How Tech Firms Can Get a Head Start on the New National Cybersecurity Strategy

Back when cybersecurity was in its infancy — about two decades ago — simply discovering that an incident occurred was considered a major victory inside an organization. As cybersecurity matured, forensic advances made it possible for organizations to identify the very source of the incident — even if the investigation was drawn out and exact details were often fuzzy.

Today, we've reached a stage where cyber attacks and other cyber crimes are increasingly discovered, monitored, and resolved by the business community. Given how rapidly cybersecurity technology develops, President Biden believes the time is right to leverage organizational intel to help protect and defend our nation's critical infrastructure going forward.

In March, the Biden Administration unveiled its National Cybersecurity Strategy, a comprehensive proposal that leans heavily on the private sector.[i] The White House press release makes plain the government's objective: "We must **rebalance the responsibility to defend cyberspace** by shifting the burden for cybersecurity away from individuals, small businesses and local governments, and onto the organizations that are most capable and best positioned to reduce risks for all of us."[ii]

The proposal asks a lot of the cybersecurity industry, which will now be required to implement security standards into the applications made by tech firms. For software manufacturers in particular, this shift is a sea change in risk management. For the first time, developers will be liable if a software vulnerability or a bad line of code results in a cybersecurity incident — not unlike the way automakers and other manufacturers are responsible for design flaws when they lead to consumer harm.

Getting a head start on implementing basic requirements of the National Cybersecurity Strategy (the "Strategy") can limit cybersecurity risk, achieve compliance, and save tech firms headaches and unnecessary costs down the road. Here's what to know.

Reducing Vulnerabilities

The Strategy consists of five pillars (see "The NCS Pillars"), the third of which, "Shape Market Forces to Drive Security and Resilience," is directed at limiting the vulnerabilities in third-party software applications.[iii] These apps are typically made and supported by software firms on behalf of hardware manufacturers. To get an idea of the scope of this risk, consider that Apple's online marketplace offers approximately 1.8 million apps for download, representing nearly 57% of total market share.[iv,v]

Another common vulnerability involves the default passwords manufacturers supply with new consumer hardware. Often, simple alphanumeric strings designed to help ease initial consumer setup can create enormous, enterprise-wide cybersecurity vulnerabilities when consumers are not forced to change them immediately once the device is operational. Threat actors can easily identify basic password patterns and infiltrate systems and networks that are still using default passwords.

The NCS Pillars [vi]

1. Defend Critical Infrastructure
2. Disrupt and Dismantle Threat Actors
3. Shape Market Forces to Drive Security and Resilience
4. Invest in a Resilient Future
5. Forge International Partnerships to Pursue Shared Goals

The White House wants software makers to seal up these kinds of vulnerabilities. The Strategy states that manufacturers — rather than end users — are best positioned to reduce risk, promote privacy, keep personal data secure and, perhaps most importantly, "incentivize the adoption of secure software development practices." [vii]

Compliance Framework

To get started on compliance, software manufacturers and technology firms should review their internal processes and procedures to determine whether they are adequately addressing security vulnerabilities per the third pillar. If not, organizations should consider implementing industry-accepted best practices such as those found in the Secure Software Development Framework developed by National Institute of Standards and Technology ("NIST").

Designed specifically for the software development life cycle, this "core set of high-level secure software development practices" is built around: 1) preparing the organizations to ensure "that their people, processes, and technology are prepared to perform secure software development at the organization level"; 2) protecting the software and "all components of their software from tampering and unauthorized access"; 3) producing well-secured software "with minimal security vulnerabilities in its releases"; and 4) responding to weaknesses "in their software releases."[viii]

Software manufacturers, too, should review the basic cybersecurity hygiene of their vendors and partners to determine whether their supply chain or third-party relationships include hidden cybersecurity vulnerabilities. Many organizations outsource specific aspects of software development to small, specialist developers who may not have the resources to implement comprehensive security protocols that meet the threshold for the new White House rules. So, while the work can be outsourced, the compliance risks cannot, which means organizations need to conduct supply chain and vendor cybersecurity due diligence to avoid liability.

Conclusion

Tomorrow's cybersecurity will be a leap ahead of today's. Yet even as the technology continues to mature, and the business community carries the development ball forward, threat actors will always be looking to exploit vulnerabilities. Tech firms can do their part now knowing that corporate America, the government, and the cybersecurity industry are behind them.

[i] "National Cybersecurity Strategy." The White House | Whitehouse.gov (March 2023). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[ii] "FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy." The White House | Whitehouse.gov (March 2, 2023). https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[iii] Ibid, p. 19

[iv] David Curry. "App Store Data (2023)." Business of Apps (February 23, 2023). https://www.businessofapps.com/data/app-stores/.

[v] "Mobile Operating System Market Share United States of America: Mar 2022 - Mar 2023." GlobalStats StatCounter (last accessed April 6, 2023). https://gs.statcounter.com/os-market-share/mobile/united-states-of-america.

[vi] Ibid, p. 4

[vii] Ibid, p. 21

[viii] Murugiah Souppaya, Karen Scarfone, and Donna Dodson. "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities." U.S. Department of Commerce, National Institute of Standards and Technology (February 2022). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf.

BRIAN BOETIG
Senior Managing Director, Cybersecurity
+1 206 689 4489
brian.boetig@fticonsulting.com