Written Testimony of Jim Richberg

Head of Cyber Policy & Global Field CISO

Fortinet, Inc.

Before the U.S. House Committee on Homeland Security

Subcommittee on Cybersecurity and Infrastructure Protection

Hearing on

“Design vs. Default: Analyzing Shifts in Cybersecurity”

December 5, 2024

Chairman Green, Ranking Member Thompson, Chairman Garbarino, Ranking Member Swalwell, and distinguished Members of the Subcommittee, I appreciate the opportunity to testify before you today on "Secure by Design", which is an important but little understood tool for improving cybersecurity. My name is Jim Richberg and I serve as Head of Cyber Policy and Global Field Chief Information Security Officer at Fortinet.

Fortinet[1] is a US company that is one of the largest cybersecurity companies in the world. While we manufacture over half of the firewalls sold worldwide, our portfolio extends across nearly 60 different integrated cybersecurity and networking solutions and services, reflecting our commitment to innovation as information technology (IT) and cyber threats continue to evolve. In addition to our products and services, Fortinet operates a robust cybersecurity training institute[2] focused on helping to address the significant global cyber workforce and skill gaps and enabling a more digitally secure society.

Fortinet is part of numerous collaborative activities between industry and the US Government, ranging from participation in the IT sector's coordinating council to collaboration on technology development through NIST's National Cybersecurity Excellence Partnership[3] and coordinated cyber threat analysis and response via the Joint Cyber Defense Collaborative[4] (JCDC) run by the Cybersecurity and Infrastructure Security Agency (CISA). Reflecting the fact that cybercrime does not stop at country borders, Fortinet also participates in global initiatives such as the World Economic Forum Centre for Cybersecurity[5] and the Cyber Threat Alliance[6].

I represent Fortinet in multiple public-private sector fora and work with governments and large enterprises across the US and globally to address complex cyber problems ranging from Artificial Intelligence to Zero Trust. My knowledge of cybersecurity, the cyber threat landscape, and the need for building cyber resilience within organizations and nationally is based upon my 33 years of service in the U.S. Government as well as my work at Fortinet. I oversaw the implementation of the

[1] https://www.fortinet.com/corporate/about-us/about-us
[2] https://training.fortinet.com
[3] NCEP: A Mechanism for Partnering with NCCoE | NCCoE
[4] Joint Cyber Defense Collaborative | CISA
[5] https://centres.weforum.org/centre-for-cybersecurity
[6] Home - Cyber Threat Alliance

whole of government Comprehensive National Cybersecurity Initiative[7] for Presidents Bush and Obama. I also served as the National Intelligence Manager for Cyber under two Directors of National Intelligence and was responsible for creating a unifying cyber strategy for the US Intelligence Community and for setting its cyber threat priorities.

Information Technology is part of US critical infrastructure, and I am honored to represent Fortinet in the Sector Coordinating Council[8] that serves as the sector's voice and partner for collaboration with CISA, which is the Sector Risk Management Agency for IT. As a Council member, I was one of the leaders in its extensive collaboration with CISA on Secure by Design and I am well positioned to talk about this initiative both broadly and in depth.

What is Secure by Design and Where did it come from?

Secure by Design was part of the 2023 US National Cybersecurity Strategy[9], which recognized the need for a fundamental shift in how the United States should allocate roles, responsibilities, and resources in cyberspace. The Strategy noted that "We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, local governments, and infrastructure operators, and onto the organizations that are most capable and best positioned to reduce risks for all of us[10]." This meant shifting the focus of responsibility towards the producers of the IT products and services which are vital to individuals, organizations, and our critical infrastructure.

