PUBLICATION

Show Your Work: The SEC Cyber Rules and Documenting Materiality Analysis Under NIST FIPS 199

Authors: Justin S. Daniels
October 24, 2023

By Justin S. Daniels and Owen Denby

The date July 26, 2023, marks the latest evolution of the cybersecurity regulation landscape as the Securities and Exchange Commission passed cybersecurity regulations for publicly traded companies. At the open meeting, SEC Commissioner Jaime Lizárraga shared the sobering information that last year 83 percent of companies experienced more than one data breach, with an average cost in the U.S. of $9.44 million; breaches increased 600 percent over the last decade and total costs across the U.S. economy could run as high as trillions of dollars per year[1]. In light of these facts, it is fair to think these new regulations will have a widespread impact on publicly traded companies and their third-party vendors. The new regulation's centerpiece is its four-day material breach reporting requirement. This means that public companies will need to include a materiality assessment as a key element within their incident response plan. In this article we explore the following five ideas: 1) what the new SEC cyber rules are; 2) how the SEC defines materiality; 3) what the National Institute of Standards and Technology (NIST) FIPS 199 is; 4) why FIPS 199 is a good framework for assessing materiality; and 5) a review of a fictional cyber event employing FIPS 199.

What Are the New SEC Cyber Rules?

The SEC cyber rules are intended to require publicly traded companies to provide investors with information surrounding cyber practices and material breaches so that investors can make informed investment decisions about a company. "Whether a company loses a factory in a fire – or millions of files in a cybersecurity incident – it may be material to investors," according to SEC Chair Gary Gensler. "Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules will benefit investors, companies, and the markets connecting them."

The SEC is taking a two-track approach. Track one requires public companies to describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. Elements may include:

Whether and how their cybersecurity processes have been integrated into overall risk management processes and systems;

Whether the company engages third parties in connection with their cyber processes; and

Whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party provider[2].

Track two requires that public companies disclose any cybersecurity incident they experience that is determined to be material and describe the material aspects of its nature, scope, and impact. This needs to happen within four business days of determining an incident was material. The rule continues that the materiality determination must be made without undue delay. What makes this even more challenging is that the definition of information systems includes systems "owned or used" by the public company. Thus, it puts information systems hosted or managed by third parties squarely within the regulation's scope. The comments to the regulation make clear that managing third-party risk is a primary concern for the SEC. Connecting these dots means a publicly traded company needs to have a good process to arrive at a materiality determination even in cases where it is a third-party vendor who had the incident. The disclosure hinges on materiality.

What is Materiality Under the SEC Rules?

The SEC cyber rules explicitly state that they wish to use the materiality standard developed under case law. That materiality standard is as follows: information is considered 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 rule further states that public companies need to consider things like data theft, asset loss, intellectual property loss, reputational damage, or business value loss as part of the materiality evaluation. Financial impact will be important for many public companies; however, litigation risk, reduction in competitiveness, reputational harm, or impairment of customer or vendor relationships are also considerations. The question becomes: How does a public company tailor the SEC materiality standard and all these disparate factors into a cohesive documentable process to determine materiality without undue delay? It also needs to be a process that withstands the pressure cooker that is incident response as well as SEC scrutiny done in hindsight. It seems a solution may reside with a long-standing NIST framework – NIST FIPS 199.

What is FIPS 199?

FIPS 199 is the Federal Information Processing Standards publication series of NIST first published in 2004. It was drafted in response to Congress passing the Federal Information Security Management Act of 2002. The purpose of NIST FIPS 199 is to create a framework that federal agencies could use to categorize all information and information systems they maintain with the objective of providing appropriate levels of information security based on the risk level.

This framework is part of the broader risk management framework for information systems used by the federal government in the U.S., and its focus is on the potential impact levels on organizations or individuals should there be a breach of confidentiality, integrity, or availability. Impact levels are categorized as low, moderate, or high.

The main elements evaluated in FIPS 199 are:

1. **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

2. **Integrity:** Guarding against improper information modification or destruction of data and includes ensuring information authenticity.

3. **Availability:** Ensuring timely and reliable access to and use of information.

The standard is applied in the context of three potential impact levels for each element identified above:

4. **Low Impact:** The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

5. **Moderate Impact:** The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

6. **High Impact:** The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

In short, since 2004, FIPS 199 has helped organizations identify their most critical systems and data and ensure that they are adequately protected. In 2023, it can be repurposed to provide a framework public companies can use to document a process to determine whether a cyber incident is or is not material. Why is FIPS 199 a good framework to include in a public company's incident response plan?

Why is FIPS 199 a Good Framework for the SEC Rules?

