written documentation that you can at least review any changes made prior to filing and have a chance to make your case for changes to the CEO or whoever the executive is who has final word on the filing.
- Seek company-paid business insurance to protect yourself. If that is declined, consider buying it yourself.
- If a CISO disagrees with the final decision, have a mechanism in place for the CISO to file a formal disagreement. This filing is private and will not initially go to the SEC. Most likely, it will be placed in an HR file. But if this situation blows up months later, the SEC will see that you did everything you could to fight it.
- When the CISO files the memo about the incident, the CISO should capture it in various ways, including screen captures. Those files should be saved in areas that the CISO fully controls, such as a flash drive and cloud accounts that the CISO privately controls. (Not accounts paid for by the company.)
- This is more controversial in that some disagree whether this will indeed deliver any protection: If the CISO is not being shown the final document before filing, decide if you want to proactively read the final version. Some CISOs have argued that the legal exposure from someone changing the details in a filing involves knowledge of a fraud. If the CISO doesn't read the final filing, the CISO would have no knowledge of the fraud. It is legally questionable whether that defense will hold up in court, but some argue that it's worth considering.

According to Joe Sullivan, "We have to pull ourselves up, we have to learn the policy side of it, and we have to learn how to make our voice heard. I think we have to develop leaders who can be real societal leaders who are experts in our profession."

The SEC's Clarifications

In a Dec. 14 public note, **Erik Gerding, the SEC's director of its corporation finance division**, gave his version of why the SEC did what it did.

"It is important to underscore what these rules do not do in order to address a potential misconception. The Commission is not seeking to prescribe particular cybersecurity defenses, practices, technologies, risk management, governance, or strategy. Public companies have the flexibility to decide how to address cybersecurity risks and threats based on their own particular facts and circumstances. Investors have indicated, however, that they need consistent and comparable disclosures in order to evaluate how successfully public companies are doing so."

Gerding also defended the SEC's requirement of materiality for a security incident to be reported.

"The final rule requires public companies to disclose the occurrence of a material cybersecurity incident and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations. This disclosure is focused on the material impacts of a material cybersecurity incident. It is narrower than what the Commission originally proposed, which would have required additional details that were not explicitly limited by materiality. In revising the disclosure requirement, the Commission took into account not only the company's compliance costs but also its need to respond and remediate incidents."

Perhaps the most misunderstood part of the SEC's rule involves the four-business day requirement. Gerding also defended that provision.

> This will lead to far more internal attention. This is no longer a line buried in hundreds of thousands of lines in a 10K.

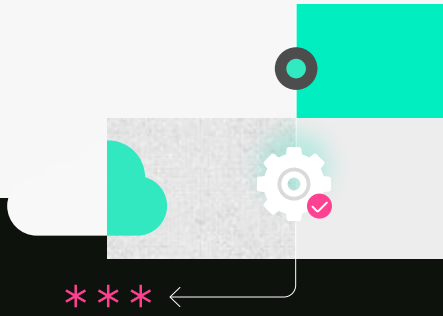
Rex Booth
SailPoint CISO

"Some have asked why the Commission chose four business days as the deadline for disclosure. This timing is consistent with the reporting of other events the Commission requires be reported on a Form 8-K, such as entry into or termination of a definitive material agreement or a bankruptcy. In adopting the four business-day deadline, the Commission explained that cybersecurity incident disclosure was not sufficiently different from other Form 8-K reporting events to warrant a different approach."

Gerding also stressed that although much of the attention has focused on the reporting of material security incidents, the new rule also "focuses on (annual) disclosures regarding management's role in assessing and managing material risks from cybersecurity threats, including, as applicable, whether and which management positions or committees are responsible for cybersecurity threats, and their relevant expertise."

Additional Reading

- https://techcrunch-com.cdn.ampproject.org/c/s/techcrunch.com/2023/12/08/ex-uber-cso-joe-sullivan-on-why-he-had-to-get-over-shock-data-breach-conviction/amp/
- https://www.sec.gov/news/speech/gerding-cybersecurity-disclosure-20231214?utm_medium=email&utm_source=govdelivery
- https://www.csoonline.com/article/1247504/how-us-sec-legal-actions-put-cisos-at-risk-and-what-to-do-about-it.html
- https://www.darkreading.com/cyber-risk/what-cisos-should-exclude-from-sec-cybersecurity-filings
- https://www.darkreading.com/application-security/do-cisos-have-to-report-security-flaws-to-the-sec
- https://www.darkreading.com/cybersecurity-analytics/confusion-surrounds-sec-new-cybersecurity-material-rule
- https://www.darkreading.com/cybersecurity-analytics/companies-must-have-corporate-cybersecurity-experts-sec-says
- https://www.darkreading.com/cybersecurity-analytics/sec-adopts-new-rule-on-cybersecurity-incident-disclosure-requirements



About Evan Schuman

Evan Schuman has tracked cybersecurity issues for enterprise B2B audiences for far longer than he will admit. His byline has appeared in The New York Times, Reuters, DarkReading, SC Magazine and CSO Online, among dozens of others. Evan has repeatedly guest lectured on cybersecurity issues for graduate classes at Columbia University and New York University and has consulted on cybersecurity content issues for McKinsey, Wipro, Microsoft, Capital One, BlackBerry, Harvard Business Review, Microsoft and MIT. He can be reached at **eschuman@thecontentfirm.com**

About Gem Security

Recognized by Gartner as a Cool Vendor™ for the Modern Security Operations Center, Gem delivers a cloud-native and agentless Cloud Detection & Response (CDR) platform that dramatically reduces the time to detect, forensically investigate, and contain multi-stage cloud attacks across all major cloud providers (AWS, Azure, GCP) and identity providers (Okta, Azure AD, Google Workspace).

Gem is backed by GGV Capital, Silicon Valley CISO Investments (SVCI), and Team8, with strategic investments by Cisco Investments and IBM Ventures. For more information, visit **gem.security**

Gem