Following the release of the US National Strategy, Secure by Design was described in greater depth in a White Paper [11]authored by CISA, other US Government agencies, and international partners in 2023. Its guidance for IT manufacturers focused on three core principles:

1. "The burden of security should not fall solely on the customer. Software manufacturers should take ownership of the security outcomes of their customer's purchase and evolve their products accordingly
2. Embrace radical transparency and accountability. Software manufacturers should pride themselves in delivering safe and secure products, as well as differentiating

[7] NSPD 54: Cybersecurity Policy
[8] IT Sector Coordinating Council - Home
[9] National Cybersecurity Strategy | ONCD | The White House
[10] National Cybersecurity Strategy | ONCD | The White House
[11] Secure By Design

themselves from the rest of the manufacturer community based on their ability to do so. This may include sharing information they learn from their customer deployments, such as the uptake of strong authentication mechanisms by default. It also includes a strong commitment to ensure vulnerability advisories and associated common vulnerability and exposure (CVE) records are complete and accurate. However, beware of the temptation to count CVEs as a negative metric, since such numbers are also a sign of a healthy code analysis and testing community.

3. Build organizational structure and leadership to achieve these goals."[12]

The White Paper also introduced the concept of 'Secure by Default', with vendors shipping products in configurations that would be effective against the most likely or prevalent threats rather than relying on users to become near-experts before they could become secure, or to follow 'hardening guides' that require the customer to take specific configuration steps to operate securely. Many have cited the multi-faceted public and private sector effort that led to dramatic improvements in motor vehicle safety[13] as proof that collective cybersecurity can be enhanced through Secure by Design manufacturer-driven action. 'Secure by Default' is similar, potentially encompassing the equivalent of seat belt chimes - 'noisy' and repeated reminders that would notify a user when they operate a product in a less-than-secure mode.

The government-drafted White Paper described the potential of Secure by Design, but it did not constitute an adequate roadmap for either producers of software or more critically, for customers to use. Making this concept usable required sustained engagement and public-private sector partnership.

Crafting a Voluntary Secure by Design Pledge

To that end, in late 2023 CISA began work with the IT Sector Coordinating Council on Secure by Design with the intent of making the concept actionable in the form of a voluntary pledge[14] that producers of software could adopt and that current or potential customers could use as a guide. I co-led this process of collaboration from the industry side.

[12] Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

[13] https://www.nhtsa.gov/how-vehicle-safety-has-improved-over-decades

[14] Secure by Design Pledge | CISA

CISA had the pen but was open to industry's input on both specific content and the structure of the Pledge. While recognizing that signing the Pledge was going to represent a purely voluntary commitment, CISA was adamant that it be viewed as an 'all or nothing' undertaking by signatories rather than something where they would 'cherry pick' goals to work on. CISA and the industry team that worked on the Pledge focused on selecting and framing actions that could be achievable even for small businesses, but also provide room for improvement by larger and more cyber-capable companies.

Our philosophy in crafting the Pledge was to agree on goals to be pursued without prescribing any specific means for reaching them. In other words, industry and CISA worked to reach agreement on outcomes (what to accomplish) and left it to signatories to determine how to tackle accomplishing these goals. This is perhaps most relevant to the Pledge goal focused on eliminating entire classes of vulnerabilities, where both the specific outcomes and the means for implementation are likely to vary significantly by signatory and the type of vulnerability they have chosen to address.

We were mindful during Pledge development that its goals should generate measurable outcomes and measures of progress that could be shared with the public and with customers. We realized that, if the Pledge was to become widely adopted, its goals had to be both attainable and impactful. We also recognized that the Pledge approach was likely to be iterative, and the initial Pledge was envisioned as a 'proof of concept' that could generate lessons learned to inform any further collaboration on a revised Pledge.

Details of the Secure by Design Pledge

By signing the Pledge, companies undertake to show measurable progress against the following goals within one year[15]:

1. **Multi-factor authentication (MFA):** demonstrate actions taken to measurably increase the use of multi-factor authentication across the manufacturer's products.
2. **Default passwords:** demonstrate measurable progress towards reducing default passwords across the manufacturers' products.

