ITI Promoting Innovation Worldwide

ITI Follow-Up Response to SEC re: Proposed Cyber Rule

ITI submitted comments responding to the SEC's Proposed Rule on *Cybersecurity Risk Management, Strategy, Governance, and Disclosure* on May 9, 2022. We subsequently met with SEC staff to discuss our perspectives. This document offers additional feedback on the Proposed Rule in follow-up to that conversation. We appreciate the opportunity to continue to engage with the SEC on the Proposed Rule as it is imperative that the SEC continue to consider the potentially significant negative cybersecurity ramifications that could result from the rulemaking if it is not appropriately tailored.

As an initial general point, some ITI members have urged to the SEC to provide additional guidance upon implementation of the rule regarding how to conduct a "materiality" analysis under this new disclosure requirement. Specifically, some ITI members asked for guidance on whether there are new factors to consider when evaluating "any potential material future impacts on registrant's operations and financial condition" in the context of a cybersecurity incident; as well as the other points raised by ITI in section IV of our May 9, 2022 comments.

Law Enforcement Exceptions/Delays

As we referenced in our initial comments, we believe that the Proposed Rule should include safe harbor provisions for law enforcement, national security, and cybersecurity interests. We also noted our concerns that any premature disclosure of vulnerability- or incident-related information would be inconsistent with industry best practices for security and may enable cyber criminals to levy an attack, further undermining the security posture of impacted parties, and the security of the nation and society more broadly.

If the SEC chooses to maintain its approach, we continue to encourage it to allow for a delay in disclosing a cybersecurity incident when there is an active law enforcement investigation underway or when it is in the interest of national security. Language illustrating how to implement such exceptions can be found in state data breach laws, which permit companies to delay data breach notices when law enforcement determines that such notices will impede an investigation. We offered language from California's data breach law as an example in our initial comments. Here, we also offer New York's language as a possible model, which states that "the notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation."[1]

Requiring companies to disclose that an incident has occurred when there is ongoing law enforcement activity could compromise the integrity of such investigations through the public disclosure of sensitive information. For example, law enforcement was involved in investigating and recovering the ransom payment after the Colonial Pipeline ransomware attack. In this instance, a law enforcement delay would have been appropriate had the Department of Justice (DOJ) indicated that publicly disclosing the incident would hamper its investigation and subsequent recovery of the ransom funds that were paid by Colonial Pipeline. To that effect, Colonial Pipeline's Chief Executive

[1] See NY Data Breach language here: https://www.nysenate.gov/legislation/laws/GBS/899-AA

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Officer Joseph Blount testified before Congress that, "I also want to now state publicly that we *quietly and* quickly worked with law enforcement in this matter from the start which may have helped lead to the substantial recovery of funds announced by the DOJ this week." It is possible that if Colonial Pipeline had been required to publicly disclose information regarding the incident prior to the conclusion of DOJ's investigation, it would have hampered the DOJ's ability to investigate and retrieve payment.

As the SEC further hones the rulemaking, we encourage it to work with DOJ and the law enforcement community more broadly to fully understand how public disclosure can jeopardize an investigation and why a provision allowing for delay is a necessary and pragmatic measure.

With regard to cybersecurity equities, if the SEC insists upon maintaining a four-day disclosure window, then a delay should also be permitted to allow for the registrant to undertake appropriate mitigation and remediation activities to triage cybersecurity incidents and contain further potential damage to a registrant's IT systems. Requiring public disclosure of an incident prior to mitigation measures being taken will serve to exacerbate cybersecurity incidents, enabling attackers to exploit such information, and could in fact, aggravate the cybersecurity impacts of the incident – not just for the impacted party but the broader ecosystem. We share more information below on why the rule should take care to avoid such results.

Public Disclosures of Unremediated Vulnerabilities and Cyber Risk Management Practices

Malicious cyber actors are becoming more proficient at and quick to exploit known vulnerabilities. This includes vulnerabilities with available patches due to the length of time some entities take to fully remediate the vulnerable technologies or networks. Indeed, subsequent to the Equifax breach, attackers continued to attempt to exploit the underlying vulnerability that led to the breach.[2] In July 2021, CISA published an Alert on Top Routinely Exploited Vulnerabilities, indicating that malicious cyber actors routinely exploited disclosed vulnerabilities to compromise unpatched systems.[3] This underscores the point that disclosing unremediated incidents or unpatched vulnerabilities can quickly invite other attackers to use that information to exploit other victims. This is why best practices for security and international standards for coordinated vulnerability disclosure, endorsed by Congress and CISA, emphasize that any premature disclosure of vulnerability information is inappropriate, and information should be kept in confidence until the release of the mitigation to the public in order to reduce risk for harm for society and ability of attackers to leverage this information.[4]

