Analysis: SEC Cybersecurity Proposals and Biden's National Cybersecurity Strategy

President Biden's National Cybersecurity Strategy was announced on March 1, 2023. 'Harmonized regulations' is a key component of this strategy. The Strategy is, however, a wish list rather than a directive. On March 15, the SEC resurrected its own cybersecurity proposals.

These two events are likely connected. A federal data protection and privacy law is an almost impossible task in partisan times, but harmonized regulations across the sectors under the aegis of the federal administration will effectively combine into a nationwide cybersecurity regulation.

Consider, for example, the FTC's recent privacy actions against BetterHelp (March 2023) and GoodRX (February 2023). Both companies can be described as healthcare firms that fall outside of HIPAA requirements. If you combine the FTC requirements and the SEC's proposal, you begin to the beginning of a federal cybersecurity strategy in action.

On March 15, 2023, the SEC announced a proposal for new cybersecurity requirements for covered entities. Specifically, it announced, "New public disclosure requirements for Covered Entities would improve transparency about the cybersecurity risks that can cause adverse impacts to the U.S. securities markets."

Disclosure requirements are critical for any set of regulations. Third party auditing is expensive, resource consuming and not often required by regulations – but this means that ensuring conformance is difficult. Required breach

disclosure can go a long way toward solving this. Since breaches will happen, and will eventually become known and trigger an investigation, requiring immediate disclosure will both enable user victims to take immediate action to safeguard themselves, and force the covered entities into being able to prove conformance with the regulations when investigated.

The best way to do that is continuous and rigorous adherence to the regulations.



Tom Kellermann

But like all regulations, the SEC cybersecurity proposals are receiving a mixed reception in the market. Tom Kellermann, SVP of cyber strategy at Contrast Security, simply told *SecurityWeek*, "While I applaud the long-awaited guidance, it doesn't go far enough. The cybersecurity requirements should align with a given standard like NIST 800-53 or the FFIEC and reporting should be required for intrusions and or cyberattacks that result in the manipulation or destruction of data."

It is a common concern that business is already overwhelmed by national, international and state-level regulations: we could add GDPR, California's CCPA and the New York DFS 23 NYCRR 500 to the list. The argument is that new regulations should align with (or instead require) existing regulations to not increase the existing and overwhelming spaghetti soup of regulatory

requirements.

Jonathan Reiber, VP of cybersecurity strategy and policy at AttackIQ, doesn't see it this way. "This is a much stronger regulation than just the New York financial one and the California one. It's a national level breach reporting law. Companies are going to have to deconflict a little bit with the states – but one of the benefits of this rule is that it sets requirements at a national level which will supersede those other states. It should make it a little bit easier to do business."



Jonathan Reiber

He believes it is on the SEC to align its proposals with existing regulations, but it will help national financial firms do a much better job of incident reporting. "The reason I like it," he continued, "is that it will force financial firms to prepare their defenses and their teams for likely incidents. I like to call that a threat informed defense strategy. And that means thinking about the adversary and exercising controls against the adversary."

Like Kellermann, Jeff Williams, CTO and co-founder at Contrast Security, also has concerns over the SEC proposals. "While it's nice to see the SEC being active about cybersecurity risks, this rule simply captures very basic cyber hygiene," he told *SecurityWeek*. "Historically, the SEC has focused on 'incidents', and it's nice to see them expanding to cover vulnerabilities as well. Still, I can't see how this will make a significant change in covered entities, all of which already

have a risk management program of some sort."

He points to the amount of risk already being carried by the covered entities. "Untriaged and unfixed vulnerabilities often number in the hundreds of thousands. Software is pushed to production without security testing. And systems containing components with known vulnerabilities are rampant. People – and Congress – were outraged when Equifax took months to fix a vulnerable Struts software framework and got breached in the meantime. What they don't know is that every covered entity is in this exact same situation right now."

Williams believes the SEC could do more. "They could require disclosure of the security defenses and assurance for each system. They could more directly require specific security outcomes."

It seems to be a hugely different viewpoint to that of Reiber – but in effect, there is little difference. Williams wants more explicit regulation of cybersecurity controls, while Reiber believes this is already implicit through the breach disclosure rule. The likelihood of a breach (and subsequent investigation) will force the covered entities to have adequate security controls in place or be found in breach of the regulation.

The real problem, and one faced by all organizations in all sectors, is how to have effective and provably effective security controls in place.

Reiber believes that developments over the last few years can provide the answer: MITRE and CISA's Known Exploited Vulnerabilities Catalog (the KEV list). If – and not just covered entities but all – organizations use MITRE to test each newly CISA-disclosed vulnerability against their security defenses, and can successfully defend against those vulnerabilities, they can adequately prove a serious cybersecurity posture even if they are subsequently breached.

This has the advantage of ensuring security without imposing specified controls. If a MITRE attack definition defeats defenses, there is an obvious necessity to improve or tweak the existing posture. If existing defenses can defeat the KEV list, there is not only less likelihood of being breached, but also a solid argument demonstrating that requirements have been followed even if there is a breach.

The key to this, and perhaps the key element of the SEC cybersecurity proposals (and perhaps all cybersecurity regulations) is the breach disclosure rule.

Related: Investors Pour $200 Million Into Compliance Automation Startup Drata

Related: Do Privacy and Data Protection Regulations Create as Many Problems as They Solve?

Related: Cyber Insights 2023 | Regulations

Related: Mapping Threat Intelligence to the NIST Compliance Framework Part 2

https://www.securityweek.com/analysis-sec-cybersecurity-proposals-and-bidens-national-cybersecurity-strategy/