[15] Secure by Design Pledge | CISA

3. **Reducing entire classes of vulnerability:** demonstrate actions taken towards enabling a significant measurable reduction in the prevalence of one or more vulnerability classes across the manufacturer's products.
4. **Security patches:** demonstrate actions taken to measurably increase the installation of security patches by customers.
5. **Vulnerability disclosure policy:** publish a vulnerability disclosure policy (VDP)
6. **CVEs**: demonstrate transparency in vulnerability reporting
7. **Evidence of intrusions:** demonstrate a measurable increase in the ability for customers to gather evidence of cybersecurity intrusions affecting the manufacturer's products.

The Pledge was designed to define a floor or minimum level of commitment in each of the areas addressed by the Goals and not to establish a performance ceiling. For example, cyber attackers often take advantage of poor identity and access management controls, so the Pledge calls on signatories to increase the use of Multi-Factor Authentication (MFA) by customers. There are multiple ways to accomplish this goal, some of which provide security against more sophisticated attacks, but even basic MFA improves security compared to employing a user id and password alone.

The Pledge was publicly released in May 2024, with 68 companies –including Fortinet–signing it at the RSA cybersecurity conference. As of 1 December 2024, over 250 companies[16], ranging from small software developers to some of the largest IT firms in the world, have signed this voluntary agreement.

Fortinet's Perspective on the Importance of the Pledge

I volunteered to lead industry's collaboration with CISA both because of my personal belief in the potential value of this approach and because of Fortinet's industry leadership in many of the concepts at the core of Secure by Design. At Fortinet, we have a long-standing dedication to proactively incorporating and adhering to security best practices aligned with government partners like CISA across our product development life cycle. As a company we believe that seeing Secure by Design precepts implemented more broadly would be beneficial to our collective security and that it is achievable by industry.

[16] Secure by Design Pledge Signers | CISA

Secure coding practices and tools continue to improve with time, and Fortinet has combined these improving industry-wide capabilities along with internally driven innovation. Our Secure Product Development Lifecycle Policy, which is based on secure-by-design and secure-by-default principles, helps ensure that security is built into each product from its inception and covers every stage of the product life cycle from initial design through to the end of product use.

Embracing Radical Transparency

Computer code is written by humans and given the size and complexity of modern software programs, mistakes in creating or maintaining software or in user configuration of a product are virtually inevitable. The growth in computing power, new modes of connectivity, and ever-expanding malicious actor tactics, techniques and procedures also drive the exploitability of vulnerabilities. In general, software vulnerabilities can be found by one of three sources:

1. The manufacturer of a product, who is arguably the most familiar with its functions and inner workings.
2. Customers who may encounter problems or anomalies during use, and third-party security researchers who explicitly look for potential problems. If these problems are reported to or shared with the manufacturer, they may be fixed or 'patched'.
3. Malicious actors who, when they find a vulnerability, exploit it rather than report it for mitigation.

Fortinet is proud that nearly 80% of the vulnerabilities discovered in its products in 2023 were identified by the company internally (#1 above) rather than found by outsiders (#2 and #3).

Radical Transparency is one of the core tenets of Secure by Design. If something matches the characteristics of a CVE, Fortinet is committed to reporting it as such rather than fixing the problem in the guise of a 'performance enhancement'. To improve national cyber resilience and consumer awareness, Fortinet believes that IT companies should collectively practice such "radical transparency" with respect to their disclosures of vulnerabilities, whether they are found internally or externally.

Correctly and comprehensively cataloging problems, patches and upgrades is important. Large organizations often devote resources to verifying that a patch works as intended and to validating that it does not break something else in an organization's IT environment before they will install the update. While well-resourced organizations may have the staff and budget to perform this validation and verification process, their resources are finite. Organizations will often make the decision whether to perform validation and verification based on whether a software update is to a function that is relevant to them. If a security vulnerability is mischaracterized as a 'bug fix', 'performance enhancement' or functional upgrade, a company may not apply a patch without realizing that its' security is affected by the underlying vulnerability that the patch addresses[17].