Threat actors are adept at penetrating networks and scanning the infrastructure for known vulnerabilities and often use automated tooling to accomplish this. Additionally, an increasing number of attacks now begin with a zero-day exploitation.[5] Therefore, public disclosure of a zero-day by one company can in turn, harm other companies that may be using the same software, as referenced above. Once notified of the vulnerability, any hacker can commence an attack, so if the

[2] https://www.wired.com/story/equifax-breach-no-excuse/
[3] https://www.cisa.gov/uscert/ncas/alerts/aa21-209a
[4] See ISO/IEC 30111, 29147, The IoT Cybersecurity Improvement Act and the Cyber Incident Reporting for Critical Infrastructure Act of 2022 and CISA BOD 20-01.
[5] A zero-day is a computer-software vulnerability, or flaw, that can be exploited before the developer has the opportunity to create a patch to fix the vulnerability.

vulnerability is disclosed prior to remediation, the registrant, as well as others with the same vulnerability, could be subjected to a targeted attack that exploits the same vulnerability.

This is an especially acute concern with sophisticated and well-resourced threat actors, such as those tied to nation states and or other Advanced Persistent Threats (APT), as these threat actors are well-positioned to exploit such vulnerabilities, often leading to cascading and devastating impacts for national security and the entire ecosystem. If a registrant was required to disclose a vulnerability publicly before having a patch, it could serve to facilitate the compromise of a much larger swatch of entities beyond just the registrant. Publicly disclosing an unremediated vulnerability is like publicly announcing that the lock on your back door does not work -- you effectively put burglars on notice and provide them an invitation into your house to take what they want – except that you are also saying that hundreds or thousands of other houses may also be unlocked. Indeed, this sort of approach would stand in direct conflict with globally-recognized standards and security best practices for coordinated vulnerability disclosure, which are followed by the technology ecosystem and governments globally.

Log4j offers a good example of continued exploits of a vulnerability. Exploits started to happen before mitigation was undertaken due to the fact that the unremediated vulnerability was public. See below a timeline of events:

- 2021-11-24 Issue discovered by Chen Zhaojun of the Alibaba Cloud Security Team and reported to the Apache Software Foundation.
- 2021-12-01 Earliest known exploit attempt 2021-12-01 04:36:50 UTC reported by CloudFlare
- 2021-12-06 Log4j released version 2.15.0, which mitigates the known attack vectors at the time
- 2021-12-09 Issue was made public on Twitter
- 2021-12-10 CVE-2021-44228 published, Apache log4j Security Page updated. The world starts patching, and begins to realize the significance of this issue

Public disclosure prior to mitigation may incentivize an attacker to accelerate anti-forensic activity (such as deleting logs to avoid further detection and hamper incident responders) escalate their attack, invite other threat actors to exploit an acknowledged unmitigated vulnerability, or signal the existence of a widespread vulnerability that could impact many other organizations. In many instances, the negative impact of these attacker activities to investors clearly outweighs the positive impact of additional transparency from disclosing an unmitigated incident. The SEC should also consider the impact of disclosure on other parties as well as national security. The registrant is unlikely to have complete information as to how disclosure of such information will impact other parties, given the nature and sensitivity of incident information and the ability of attackers to exploit it. Indeed, the report released by the Cyber Safety Review Board on Log4J emphasized the need to avoid premature disclosure and follow best practices and international standards for coordinated vulnerability disclosure.[6]

[6] CSRB *Review of the December 2021 Log4j Event* available here: https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf

Concerns Regarding the Four-Day Disclosure Window

We went into significant depth with our concerns related to the four-day post-materiality assessment disclosure window in our initial comments. However, we have reiterated several of our concerns here, and also offer some additional thoughts on the issue of appropriate timelines, as well as an example to illustrate some of our concerns.

Although a company may be able to make a materiality determination and subsequently disclose within four business days, in many cases a registrant will not have the information necessary to make a meaningful disclosure that is valuable to investors within that time period. Cybersecurity incidents can take many months to investigate, with forensic analysis producing new information that likely alters factors relevant to the incident's technical and cybersecurity significance and broader business impacts.

An illustrative example of a security incident that when examined in its totality was certainly significant, but when examined on a company-by-company basis would have in some cases been determined as material, and in some cases, not material, involves the SolarWinds breach. The SolarWinds supply chain compromise is considered one of the largest cybersecurity incidents as it involved the compromise of a third-party vendor with access to the networks of its customers. In this case, SolarWinds' Orion software was used by approximately 30,000 organizations to manage their IT networks. The hackers were able to inject a backdoor containing malicious code into a software update that *potentially* exposed any SolarWinds customers who downloaded the Orion software containing the malicious code. It has been reported that roughly 18,000 SolarWinds customers downloaded the malicious updates, with the malware spreading undetected for months to a year or more.[7] Reports indicate that hackers ultimately chose to access fewer than 100 networks.

