‘Cyclops Blink’ Shows Why the SEC’s Proposed Cybersecurity Disclosure Rule Could Undermine the Nation’s Cybersecurity

By **Sasha Hondagneu-Messner**, **Steve McInerney**, **Alan Charles Raul**

Tuesday, August 30, 2022, 8:01 AM

**This article was originally published in Lawfare. Link to original article here.*

On March 9, the Securities and Exchange Commission (SEC) proposed a new rule intended to enhance and standardize disclosure requirements for cybersecurity risks. Among other things, the rule requires all publicly traded companies to report all “material” cybersecurity incidents within four business days of determining the event’s materiality. But shockingly, this notice requirement does *not* include an exception for active investigations by law enforcement, coordination with intelligence and national security agencies, or compliance with court orders that may restrict the timing of permissible cybersecurity disclosures—nor does it provide an exception where premature disclosure of an incident could cause significant damage to other vulnerable businesses or government entities. In theory, this could mean that a company would be required to disclose a breach before the vulnerability could even be patched.

The SEC has not thought through this proposed rule carefully enough. Finalizing the proposal in its current form would seriously disrupt the government’s essential partnership with the private sector—involving close coordination and confidentiality—to combat significant cyberattacks. Indeed, on July 19, Deputy Attorney General Lisa Monaco stated in a major address to a cybersecurity conference that, “[b]y working closely with … the manufacturer of the network devices targeted by the malware, … we were able to prevent that next cyber-attack” and “disable[] the GRU’s control over those devices before they could be used to initiate an attack—an attack against Ukraine, against us, against our allies.” U.S. cybersecurity agencies and the Biden administration alike recognize the strategic necessity of working closely with private companies to bolster the nation’s and world’s cyber defense. The SEC should not undermine this cooperation.

Remarkably, the SEC’s new disclosure requirement would not allow for delaying public disclosure during an active law enforcement investigation *even though* it recognizes that requiring immediate notification from a company could hinder its response. The SEC itself acknowledges that its new four-business-day disclosure mandate could enable “[m]alicious actors … [to] engage in further attacks based on the information, … thereby potentially exacerbating the ongoing attack.” The agency further conceded “that a delay in reporting may facilitate law enforcement investigations aimed at apprehending the perpetrators of the cybersecurity incident and preventing future cybersecurity incidents.” Nonetheless, the SEC apparently concluded that actual cybersecurity was secondary to informing investors about an ongoing incident—a confounding conclusion that directly threatens cybersecurity throughout the country. The proposal further fails to allow delayed publicity to permit coordination with national security agencies, or even compliance with court orders that prohibit any disclosure.

Therefore, by its own lights, the SEC’s proposed disclosure rule could advantage “malicious actors” and disadvantage “law enforcement investigations.” And for this trade-off, the agency presents little justification: The SEC provides absolutely no countervailing evidence that public companies have a track record of underreporting material cyberattacks. To the contrary, the SEC has brought hardly any enforcement actions against public companies for failing to disclose material incidents. While the SEC’s proposal expressly disclaims any intent to change the standard for materiality in the cybersecurity context, some of the examples it cites are so routine that companies will feel pressure to dumb down materiality, or risk agency enforcement. Given these realities, the misplaced priorities of the SEC’s new cyber proposal could significantly undermine law enforcement and national security interests, and risk harming vulnerable businesses or entities exposed to an “exacerbat[ed] … ongoing attack.”

Just a month after the SEC announced its proposal, a clear example of the value of public-private cooperation emerged. On April 6, FBI Director Christopher Wray—standing beside Attorney General Merrick Garland and Deputy Attorney General Lisa Monaco—announced the successful disruption of a global botnet known as Cyclops Blink. The botnet was created by Sandworm, an elite and aggressive hacking team within the GRU,

Russia's military intelligence agency. Wray repeatedly and directly attributed the success of the disruption to close coordination between the government and a company that had been infected by the malware: "Our partnership with the private sector was key here. [The company] enthusiastically cooperated with the FBI to figure out the source of the infection and to counter it," Wray stated. "That kind of cooperation makes successes like the one we're announcing today possible, and it will continue to be important going forward." Garland added, "Fortunately, we were able to disrupt this botnet before it could be used."

