Published on *The National Law Review* https://natlawreview.com

New CISA Guidelines Lay Out Unified International Principles on Security-by-Design and Security-by-Default

Article By:

Kristin L. Bryan

Shea Leitch

2023 has swiftly become the year of the U.S. National Cybersecurity Strategy. On March 2, 2023, the Biden Administration issued its National Cybersecurity Strategy brief, outlining its vision to: (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; and (5) forge international partnerships to pursue shared goals. In furtherance of the goal to defend critical infrastructure, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default" (the "Report"), on April 13.

Calling the current state of technology "vulnerable by design," the Report aims to encourage technology manufacturers to integrate security into their products from the ground up, factoring security into product development beginning at the design phase. In addition to the CISA, several American security agencies (the National Security Agency and Federal Bureau of Investigation) and international cybersecurity agencies (from Australia, Canada, the United Kingdom, Germany, the Netherlands, and New Zealand) collaborated to provide a unified recommended approach to the development of both software and hardware. Below, we break down what the Report means for the tech sector.

Security-by-Design, -Default Overview

As the Report notes, **Security-by-Design** "means that technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure." This layered approach to design requires every step of the product design and development to be informed with security as a top priority.

Security-by-Default "means products are resilient against prevalent exploitation techniques out of the box without additional charge." While the security of the products is a default, customers are aware that they can expose themselves to risk if they deviate away from default settings.

Both concepts apply to software and hardware products, and the Report encourages manufacturers

of these technologies to build their products with security at the forefront. Customers are also encouraged to hold their key IT suppliers accountable for the security outcomes of their products.

Shifting Responsibility from Consumer to Manufacturer: Key Principles to Remember and Tactics to Embrace

At bottom, the Report seeks to shift responsibility in managing cybersecurity risk from the customer to technology manufacturers. The Report establishes three "core principles" to guide technology manufacturers in their security-by-design and -default efforts:

- The burden of security should not fall solely on the customer;
- Embrace radical transparency and accountability;
- Build organizational structure and leadership to achieve these goals.

The CISA Report acknowledges this challenge, and suggests operational tactics to support manufacturers, many of which are borrowed from the Secure Software Development Framework published by the National Institute of Standards and Technology. The agencies suggest that manufacturers:

1. *Convene routine meetings with company executive leadership to emphasize the importance of Security-by-Design and Security-by Default.*

This principle emphasizes the importance regulators are increasingly placing on the involvement of company leadership in data protection issues. As noted in a prior blog post, the SEC has signaled that boards of directors of publicly-traded companies will be required to make attestations regarding (and, consequently, be held responsible for) their companies' cybersecurity program, board members' cybersecurity expertise, and material security incidents.

The FTC has also been turning up the heat on company leadership, recently imposing conditions within consent decree on the CEO of Drizly after finding that he had failed to "implement, or properly delegate the responsibility to implement, reasonable information security practices" within the organization.

Executive liability has not been limited to regulatory penalties arising from enforcement actions. Uber's former Chief Security Officer was convicted of a felony for concealing a security incident from the FTC, when the ridesharing company was under a consent decree with the FTC which obligated the organization to Report such incidents. The fact that CISA emphasizes the need for company leadership to drive a culture of cybersecurity within technology manufacturers further enforces the necessity of top-down focus on security within companies.

2. *Operate around the importance of software security to overall business success.*

CISA's second principle encourages organizations to prioritize cybersecurity governance within their organization, shifting the perception of cybersecurity within the organization from a cost-center to a business differentiator. To do this, CISA recommends that organizations designate a software

security leader or team to ensure accountability for cybersecurity within the organization and focus the organization's emphasis on cybersecurity. Additionally, the Report emphasizes the need for product security assessments in the product development process.

3. *Use a tailored threat model during development.*

Building on the principle of accountability within cybersecurity product teams, the guidance encourages development teams to consider product use-cases when determining the appropriate threat model to use for such products. Company leadership is encouraged to hold team members accountable for delivering secure, high-quality products.

Recommended Development Tactics for Implementation of Security-by-Design

In addition to the principles outlined above, CISA's guidance includes recommended development strategies and tactics to ensure security-by-design and -default are baked into technology products. Among the features recommended are the use of memory safe programming language, secure hardware architecture, secure software components (like software libraries, modules, middleware, and frameworks), secure web template frameworks, a secure code review process, and use of defense-in-depth to ensure layered security features.

Recommended Development Tactics for Implementation of Security-by-Default

The Report also outlines several tactics technology manufacturers can employ to implement security-by-default. Recommended security-by-default strategies include elimination of default passwords and mandatory multi-factor authentication, implementation of single sign-on, secure, robust logging capabilities, providing guidance to customers on appropriate authorized profile roles and use cases, and consideration of user experience in security design.

Implications and Challenges of Implementing Security-by-Design and -Default

There is no doubt that this shift will be a learning curve for — and require deep investment from—the tech sector. Additionally, the Report acknowledges that customers sometimes push back on or fail to implement recommended security controls, resulting in latent vulnerabilities. In such cases, CISA recommends that manufacturers incentivize customers to implement their products in a secure manner rather than "allow[ing] them to remain vulnerable indefinitely." The Report notes that technology manufacturers often develop hardening guides to enable customers to embed additional security features into their products. By implication, this means that the products are not optimally secure out-of-the-box. Accordingly, CISA encourages companies to implement the hardened version of their product and publish "loosening guides," rather than hardening guides. If approached in this way, the secure configuration would become the default, and the customer would be enabled to reduce security controls at their discretion.

Conclusion

As the Biden administration continues to press its emphasis on cybersecurity and data privacy, compliance can quickly become extremely challenging and complex. To assist, SPB offers in-depth guidance on the development of appropriate security practices to ensure a defensible cybersecurity posture in light of today's constantly-evolving threat landscape. *Privacy World* will continue to keep

you updated on the national cybersecurity strategy and other state and federal privacy developments as they continue to develop.

National Law Review, Volume XIII, Number 123