DARKREADING

APPLICATION SECURITY

Do CISOs Have to Report Security Flaws to the SEC?

The new SEC rules make it seem that there is no need to report the presence of security vulnerabilities, but that doesn't quite tell the full story.

Evan Schuman, Contributing Writer, Dark Reading
September 22, 2023

4 Min Read

SOURCE: BAONA VIA ISTOCK

Now that the SEC wants to know about any material security incidents within four days of determination, CISOs must determine what constitutes a material security incident — which goes far beyond a mere data breach.

One thorny element revolves around security vulnerabilities, regardless of whether they were discovered internally or reported by an external source. Security leaders need to ask: What could happen if attackers discover and use that flaw? How damaging would that be? Those answers could help security leaders figure out whether the security flaw should be reported to the SEC.

The final text of the SEC rule describes a cybersecurity threat as "any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."

But the focus is on the process — not an individual vulnerability. As such, maybe security vulnerabilities don't have to be reported under the new SEC rule? If a security flaw has been fixed, then there is no ongoing risk. And if a security flaw has not yet been fixed, the SEC has carved out an exception in reporting if it would weaken the company's cybersecurity posture.

It can't be that straightforward because cybersecurity compliance is rarely that simple.

"When I think about materiality, I consider the outcome of a breach that would exploit the vulnerability, rather than direct attributes of the vulnerability itself," says Andy Ellis, operating partner at YL Ventures, who also served as the CISO at Akamai for 25 years. "If a breach using this vulnerability would be disastrous, I think that drives materiality."

It is less about the vulnerability and more about the company's risk management process and procedures, he adds.

"Are you actually doing coherent risk management? The [security] hole in a vacuum doesn't really matter. The SEC missed an opportunity. If you are doing good risk management, then you are fixing problems. They *should* have required that companies disclose risk management metrics," Ellis says. "How many holes were patched? How did you detect those risks and reduce them?"

A Reasonable Timeline for Disclosure and Fixes

Weaknesses that CISOs don't know about exist everywhere, says Nick Vigier, who was the CISO at Talend until September when he left to launch his own cybersecurity consulting business called Rising Tide Security.

"There are always gaps and potential issues, and it's impossible to enumerate every potential issue," he says. "Some [attacks using security holes] are extraordinarily unlikely."

"The difficulty of actual remediation often overtakes what the policy says. It is a very very slippery slope," adds Justin Greis, a McKinsey partner leading cybersecurity work in North America within the Risk & Resilience Practice. "What if the repair requires tens of thousands of servers patched and it can't be done with automation? It may not be a push-button patching."

Enterprise security leaders need to start with a strict process for evaluating security vulnerabilities and creating a priority list of repairs that factors in both security and business needs. A common target is for critical security flaws to be resolved within seven days, high-vulnerability ones within two weeks, and low-severity within 30 days, Greis says.

"When enterprises have such poor cybersecurity hygiene that they leave holes open too long, those are problems waiting to happen," he says. "Put in a policy about how quickly those things *need* to be fixed."

Cloud environments also add complexities because the enterprise needs to rely on the cloud vendor to do some of the repairs.

Ellis says that when he was CISO at Akamai, "we had some vulnerabilities that took years to resolve because all customers had to deploy the fix first."

Monday Morning Quarterback

If an attacker leverages a security vulnerability and executes a successful attack, and the enterprise reports that data breach to the SEC as a material security incident, it can lead to shareholder frustration and even lawsuits. But without the resources to fix every vulnerability immediately, the CISO is placed in an impossible predicament.

"Identifying and not immediately fixing a vulnerability is a risk-based process. There is nothing in the SEC rules that says that companies have to have zero risk," says Mark Rasch, an attorney specializing in cybersecurity enforcement who used to head the U.S. Justice Department's unit handling high-tech crimes.

The CISO must consider the nature of the vulnerability itself, Rasch adds.

"Are there exploits that we know of? What is the likelihood of an exploit being developed? What is the skillset necessary to create an exploit? Are we talking script kiddies or nation state?" he asks "What is the likelihood of harm? Are there acceptable compensating controls? What costs are involved? We're not just money but also business interruptions and process interruptions. Then there is calculating the likely cost of mitigation."

About the Author

Evan Schuman

Contributing Writer, Dark Reading

Evan Schuman has tracked cybersecurity issues for enterprise B2B audiences for far longer than he will admit. His byline has appeared in The New York Times, Associated Press, Reuters, SCMagazine/SCMedia, VentureBeat, TechCrunch, eWEEK, Computerworld, and various other technology titles. He's been quoted on security issues in The Wall Street...

Source: https://www.darkreading.com/application-security/do-cisos-have-to-report-security-flaws-to-the-sec