This type of partnership is the future of cyber defense in the United States and around the world. The partnership touted by government leaders after Cyclops Blink is not an anomaly. Other key government leaders have echoed the same theme recently:

- President Biden has stressed the importance of "public-private partnerships and initiatives to enhance cybersecurity."
- In February 2021, Deputy National Security Adviser for Cyber and Emerging Technology Anne Neuberger emphasized that "partnership has to be a core part of national cyber defense."
- In October 2021, National Cyber Director Chris Inglis, FBI Deputy Director Paul Abbate, Cybersecurity and Infrastructure Agency (CISA) Director Jen Easterly, NSA Director of Cyber Security Rob Joyce, and Berkshire Hathaway Energy CEO William J. Fehrman discussed the importance of public-private partnership on a panel moderated by the McCrary Institute.

Not Your Grandfather's Cyberattacks: Rising Number of Nation-State-Sponsored Attacks and the Importance of Public-Private Partnership

Data breaches used to consist primarily of hackers breaking into computer systems to steal personal identifiable information, followed by the affected company sending individuals notification letters and offering a year or two of complimentary credit monitoring. Those breaches have been bad. But the level of danger presented by new attacks has ratcheted the risk way up.

You do not need to be steeped in cyber law and incident response work to know that nation-state-sponsored attacks are on the rise—in terms of both quantity and sophistication—along with the dedication of a significant degree of new federal resources to combat these threats. Just this year, the U.S. government has made numerous front-page headlines in this space:

- On Jan. 19, President Biden signed a National Security Memorandum, which implemented requirements from Executive Order 14028 ("Improving the Nation's Cybersecurity") by setting out specific cyber requirements for government agencies and contractors, such as multifactor authentication, encryption, cloud technologies, and endpoint detection services.
- In March, Congress passed and President Biden signed the Strengthening American Cybersecurity Act, which would require critical infrastructure entities to report cyber incidents within 72 hours and ransomware payments within 24 hours to CISA.
- CISA issues continuous updates through Shields Up, and on April 7, CISA issued "Guidance on Sharing Cyber Incident Information" to provide its "stakeholders with clear guidance and information about what to share, who should share, and how to share information about unusual cyber incidents or activity."

Embedded in all of these actions by the U.S. government is the continued emphasis on the critical role of public-private collaboration to defend against serious cyberattacks. The expert agencies also understand that cyber-attacked companies are victims in their own right. As CISA Director Jen Easterly has colorfully noted, "[W]e don't stab the wounded."

Indeed, Easterly recently described CISA as a "coequal partner" with the private sector in securing U.S. infrastructure. She emphasized that the agency's aim is to rally the community to remediate cyber vulnerabilities, for example, noting CISA's vulnerability scoring system and exploited vulnerability advisories as useful guides. Unlike the SEC's proposed rule, agencies that request information on security incidents, such as CISA

and the FBI, have stressed that they do not share breach report data with regulatory agencies such as the Federal Trade Commission or the SEC.

Collaboration with the U.S. government has proved essential to provide effective assistance to companies in remediating and disrupting cyberattacks. In addition to the Cyclops Blink example, the U.S. government makes a point of promoting cooperation by showcasing the contribution of companies that provide valuable assistance, such as in the cases here and here.

As SEC Chair Gary Gensler explained earlier this year, "Other government entities, such as the Federal Bureau of Investigation and CISA, captain Team Cyber, but the SEC has a role to play as well." Gensler described a broad cybersecurity function for his agency, including the proposal discussed above. While conceding cyber captaincy to other government agencies, Gensler explained the SEC's role by discussing other SEC cybersecurity initiatives. For example, in February, the SEC proposed cybersecurity risk management and reporting rules for investment advisers registered with the SEC, and in May 2022, the SEC announced that it had nearly doubled the size of its Crypto Assets and Cyber Unit. SEC rules to come will likely also include enhanced data security and breach notification requirements for the personal financial information of investors held by securities firms.

But the factual predicate for the SEC's March public company proposal, underreporting of material cyber incidents to investors, is merely presumed rather than substantiated by the SEC. Indeed, the agency has long provided guidance to public companies, including in 2018, when the SEC published a "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," which discussed and explained in detail the array of factors that may affect whether an incident should be disclosed to investors with respect to cybersecurity. In other words, the new, mandatory four-day reporting trigger, with no deference to the "captains" of Team Cyber, as Gensler put it, is neither necessary nor wise.

