LAWFARE
HARD NATIONAL SECURITY CHOICES

"Security by Design" in Practice: Assessing Concepts, Definitions, and Approaches

Eugenia Lostri* and Justin Sherman**

AUGUST 2024

There is significant consensus about the meaning of "security by design," but less on the definition and utility of "security by default."

INTRODUCTION

The software and hardware on which we rely is pervasively insecure. This insecurity is made all the more damaging because of how ubiquitous and integrated technology has become. From smart devices and automobiles to cloud computing environments and critical infrastructure, the software and hardware underpinning key societal functions routinely have major security failures that would be unacceptable in other product domains.[1] Companies, through their design practices, create risk that disproportionately falls on users—other companies, individuals, and society broadly—that rely on their software. The U.S. government's 2023 National Cybersecurity Strategy aims to realign the incentives for companies around cybersecurity through the concept of "security by design" and by exploring liability on product vendors for insecure software.[2]

At a high level, the idea of security by design is straightforward. Major technology products are often designed without the most basic security measures, so by integrating cybersecurity considerations into the design process, product managers, software developers, engineers, and other involved parties can build in security best practices *before* products are built and deployed into the world. But in practice, many questions remain—such as how the concept is implemented, whether security by design looks different across product verticals or company sizes, and what incentives will compel companies to implement security-by-design processes.

***Eugenia Lostri** is *Lawfare*'s Fellow in Technology Policy and Law.
****Justin Sherman** is a contributing editor at *Lawfare* and the founder and CEO of Global Cyber Strategies.

[1] This introduction draws on Benjamin Wittes and Paul Rosenzweig, "Announcing a New Lawfare Project on 'Security by Design,'" *Lawfare*, Aug. 28, 2023, https://www.lawfaremedia.org/article/announcing-a-new-lawfare-project-on-security-by-design.

[2] The White House, *National Cybersecurity Strategy*, March 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 5.

The Lawfare Institute announced a multi-year project to evaluate the meanings, potential implementations, and likely implications of "security by design" for software in August 2023. Following the project's launch, we sought to answer two foundational research questions to frame the project: How much consensus is there among industry and government stakeholders around the meaning of the term "security by design"? Relatedly, how much consensus is there around the meaning of the term "security by default"?

This paper seeks to answer these questions by examining the ways in which different stakeholders understand and implement security by design in software products, and what their understanding and implementation of security by design might illuminate about *Lawfare*'s relevant work. It focuses on U.S. companies and organizations and explicitly excludes hardware products from its scope. This paper explores the research questions by drawing on a literature review of major security-by-design publications in the executive branch, industry, and academia. It then presents novel findings from interviews with major software developers, members of the open-source software community, cybersecurity vendors, U.S. government officials, and other players in the U.S. technology and cybersecurity ecosystem.

Major themes of the paper and the underlying interviews orient around the definitions and concepts of "security by design" and "security by default," the necessity and challenge of scaling security by design in organizations, the market incentives and disincentives for security by design, and the unique challenges that open-source communities and software products face when defining and implementing security by design.

Two distinct findings emerge from our research: First, there is relative consensus about the meaning of security by design at a high level—such as that security by design is about processes and principles more than the use of specific technologies or specifications per se—but perspectives on how to practically implement security by design are less unified. Second, there is considerable skepticism about the usefulness of "security by default" as a concept and the extent to which it is meaningfully different from security by design.

This is not just semantics. Security by design may come to play an increasingly important role in potential federal law, regulation, and policy on software security—as well as liability for software insecurity. High-level concepts and principles about security by design must be interpreted and translated down by companies, government organizations, open-source communities, and other stakeholders into specific design processes, development policies, and technical guidance. Thus, how companies, government organizations, and others understand and interpret these terms impacts not just the security of software products themselves but also those organizations' and developers' legal compliance, regulatory exposure, and potential liability for poor security practices. And evaluating how the concepts of "security by design" and "security by default" are evolving and how stakeholders perceive them also enables us to assess the U.S. government's efforts to market and build out the ideas.

After presenting these findings, the paper concludes with a discussion of open questions and areas for future research.

METHODOLOGY AND INTERVIEWS

This paper seeks to answer two research questions, scoped around U.S. software products:

- How much consensus is there, among industry and government stakeholders, around the meaning of the term "security by design"?
- Relatedly, how much consensus is there around the meaning of the term "security by default"?