As a rule, smaller organizations and individual users typically don't have a formal process or policy with regards to patching. They often fail to patch due to resource limitations or because they are not even aware of an update's existence. For these users, a vendor policy of automatically updating software will result in more widespread patching and increased security for these enterprises and users.

Fortinet's Performance on the Pledge

Fortinet has been making significant progress implementing the specific goals outlined in the CISA Secure by Design Pledge since signing it in May 2024. Our efforts[18] include:

- Eliminating default passwords and prompting users to create strong passwords during the product installation process.
- Implementing automatic/by default update capabilities for products typically used by small and medium-sized organizations – automatically remediating security issues (applying security patches) while allowing users to opt out if desired.
- Demonstrating transparency through reporting all Common Vulnerabilities and Exposures (CVEs) along with the accompanying Common Weakness Enumeration (CWE). This is important since CISA has observed that many organizations will report a vulnerability without noting the class (CWE) of activity it belongs to. This omission makes it difficult to use the National Vulnerability Database of CVE's for either strategic analysis (e.g., to determine which are the most prevalent classes of vulnerability) or tactically (enabling an organization to search by the classes of weakness relevant to itself).

[17] How Proactive Responsible Radical Transparency Benefits Customers | Fortinet
[18] https://www.fortinet.com/blog/industry-trends/fortinet-progress-on-its-secure-by-design-pledge-commitments

- Publishing a machine-readable security policy and portal for our customers or third-party researchers to use in reporting any vulnerabilities they find in Fortinet products.
- Working to eradicate whole classes of vulnerability.

Fortinet is working on numerous initiatives aligned to the other Pledge objects as well, such as providing greater support to help customers using end-of-life products transition to newer supported versions.

What's Next? Looking beyond the Secure by Design Pledge

Secure by Design and Secure by Default have been shown by Fortinet and other early adopters to be viable for IT manufacturers to implement and to generate measurable improvements in their customers' security. However, this approach will only succeed if it is recognized and desired by the marketplace—and unfortunately this is not like the movie *"Field of Dreams"* where if you build it, they (customers) will automatically come. The crucial step will be in creating viable 'Secure by Demand'.

I speak frequently with cybersecurity and IT executives at major companies and have found that few of them are aware of Secure by Design—but that virtually all of them were interested in considering it as a possible factor in procurement decisions. A logo or symbol indicating that a manufacturer has signed the Pledge and an accompanying consumer awareness campaign could help increase overall user awareness of Secure by Design. There is a potential role for both government and the private sector in accomplishing this.

At this point, over 250 companies representing a significant portion of the software market have signed the Pledge, and customers likely can find a supplier in most major categories of software who has signed the Pledge and made a commitment to showing what they have done to implement it. Over a dozen allied governments joined the US in co-authoring the Secure by Design White Paper[19], making participation in fielding products demonstrating the Secure by Design approach more attractive to companies that sell IT in multiple national markets.

Broadening the scope and application of this concept beyond IT could also help build demand, and work is underway to apply the concept to Operational Technology (OT) as well. But while the Operational Technology environment has a significant overlap with IT in terms of security problems

[19] Secure-by-Design | CISA

and solutions, significant differences make a wholesale ‘lift and shift’ of the IT-focused model impractical for OT. The ecosystem of producers and customers is different, and the product lifecycle is dramatically longer, with OT systems often kept in service for 30 years or more rather than replaced every few years as in IT. Mission priorities also differ, with OT operators emphasizing safety and reliability over security.

Conclusion

As one who has worked on cybersecurity in both the public and private sectors, I believe that letting market forces drive broad change is a powerful and practical approach to improving our cybersecurity and digital resilience. Secure by Design is not a panacea but it can be a powerful lever for private sector-led enhancement of our cybersecurity. This concept is a work in progress, and like the process of creating the current Secure by Design Pledge, its ultimate success will require continued public-private partnership. We in industry stand ready to assist the Committee, and I thank you for the opportunity to be part of this important hearing. I look forward to today’s discussion and I welcome your questions.