RAPID7

Comments to the Securities and Exchange Commission

Re: Proposed Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
RIN 3235-AM89

August 29, 2022

Rapid7, Inc. ("Rapid7" or "we") met with staff of the Securities and Exchange Commission (SEC) on August 9, 2022 to discuss our feedback regarding the SEC's proposed rule on Cybersecurity Risk Management, Strategy, Governance, and DIsclosure.[1] These comments reflect the feedback that Rapid7 provided to the SEC during that meeting. We greatly appreciate the SEC's openness to our input and consideration of these comments.

Rapid7 supports many aspects of the proposed rule. Cybersecurity is of growing importance to modern corporate governance, risk assessment, and other key factors that stockholders weigh when making an investment decision. We agree with the SEC that a public company's cyber risk management posture, governance, and incident handling capabilities are appropriate factors that investors and other stakeholders should consider, and believe that the proposed rule advances this principle. *However, Rapid7 has serious concerns about the potential negative ramifications of the public disclosure of uncontained or unmitigated cyber incidents.*

The below comments explain why we believe public disclosure of material cybersecurity incidents prior to containment or mitigation may lead to the mispricing of securities and cause greater harm to investors than a delay in public disclosure. *We also recommend an exception to the proposed rule that would enable a company to delay public disclosure of an uncontained or unmitigated incident if certain conditions are met.* Additionally, we explain why we believe other proposed solutions may not meet the SEC's goals of transparency and avoidance of harm to investors.

Premature public disclosure of cyber incidents puts investors at risk

Although Rapid7 generally supports cyber incident reporting, the SEC's proposed rule is distinguished from nearly all other incident reporting requirements by making the report

[1] Securities and Exchange Commission, Proposed Rule, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 87 Fed. Reg. 16590, Mar. 23, 2022.

publicly available within a short timeframe.[2] Crucially, the SEC's proposed rule makes no distinction between public disclosure of incidents that *are contained or mitigated* and incidents that *are not yet contained or mitigated*.[3] The proposed rule would require publicly traded companies to report cybersecurity incidents on Form 8-K within four days of determining that the incident is material, and the 8-K report would become publicly available via the EDGAR system.[4] When the information is public, it becomes accessible to attackers as well as investors.

Public disclosure of an unmitigated or uncontained cyber incident will likely lead to attacker behaviors that cause additional harm to investors. Cybercriminals often aim to embed themselves in corporate networks without the company knowing in order to steal data over time and steadily gain greater access across networks – sometimes over a period of years. But when an attacker knows it has been discovered, this can lead to reactions that cause additional harm if the attack has not yet been contained or mitigated. Specific risks to investors from premature public disclosure include

- **Escalated attack:** A discovered attacker may forgo stealth and accelerate data theft or extortion activities, causing more harm to the company and its investors. Consider this passage from the MS-ISAC's 2020 Ransomware Guide: "Be sure [to] avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access [or] deploy ransomware widely prior to networks being taken offline."[5]

- **Anti-forensic activity:** A discovered attacker may engage in anti-forensic activity (such as deleting logs), hindering post-incident investigations and intelligence sharing that could prevent future attacks that harm investors. As noted in CISA's Incident Response Playbook: "Some adversaries may actively monitor defensive response measures and shift their methods to evade detection and containment."[6]

---

[2] Rapid7, Cyber Incident Reporting Regulations Summary and Chart, Aug. 26, 2022, https://www.rapid7.com/blog/post/2022/08/26/incident-reporting-regulations-summary-and-chart.
[3] In general, the objective of "containment" activities is to prevent a cyber incident from spreading. Containment is part of "mitigation," which includes actions to reduce the severity of an event or the likelihood of a vulnerability being exploited, though may fall short of full remediation. See CISA, Cybersecurity Incident & Vulnerability Response Playbooks, pg. 14, Nov. 2021, https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.
[4] 87 Fed. Reg. 16595, 16603. Foreign private issuers would file on Form 6-K. 87 Fed. Reg. 16597.
[5] Multi-State Information Sharing & Analysis Center, Ransomware Guide, pg. 11, Sep. 2020, https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf.
[6] CISA, Cybersecurity Incident & Vulnerability Response Playbooks, pg. 14, Nov. 2021, https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