The research process began with a literature review, surveying major government, industry, and academic publications related to the concept of "security by design." The literature review focused in particular on sources that defined the concept of "security by design" or a very similar term. Doing so helped us establish a baseline of different conceptual definitions and how security by design (and security by default) could be implemented in practice to improve software cybersecurity. The literature review was not designed to include every single source published on the topic, nor was it designed to cover all sources that touched in some way on the issues of insecure software development; it was intended to provide a snapshot of the landscape. We describe some of the findings from this literature review below, and the full annotated version of the literature review is published on *Lawfare*, along with co-author Reganne Hardy.[3]

We then interviewed experts at Google and Microsoft about how they and their organizations view the concepts of "security by design" and "security by default." We selected these companies because they are major software vendors. We likewise asked Apple to make some of their experts available for an interview for this study, but Apple declined.

We also interviewed experts at the Cybersecurity and Infrastructure Security Agency (CISA), CrowdStrike, a major open-source software organization, and Schneider Electric. All the interviews were conducted before May 2024. We selected these organizations for various reasons. For example, we were interested in input from CISA because of its role in promoting the concept of security by design and the unnamed open-source software organization because of the unique challenges of securing open-source software.[4] Schneider Electric offered insight into the problem from an operational technology perspective. When identifying the source of statements from individuals within the organizations we interviewed, we do not name the specific employees but state the company at which an employee works—except for the statements made in our conversation with the open-source software organization. We agreed to conduct that conversation without attribution to the organization because it allowed us to include implications of our findings related to security by design and security by default for the

[3] Reganne Hardy, Eugenia Lostri, and Justin Sherman, "Security by Design: An Annotated Resource List," *Lawfare*, Feb. 28, 2024, https://www.lawfaremedia.org/article/security-by-design-an-annotated-resource-list.
[4] John Speed Meyers and Paul Gibert, "Questioning the Conventional Wisdom on Liability and Open Source Software," *Lawfare*, April 18, 2024, https://www.lawfaremedia.org/article/questioning-the-conventional-wisdom-on-liability-and-open-source-software.

open-source community. (We would not have been able to interview members of the organization for this paper if we were to name it.)

The interviews focused on the concepts of "security by design" and "security by default" and, in line with our research questions, how organizations and individual experts viewed the concepts. The questions for each session were highly similar but not identical. Every interview was designed to draw out perspectives from law, technology, and policy. We describe the findings from the interviews below, along with our analyses.

THEMES AND TAKEAWAYS

After conducting interviews with the stakeholder organizations, we analyzed the conversations and grouped the takeaways into three themes: definitions and terminology, scalability of solutions and processes, and the incentives and disincentives at play in the market (including security by design as part of corporate culture).

Definitions and Terminology

There is much discussion of "security by design" and "security by default" as concepts, but it's not clear if there are cohesive definitions across industry and government. Our literature review made this clear. In a February 2023 article, CISA Director Jen Easterly and Executive Assistant Director Eric Goldstein defined the terms as follows:

- Secure by design: "[T]he expectation that technology is purposely designed, built, tested, and maintained to significantly reduce the number of exploitable flaws before it is introduced to the market for broad use."

- Secure by default: "[P]roducts have strong security features … at the time of purchase, without additional costs."[5]

In an April 2023 paper, CISA's definitions of "secure by design" and "secure by default" shifted slightly from the ones offered by Easterly and Goldstein two months prior:

- Secure by design: "Technology products are built in a way that reasonably protects against malicious cyber actors successfully gaining access to devices, data, and connected infrastructure."

[5] Jen Easterly and Eric Goldstein, "Stop Passing the Buck on Cybersecurity," *Foreign Affairs*, Feb. 1, 2023, https://www.foreignaffairs.com/united-states/stop-passing-buck-cybersecurity.