Just as your algebra teacher wanted you to show your work, a key element to complying with the SEC cyber rules is being able to show how your company arrived at its materiality determination. The NIST FIPS 199 provides a legitimate, respected methodology to show your work when it comes to a materiality analysis. The reason is that NIST is a non-partisan part of the U.S. Department of Commerce that is well respected across the cybersecurity industry. The SEC cyber rules contain language in response to public comments that specifically refer to NIST. The NIST influence is also clearly present in the SEC regulation itself. The regulation defines cybersecurity incidents and threats as either jeopardizing or adversely affecting the "confidentiality, integrity, or availability" of information systems or information contained in them. The confidentiality, integrity, and availability triad as well as the information systems and information contained on them are FIPS 199 concepts. The tangible benefit of using FIPS 199 is it starts the public company down the pathway of a documentable process that supports a materiality determination of a cyber incident. The SEC will be challenged to say FIPS 199 is not a legitimate framework given how much the regulation shares in common with NIST 199 concepts.

NIST FIPS 199 in Action

Cybersecurity incident response means placing a team comprised of the board, the c-suite, legal, forensics, and crisis communications under time pressure with incomplete information that can change hourly. This is a tall task under the best of circumstances, especially if it is a ransomware incident or a threat to disclose exfiltrated information on the dark web. The SEC cyber regulation means that public companies must have in place a methodology to evaluate if the cyber event is or is not a material one. The regulation calls for making this determination without undue delay. That means this analysis is added to the laundry list of activities that take place from investigating the incident and communicating with customers, employees, or the media, to ransom negotiations. That means planning for and executing a documented materiality analysis needs to be in place long before an incident happens.

A fictitious ransomware tale is a good way to look at real-world practical applications for FIPS 199 in a breach context. HealthcareCorp is a publicly traded software development company that uses a third-party privately owned cloud provider to house HealthcareCorp's latest AI software. HealthcareCorp believes the software will revolutionize its industry and has hinted at its coming release in the news and its public filings. One day, HealthcareCorp receives a notification from its third-party cloud provider that the third party has been breached and the threat actor is demanding a ransom or it will release HealthcareCorp's beta code onto the dark web. HealthcareCorp is now in a very unenviable position of having to rely on the third-party cloud vendor for information so that HealthcareCorp can, among other things, decide if this breach is material and must be reported to the SEC.

If HealthcareCorp has adopted NIST FIPS 199 prior to the incident, it can readily evaluate the software code breach in light of confidentiality, integrity, and availability of this particular piece of software. HealthcareCorp can also infuse into this analysis how significant the financial impact might be, as well as the potential to undermine its reputation and competitiveness in the industry. As a best practice, HealthcareCorp should already have various scenarios evaluated for materiality so that, if it encounters an unexpected incident, it can draw on its experience of how it has evaluated other types of incidents. Let's assume HealthcareCorp runs through the analysis and concludes the breach is not material. However, two weeks later, after the determination was made, HealthcareCorp finds out personal information was exfiltrated as part of the incident. As a result, breach notification is required under state law. A consequence of the breach notification is the SEC learns of the incident. While a breach notification does not necessarily mean the breach was material, the SEC may decide to investigate HealthcareCorp's materiality determination.

The prospect of the SEC investigation means that HealthcareCorp must be able to document its materiality process and how it arrived at its conclusion that this incident was not material. Even if the SEC does not agree with HealthcareCorp's conclusion, HealthcareCorp can demonstrate it had a well-considered process to arrive at its determination. Consider how it would look if the response to the SEC were simply that HealthcareCorp deemed the incident not material and HealthcareCorp cannot show its work to support its conclusion. The HealthcareCorp board meeting where management explains that it cannot show its work would not be a pleasant one.

Conclusion

The SEC cyber regulations are the latest milestone in cybersecurity regulation in response to rising costs of data breaches. The coming landscape will require significantly more documentation on how publicly traded companies and their third-party vendors manage cyber risk and respond during a cybersecurity incident. The trigger for the four-day incident response reporting requirements is materiality. The regulations do not define materiality well as specifically applied to cyber events. We believe that NIST FIPS 199 is an excellent framework for public companies to use to document their analysis and determination as to whether a cyber event is material. NIST is well respected in the cyber industry and concepts from FIPS 199 appear directly in key definitions in the new regulations.

Incident response requires a group of people who may have never worked together to make tough business decisions under time pressure with incomplete facts that change rapidly. It will be essential that publicly traded companies have a materiality framework they have practiced since this exercise will now be part of every public company incident response plan. At its core, it means being able to document how the company evaluated one or a series of events that led to a data breach that culminates in a materiality determination. Think of the SEC as your high school trigonometry teacher. When the SEC asks you how you arrived at your materiality conclusion, you do not want to meekly respond that your dog ate your homework.

Justin S. Daniels is a shareholder at the law firm Baker Donelson and author of the best-selling book "Data Reimagined: Building Trust One Byte at a Time." Owen Denby is general counsel for Security Scorecard, Inc., a large managed security services provider.

[1] https://corpgov.law.harvard.edu/2023/08/09/sec-adopts-final-rules-on-cybersecurity-disclosure/

[2] https://corpgov.law.harvard.edu/2023/08/09/sec-adopts-final-rules-on-cybersecurity-disclosure/