PERSPECTIVES ON RECENT SEC ACTIONS

Online Summary of the Full Report

Prepared by:

IMBRICATE SECURITY
SECURE PRODUCTIVITY

Aedify

PERSPECTIVES ON RECENT SEC ACTIONS

The SEC action regarding SolarWinds and its CISO Tim Brown was issued on 30 October. As cybersecurity risk management practitioners, we provide advisory clients with actionable feedback. Here are our thoughts on the SEC action, emphasizing that we are not lawyers, and this note does not constitute legal advice[1] in any way.

THE USG PUSHES FOR MORE SECURITY THROUGH ACCOUNTABILITY

While the US government pushes better security through accountability, many within the CISO community take exception to this SEC action, expressing the feeling that it can deter CISOs and hinder their security initiatives. Specifically, practicing CISOs with whom we've spoken are concerned that the action taken was taken against an individual who at the time of breach did not have sufficient title or stature within the organization to effect change. They are also concerned that the SEC took informal statements from individual contributors at face value and out of context, and that those statements are reflective of what many penetration testers and engineers might say about an organization irrespective of business context and risk.

KEY TAKE-AWAYS

1. Consult with legal counsel to consider a 10-year lifetime for data related to your risk management framework, cybersecurity risk roles and responsibilities, risk registers, risk adjudication, security sign-offs, and related contemporaneous policies, standards, processes, and executive decisions.

2. Provide all legal, security, audit, and risk staff with training and guidelines for communicating about the organization's cybersecurity initiatives, security posture, potential exposures or vulnerabilities, and any other similar aspect.

3. Formalize and emphasize the separation of security functions from risk, audit, and compliance functions. This separation can allow more candor within security, while also formally managing and tracking escalations within other functions.

    a. While blunt statements can be a hallmark of a functioning team, organizations should ensure official internal statements about risk include proper context such as current conditions, probable causes, planned actions, likely impacts, and corresponding decisions.

1 Note that we have no comment about whether the events alleged in the SEC action occurred as stated or about any other aspect of anyone's guilt or innocence. Our purpose here is to help reasonable organizations establish reasonable practices that make their risk management strategy more robust and transparent so that it works even when mistakes and unexpected events occur.

b. What about unofficial statements, such as statements made by an employee that a setup is "not very secure" or that "[a]ccess and privilege to critical systems / data is inappropriate"? Employees should certainly voice their concerns and there will be occasions where that must be done in writing. But what happens when someone reads that sentence fragment years later? Managers that receive such staff feedback should create a reporting trail to show that expressed concerns were elevated to a responsible party within an accountable group .

4. Create and publish a sober and factual “Security Statement” or externally facing “Cybersecurity Initiative Explainer” about the people, process, technology, and cultural controls present in the software lifecycle and broader cybersecurity processes.

5. Every organization, especially private companies, must consult with appropriate legal counsel to determine whether the SEC would consider that it's engaging in an offer of a security. If the organization is doing so, then it should quickly establish or improve its risk management program to align with evolving SEC (and other US government) expectations.

a. The SEC states on its website that it "regulates the offer and sale of all securities, including those offered and sold by private companies. Under the federal securities laws, every offer and sale of securities, even if to just one person, must be either registered with the SEC or conducted under an exemption from registration. This is true for companies of all sizes, private and public alike, and includes sales made to anyone, including friends, family, angel investors, and venture capital funds" It continues on to give examples a security that include stock, membership interest, stock option, restricted stock, convertible instruments, and debt. It also notes that some "other early-stage capital raising options may not involve a security, such as" federal grants, donations, and reward or pre-purchase of product.

6. Always be prepared to explain your program and how it is self-correcting. Be prepared with policies and procedures for governing when and how this sharing occurs.

7. CISOs must be diligent in explaining the intricacies of cybersecurity risk in multiple languages–technical, management, staff, investor, and more.

ADDITIONAL POINTS

Every CISO must be capable of describing risk scenarios. This is key to cybersecurity success and requires a mix of soft and hard skills tuned to the organization.

Every CISO must ensure they have a clear and confirmed understanding of the tone at the top and associated risk appetite for a wide variety of risk scenarios.

Each CISO, who is obviously already an executive, should demand to be a full corporate officer and therefore be covered by D&O insurance. Every CISO should do this in every jurisdiction where it's allowed. If it's denied or not allowed, demand a title (e.g., CRO, CSO) that is covered. Even so, getting coverage for legal fees, damages, settlements, and so on does nothing to repair a reputation. Don't take a CISO role that is tantamount to taking a scapegoat role.

So, what happens after a presentation and no investment? Can the CISO give the other executives a quiz after each risk briefing? "Please select below the sentence that best describes your view of the risk scenarios presented today?" If the executives fail the quiz, is it again time to move on?

Again, we're not lawyers and we're certain we've missed nuances in, or outright misinterpreted, some points of the SEC's action. However, we feel confident in the practicality of our risk management approach.

MANAGING THE RISK OF RISK MANAGEMENT

Mature risk management entails continually improving vulnerability discovery capabilities. It's also about understanding the risk tolerance of an organization's executives, stakeholders, and investors. The fact that there aren't infinite dollars or perfect controls means there will always be an exposure gap that will remain, perhaps indefinitely, as the business operates and innovates. Executives must strike a balance between no effort, simply finding issues and moving on, and a best-effort security process that identifies and routinely mitigates potential risk as well as encourages its staff's candor about areas for improvement. This requires a formal and well-documented regimen for risk measurement, analysis, remediation, and acceptance, along with the freedom to continue to innovate and 'move fast' for customers.

The SEC action means that security executives will have to become savvier at explaining to the investing public just how messy software really is, how every organization is constantly under attack, and how attackers win far too often.

Sammy Migues (smigues@imbricatesecurity.com)
John Steven (john@aedify.com)