BANK POLICY INSTITUTE

Fool's Gold: Why the Exceptions to the SEC's Cyber Disclosure Rule Cannot and Will Not Work, and the Damage that Will Ensue

Heather Hogsett | Dec. 18, 2023

Cyber attacks are one of the top risks on investors' and executives' minds, but the way they are treated under a new SEC regulation would empower hackers and blunt companies' defenses.

Under current law, a cyber event is treated like any other event; firms file a Form 8-K if they determine that a reasonable investor would want to know of it, with a vast superstructure of regulations and enforcement to ensure they do. This system works because it balances investors' desire for information and maximizes a firm's ability to defend against hackers, while providing the least information to the rogue nation-states and criminals attempting to gain access.

A recent rule adopted by the SEC upends that precedent. The rule going into effect Dec. 18 requires disclosure within four business days of determining that a cyber event is material, requiring that firms describe the nature, scope and timing of the incident as well as its likely effects. Innumerable issuers and others objected to both the proposed and final rule on the grounds that, in some cases, disclosure would do serious harm to the firm – something a reasonable investor would certainly not want. Most importantly, it means divulging to attackers around the globe how the firm has been affected and how it is responding, giving hackers valuable information to help plan their next attack. It also means the company's first responders will be diverted from fighting the attack to, instead, working on securities disclosures.

Why the delay exception won't work

There is an exception in the rule to delay disclosure of an attack, but that exception is not viable because of the mismatch between a rapid timeline for pursuing it and the need for complex details to inform it.

The SEC's answer in the final rule is a process by which the Attorney General may authorize a delay of up to 30 days, and subsequent extensions up to a maximum of 120 days, if he or she determines that a disclosure would pose a risk to national security or public safety. There is only one thing to understand about this process: *virtually no company will be able to avail themselves of this disclosure delay.*

We have now seen how one link in a long and confusing chain of events will look, as the FBI has issued guidance[1] on how it will be forced to rapidly process delay requests; this process is practically unusable.

Under the guidance, a victim company must immediately alert the FBI when it determines an event is material and file a request including a variety of details, some of which may not be available, accurate or clear in the early phase of a response (e.g., the type of incident, intrusion vectors, data that were affected and how). Within two hours the

[1] https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements-request-a-delay

FBI must (1) confirm the company is eligible to make the request and (2) ask other federal agencies for their input on whether a disclosure would have an adverse effect on national security or public safety.

If the event involved a financial institution, the Treasury Department would be asked to opine and would then have 12 hours to conduct an assessment and provide it to the FBI. Considering the diversity in size and business model across the financial industry, it would likely be difficult for Treasury to have a well-informed view of the downstream effects disclosure might have and certainly not plausible within such a short timeframe. Providing meaningful input and analysis would seem to require Treasury have a 24/7 watch floor or similar round-the-clock staffing and an escalation procedure. It currently does not; neither do other federal agencies that might be called upon for input.

Why don't they? And why won't they? Because no rational government could be expected to deal with a request for an exception from the securities laws on the same timeline as a responding to an earthquake.

Following the FBI's 30 hours of fact gathering and analysis, the referral is then passed to the Department of Justice to make a final determination. DOJ's own guidance[2] outlines the limited circumstances under which it may issue a delay.

The problems with the exception are not just procedural but involve human nature. For example, how comfortable are national security officials going to feel about overriding an SEC disclosure rule on short timelines with limited information? And if they ever do grant an exemption, they can look forward to testifying before Congress or in court about why they allowed investors to be kept in the dark, after which, it's safe to say any request for a delay would likely be denied.

Confirming all of the above, it was reported[3] last week that senior officials from the Department of Justice, FBI and CISA put together a call with reporters with the express intention of saying that exceptions are unlikely to be granted under the rule. Regulators don't generally hold press conferences to say that exceptions to the rules they are about to adopt are dead letters. That said, the regulator here is the SEC, which did not join the press call, so perhaps this is a sign that there is a bit of a disconnect.

Preserving progress

At a time of rising geopolitical tensions when cyberattacks can be used to influence public sentiment and government action, we should be continuing to build upon the work of the last decade to establish trust and drive meaningful partnerships between the private and public sectors through confidential reporting. CISA, the FBI, Treasury and the prudential banking regulators have made great strides in building information sharing and collaborative efforts with industry to bolster national cybersecurity.

With the passage of the Cyber Incident Reporting for Critical Infrastructure Act, Congress reaffirmed the central role of CISA in helping defend the nation against cyber threats by confidentially collecting incident information and using it to help protect others. Rather than competing with these efforts and limiting their effectiveness, the SEC should have considered how other national policy goals can and will help the interests of investors far more than requiring the premature public disclosure of an ongoing attack.

Meanwhile, the new requirements further complicate an already challenging response to cyber incidents and increase risks for other companies. Putting sensitive information into the hands of hostile nations and criminal hackers makes their job easier. We already saw a threat actor report its own ransomware victim to the SEC for failure to disclose, becoming yet another method for extortion.

[2] https://www.justice.gov/media/1328226/dl?inline
[3] https://subscriber.politicopro.com/article/2023/12/officials-tamp-down-expectations-for-carve-outs-under-new-sec-rule-00131662?source=email

Congress will soon consider whether the rule should be invalidated under the Congressional Review Act. It should do so. Failing that action, or a Presidential veto, it will be left to a future SEC or Congress to rescind the rule. If foresight fails, perhaps hindsight will succeed.

_____

Disclaimer: The views expressed do not necessarily reflect those of the Bank Policy Institute's member banks, and are not intended to be, and should not be construed as, legal advice of any kind.