- **Copycat attacks:** Announcing that a company has an incident may cause other attackers to probe the company and discover the vulnerability or attack vector from the original incident. If the incident is not yet mitigated, the copycat attackers can cause further harm to the company and its investors. From the CERT Guide to Coordinated Disclosure: "[M]ere knowledge of a vulnerability's existence in a feature of some product is sufficient for a skillful person to discover it for themselves. Rumor of a vulnerability draws attention from knowledgeable people with vulnerability finding skills[.]"[7]

- **Copycat attacks on other companies:** Public disclosure of an unmitigated cybersecurity incident may alert attackers to a vulnerability that is present in other companies, the exploitation of which can harm investors in those other companies. Publicly disclosing "the nature and scope" of material incidents within four business days risks exposing enough detail of an otherwise unique zero-day vulnerability to encourage rediscovery and reimplementation by other criminal and espionage groups against other organizations.[8] For example, fewer than 100 organizations were actually exploited through the Solarwinds supply chain attack, but up to 18,000 organizations were at risk.[9]

Premature public disclosure of cyber incidents may misprice securities

Several aspects of the SEC's proposed rule are intended to help investors assess a registrant company's cybersecurity risk management posture and capabilities, which Rapid7 generally supports.[10] If a registrant company has a mature cybersecurity program, it may aim to adhere to best practices for cyber incident response. Established cyber incident response protocol is to avoid tipping off an attacker until the incident is contained and the risk of further damage has been mitigated, for the reasons described in the previous section.[11] See, for example,

---

[7] CERT, Guide to Coordinated Vulnerability Disclosure, 5.7 Disclosure Timing, Sep. 16, 2019, https://vuls.cert.org/confluence/display/CVD/5.7+Disclosure+Timing#id-5.7DisclosureTiming-ReleasingPartialInformationCanHelpAdversaries.

[8] The time to exploitation, the time between when vulnerabilities become known and when they are exploited "in the wild," has shrunk drastically year over year. Rapid7, 2021 Vulnerability Intelligence Report, pg. 10, Mar. 28, 2022, https://information.rapid7.com/rs/411-NAK-970/images/Rapid7%202021%20Vulnerability%20Intelligence%20Report.pdf.

[9] Solarwinds Corp., 8-K Current Report, 001-38711, May 7, 2021, https://www.sec.gov/ix?doc=/Archives/edgar/data/1739942/000173994221000076/swi-20210507.htm.

[10] See Subsection D. Disclosure of a Registrant's Risk Management, Strategy and Governance Regarding Cybersecurity Risks, 87 Fed. Reg.16599.

[11] For similar reasons, it is commonly the goal of coordinated vulnerability disclosure practices to avoid, when possible, public disclosure of a vulnerability until the vulnerability has been mitigated. See, for example, the CERT Guide to Coordinated Disclosure, 5.7 Disclosure Timing, Sep. 16, 2019, https://vuls.cert.org/confluence/display/CVD/5.7+Disclosure+Timing#id-5.7DisclosureTiming-ReleasingPartialInformationCanHelpAdversaries.

CISA's Incident Response Playbook,[12] as well as NIST's Computer Security Incident Handling Guide.[13] If the registrant were able to follow best practices and ensure containment or mitigation before public disclosure, it may prevent some of the additional harms that would arise from premature public disclosure.

However, if the SEC's proposed cyber rule requires public disclosure of uncontained or unmitigated cyber incidents, this could distort the price of securities. While adherence to cybersecurity best practices should be a positive influence on investors' assessment of the appropriate value of the company's securities, the proposed rule would require companies to contradict best practices in some instances. By contradicting best practices for cyber incident response and inviting new attacks, the premature public disclosure of an uncontained or unmitigated incident may provide investors with an inaccurate measure of the registrant company's true ability to respond to cybersecurity incidents. Moreover, a premature disclosure during an early stage of the incident response process may result in investors receiving inaccurate information about the scope or impact of the incident.

Proposed solution: A exception providing a delay in limited circumstances

Rapid7 encourages the SEC to consider an alternative approach that achieves the SEC's ultimate goal of investor protection by requiring timely disclosure of cyber incidents and simultaneously avoiding the unnecessary additional harm to investors that may result with premature disclosure.