Two important questions are raised by the SolarWinds hack that are directly relevant to the 4-day disclosure timeline, as well as a point ITI raised in our initial submission regarding the likelihood of vast overreporting under the proposed rule. First, *which* companies "involved" in the SolarWinds breach should have been required to report that they suffered a "material" breach under the SEC's current rule? Second, *when* would it be appropriate for those companies to make such a disclosure?

It makes sense to address the "when" question first. Below is a timeline of t**he SolarWinds hack:**

- **September 2019.** Threat actors gain unauthorized access to SolarWinds network
- **October 2019.** Threat actors test initial code injection for Orion
- **Feb. 20, 2020.** Malicious code known as Sunburst injected into Orion
- **March 26, 2020.** SolarWinds unknowingly starts sending out Orion software updates with hacked code
- **December 2020.** Existence of SolarWinds breach is first detected, by the security company FireEye.

[7] SolarWinds SEC filings available here: https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000162828020017451/swi-20201214.htm

It is noteworthy that FireEye's discovery of the breach occurred approximately 15 months after hackers' initial compromise of SolarWinds. As mentioned above, approximately 100 other entities (government agencies and companies) did in fact discover that hackers had used the Orion backdoor to access their systems. But each of those 100 companies discovered their breaches at different times. As indicated by the above timeline, all 30,000 SolarWinds Orion customers were potentially at risk of being compromised as of September 2019, or at least October 2019. It would have been unreasonable to expect those companies to conduct a materiality assessment and then disclose anything at that point. What about in March 2020, when SolarWinds started sending out Orion software updates with malicious code to its customers? Were those customers "breached" then, and should they have been required to conduct a materiality assessment and disclose? In our view, the answer would be no since they were not aware of the malicious software update at that point. What about in December 2020, when the breach was discovered by FireEye, and was widely reported as one of the "worst ever" in the news shortly thereafter?

The SolarWinds incident helps illustrate why constructing any bright lines around "when" to disclose is counterproductive, including to potentially limit the time afforded a company to make a "materiality" determination in the first place, as some commenters have apparently advocated for and which we strongly advocate against. It also helps illustrate – particularly in the context of a large-scale, widely publicized incident such as SolarWinds– why SEC staff has perhaps sometimes read about a company potentially being victimized by an incident in the news well prior to receiving a disclosure filing from that company, if it ever receives one at all. For instance, there were numerous articles published in the wake of the SolarWinds breach suggesting that hundreds of high-profile companies, as well as government agencies, were potentially victimized by the SolarWinds hack who in fact were not.[8] SolarWinds is a good reminder that newsworthiness is not a reliable indicator of materiality.

The "which" or "who" question is arguably even more important. Which entities should have been required to disclose the SolarWinds hack when ultimately it was found that less than 100 had actually been compromised, and when? It seems obvious SolarWinds should have disclosed as soon as they became aware of the breach, but what about their customers? Should all of SolarWinds' 30,000 Orion software users have disclosed? The 18,000 who downloaded the updates with malicious code? The 100 or so companies whose systems the hackers actually accessed through the maliciously installed backdoors? Or a subset of those companies who determined the breach of their systems was actually "material"?

The answer to "which companies should have been required to disclose" and the series of rhetorical questions posed above of course turns on if and when those companies determined that the SolarWinds breach was "material" to them and their investors. If using SolarWinds as a hypothetical case for application of the Proposed Rule, it is important that the SEC recognize that each company would have likely made such a determination at a different point in time, and also that once they publicly disclosed the fact that they were breached, they would have alerted both the SolarWinds hackers as well as other potential hackers that they had a backdoor installed on their system that could potentially be hacked. Not only would a hundred or more disclosures

[8] See, e.g., Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit, *New York Times*, Dec. 14, 2020. Retrieved at https://www.nytimes.com/2020/12/14/us/politics/russia-hack-nsa-homeland-security-pentagon.html

flooding the EDGAR system not have been helpful to investors, but they would potentially have exposed these companies to further hacks utilizing the information they had just disclosed. SolarWinds provides an instructive example of both why imposing any type of hard timeline for public disclosure is dangerous in terms of potential cybersecurity exposure and can lead to over-notification that would not meaningfully help investors.

As we reference above, it is possible that the company makes a materiality determination at a stage when publicly disclosing the incident could further undermine cybersecurity because the incident has not yet been mitigated or remediated. Please see above, where we discuss the tactics of attackers, and how they can utilize unpatched vulnerabilities to attack a larger swath of companies beyond the immediately impact registrant. As such, there must be exceptions to disclosing unremediated cybersecurity incidents.

With regard to cybersecurity equities, if the SEC insists upon maintaining a four-day disclosure window, then a delay should also be permitted to allow for the registrant to undertake appropriate mitigation and remediation activities to triage cybersecurity incidents and contain further potential damage to a registrant's IT systems. Please also see above, where we discuss this further.

If a timeline must be included in a Proposed Rule, compliance teams within our member companies have indicated that disclosures should be made "without undue delay" rather than including a specific number of days in which a disclosure must be made. This would be more appropriate and feasible.