As explained in this post, the pending proposal is a step backward for U.S. cyber defense. Indeed, regulator and individual notification (where personal data has been compromised) is a critical component of proper incident response. However, the timing of such notification should not come at the cost of public-private coordination with government agencies focused on protecting the nation's information technology infrastructure, the national economy, and national security. Notification to—and close coordination with—law enforcement is key for companies responding to sophisticated nation-state-sponsored attacks. The explicit lack of a law enforcement (and national security and cybersecurity agency) exemption in the SEC's proposal will undermine critical national, corporate, economic, and personal security interests.

The Proposed Rule, While Well Intended, Will Hinder Public-Private Collaboration and Undermine "Responsible Disclosure"

There is a time and a place for everything, including disclosure to shareholders, but the current proposed rule threatens to put the nation's cyber defense at risk. Not only does the proposal omit deference to the captains of Team Cyber, but it also fails to make any accommodation for courts. Such accommodation, however, is of critical importance: In Cyclops Blink, the government obtained court orders dictating confidentiality until official authorization was granted—and the takedown of Russia's malicious botnet could be effectuated. It was only after close collaboration and cooperation with the Justice Department and FBI that the relevant company could publicly disclose the incident and remediation methods.

And if law enforcement, national security, and judicial requirements were not enough to prompt reconsideration of the SEC's proposal, the long-standing doctrine in the software development community known as "responsible disclosure" should be. Responsible disclosure requires software developers and ethical hackers to publicly disclose newly discovered, or "zero-day," vulnerabilities only *after* a patch or remediation is developed. The underlying concept being, if a zero-day vulnerability is publicly disclosed *without* a patch or remediation, then copycat attackers could use knowledge of the vulnerability to initiate new attacks.

The reasons for this approach are obvious. Defects are inevitable, defects can lead to vulnerabilities, and known vulnerabilities can be exploited. Determining whether a vulnerability can be exploited requires developing a proof of concept for a successful attack, and closing exploitable vulnerabilities by fixing defects or other countermeasures can take time.

It is not at all far-fetched to think of a scenario in which the SEC's proposed disclosure obligations would come in conflict with this doctrine. For example, if a company discovers it has been impacted by a zero-day vulnerability in widely used software, the company may be required by the SEC to report it publicly before the company has had sufficient time to put in place a patch or other remedial measures. Accordingly, other companies will be caught exposed, while malicious actors are able to exploit—or exacerbate—the vulnerability across multiple companies. Premature disclosure may, moreover, conflict with CISA's Coordinated Vulnerability Disclosure Process, which calls for "CISA, the affected vendor(s) and/or service provider(s), … all [to] disclose simultaneously."

Balancing Cybersecurity Disclosures and Cybersecurity Effectiveness

As nation-state actors increase their malicious cyber capabilities toward companies, U.S. regulators such as the SEC have understandably increased their regulatory focus on cybersecurity. The SEC is of course a well-intended member of Team Cyber, and investors in public companies might benefit from some aspects of the SEC's proposal: Increased knowledge of a company's cybersecurity risks, experience, governance, and resiliency could be important to their decision-making. But the proposal is dangerous to the extent that it jeopardizes important safety, security, and geopolitical interests in the name of disclosure. Put simply, the SEC's proposal must be revised to assure responsible (not reckless) public disclosure. The SEC should not force public companies to choose between SEC liability and effective collaboration with the government's cybersecurity-focused agencies. As is, the proposed rule could increase the risk to the U.S.'s critical infrastructure, economy, homeland, and allies. The proposal should include deference for exigent law enforcement, national security, and judicial needs, and allow delay where appropriate for ongoing, unpatched incidents when premature disclosure could harm a broad swath of vulnerable companies and even government agencies.

***

The authors represented the company involved in collaborating with the Justice Department, the FBI, the Cybersecurity and Infrastructure Security Agency, the U.K. National Cybersecurity Centre, and others on Cyclops Blink. They also assisted in the preparation of comments submitted to the Securities and Exchange Commission regarding the proposed rule discussed in the post *on behalf of various clients.*