Specifically, we suggest that the proposed rule remains largely the same— i.e., the SEC continues to require that companies determine whether the incident is material as soon as practicable after discovery of the cyber incident, and file a report on Form 8-K four days after the materiality determination under normal circumstances. However, we suggest that the rule be revised to also provide companies with a temporary exemption from public disclosure if each of the below conditions are met:

- The incident is not yet contained or otherwise mitigated to prevent additional harm to the company and its investors;
- The company reasonably believes that public disclosure of the uncontained or unmitigated incident may cause substantial additional harm to the company, its investors, or other public companies or their investors;

[12] CISA, Cybersecurity Incident & Vulnerability Response Playbooks, pgs. 9 and 14, Nov. 2021, https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.
[13] NIST SP 800-61, Computer Security Incident Handling Guide, 2.3.4 Sharing Information With Outside Parties, pg. 9, Aug. 2012, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

- The company reasonably believes the incident can be contained or mitigated in a timely manner; *and*
- The company is actively engaged in containing or mitigating the incident in a timely manner.

The determination of the applicability of the aforementioned exception may be made simultaneously to the determination of materiality. If such determination is made, the company may delay public disclosure until such time that any of the conditions are no longer occurring, at which point, they must publicly disclose the cyber incident via Form 8-K, no later than four days after the date on which the exemption is no longer applicable. The 8-K disclosure could note that, prior to filing the 8-K, the company relied on the exemption from disclosure. Existing insider trading restrictions would continue to apply during the public disclosure delay.

If an open-ended delay in public disclosure for containment or mitigation is unacceptable to the SEC, then we suggest that the exemption only be available for 30 days after the determination of materiality. In Rapid7's experience, the vast majority of incidents can be contained and mitigated within that time frame. However, cybersecurity incidents can vary greatly, and there may nonetheless be rare outliers where the mitigation process exceeds 30 days.

Drawbacks of other solutions

There are drawbacks to other solutions being floated to address the risks of premature public disclosure of unmitigated or uncontained cyber incidents. Some of these solutions do not align with the purpose of the SEC rule, while others don't adequately address the risks of premature public disclosure. For example:

- **AG delay:** The SEC's proposed rule considers allowing a delay in reporting the incident when the Attorney General (AG) determines the delay is in the interest of national security.[14] Rapid7 supports integrating this delay into the final rule, but it is insufficient on its own. This AG delay would apply to a very small fraction of major cyber incidents and not prevent the potential harms described above in the vast majority of cases.

- **Law enforcement delay:** The SEC's proposed rule considers, and then rejects, a delay when incident reporting would hinder a law enforcement investigation.[15] Rapid7 supports integrating this delay into the final rule as well, to ensure law enforcement can help prevent future cyber incidents that would harm investors. However, it is unclear if

[14] 87 Fed. Reg. 16598.
[15] 87 Fed. Reg. 16596.

this delay would be triggered in many cases. First, the SEC's proposed timeframe (four days after concluding the incident is material) poses a tight turnaround for law enforcement to start a new investigation or add to an existing investigation, determine how disclosure might impact the investigation, and then request delay from the SEC. Second, law enforcement agencies already have investigations opened against many cybercriminal groups, and so public disclosure of another incident may not make a significant difference in the investigation. Although a law enforcement delay would be used more than the AG delay, we still anticipate it would apply to only a fraction of incidents.

- **Vague disclosures:** Another potential solution is to continue to require public companies to disclose unmitigated cyber incidents on the proposed timeline, but to allow the disclosures to be so vague that it is unclear whether the incident has been mitigated. Yet an attacker embedded in a company network is unlikely to be fooled by a vague incident report from the same company, and even a vague report could encourage new attackers to try to get a foothold in. In addition, very vague disclosures are unlikely to be useful for investor decision-making.

- **Materiality after mitigation:** Another potential solution is to require a materiality determination only after the incident has been mitigated. However, this risks unnecessary delays in mitigation to avoid triggering the deadline for disclosure, even for incidents that could be mitigated within the SEC's proposed timeline. Although containment or mitigation of an incident is important prior to public disclosure of the incident, completion of mitigation is not necessarily a prerequisite to determining the seriousness of an incident.

* * *

The SEC has long been among the most forward-looking regulators on cybersecurity issues. We applaud the SEC's acknowledgement of the significance of cybersecurity to corporate management, and for taking the time to listen to feedback from the community. Rapid7's feedback is that we agree on the usefulness of disclosure of material cybersecurity incidents, but we encourage the SEC to ensure its public reporting requirement avoids undermining its own goals, harming investors, and providing more opportunities for attackers.

We appreciate the opportunity to share our views. If there are additional questions or if Rapid7 can provide any further assistance, please contact Harley Geiger, Senior Director for Public Policy, at [redacted]. Thank you.