- Secure by default: "[P]roducts are resilient against prevalent exploitation techniques out of the box without additional charge."[6]

Adjacent to these definitions, the Office of Management and Budget (OMB), in a 2023 Memorandum on the Administration Cybersecurity Priorities for the FY 2025 Budget, said budget submissions for federally funded programs should show that the agency is supporting projects that are "designed, developed, fielded, and maintained with cybersecurity resilience in mind."[7] And the National Institute of Standards and Technology (NIST) published its guide on Engineering Trustworthy Secure Systems that lays out "principles, concepts, activities, and tasks" to ensure that technology systems are engineered to certain levels of security.[8]

There is also a robust academic and industry literature around maximizing cybersecurity in software and technology design. In a 1975 paper, Jerome Saltzer and Michael Schroeder identified several principles to guide the development of systems without security flaws[9]: "[e]conomy of mechanism,"[10] "[f]ail-safe defaults,"[11] "[c]omplete mediation,"[12] "[o]pen design,"[13] "[s]eparation of privilege,"[14] "[l]east privilege,"[15] "[l]east common mechanism,"[16] and "[p]sychological acceptability."[17] In 2018, the nonprofit SAFECode released its Fundamental Practices for Secure Software Development,[18] which referred to Saltzer and Schroeder's work

[6] Cybersecurity and Infrastructure Security Agency, "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default," April 13, 2023, https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf.
[7] Office of Management and Budget, "Memorandum for the Heads of Executive Departments and Agencies," June 27, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-18-Administration-Cybersecurity-Priorities-for-the-FY-2025-Budget-s.pdf.
[8] Ron Ross, Mark Winstead, & Michael McEvilley, "Engineering Trustworthy Secure Systems," National Institute of Standards and Technology, SP 800-160 Vol. 1 Rev. 1, November 2022, https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final.
[9] Jerome H. Saltzer and Michael D. Schroeder, "The Protection of Information in Computer Systems," 1975, https://web.mit.edu/Saltzer/www/publications/protection/index.html.
[10] Ibid. ("Keep the design as simple and small as possible.").
[11] Ibid. ("Base access decisions on permission rather than exclusion.").
[12] Ibid. ("Every access to every object must be checked for authority.").
[13] Ibid. ("The design should not be secret.").
[14] Ibid. ("Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.").
[15] Ibid. ("Every program and every user of the system should operate using the least set of privileges necessary to complete the job.").
[16] Ibid. ("Minimize the amount of mechanism common to more than one user and depended on by all users.").
[17] Ibid. ("It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.").
[18] SAFECode, "Fundamental Practices for Secure Software Development: Essential Elements of a Secure Development Lifecycle Program," 3rd ed., March 2018, https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf.

with additional principles of "[d]efense-in-depth,"[19] "[f]ail securely,"[20] and "[d]esign for updating."[21] The list goes on.

During the expert interviews for the paper, the first questions focused on organizations' and individuals' definitions and broader conceptualizations of "security by design" and "security by default." At a high level, there was relative consensus across interviews with Microsoft, Google, CISA, and the other interviewees that security by design is about building security processes not just into software design itself—as in policies for product managers, tool sets for software engineers, etc.—but also into how policy and legal elements of the organization conceptualize cybersecurity.

This is not necessarily surprising; many individuals at software vendors have a stake in cybersecurity. But it is an important point given how much of the security-by-design discourse has focused on software development processes and on public policies around software liability, rather than also on emphasizing the importance of internal company policies to facilitate security by design. For instance, multiple software companies we interviewed spoke about the importance of creating and enforcing internal policies and technical access controls that require software developers to use specific memory-safe programming languages—and to get explicit sign-off before they are permitted to deviate from the policies. Such policies must be informed (or even written) by technical security experts, and they are also what guide software engineers to improve their products' security in practice.

All of which is to say that, from a process standpoint, several interviewees commented that they believed there to be a relative consensus among industry software vendors on security by design, such as by looking to the processes in NIST's Secure Software Development Framework[22] and cybersecurity process guidance from the International Organization for Standardization (ISO).

More specific questions about *how to implement* security by design yielded more varied answers. Microsoft pointed to its Security Development Lifecycle as an example of a framework implementing security-by-design principles.[23] One expert at Microsoft noted that customer demand plays a role, too. For example, in payment processing, security-by-design practices

[19] Ibid. ("design the system so that it can resist attack even if a single security vulnerability is discovered or a single security feature is bypassed.").
[20] Ibid. ("[A] counterpoint to defense in depth is that a system should be designed to remain secure even if it encounters an error or crashes.").
[21] Ibid. ("[N]o system is likely to remain free from security vulnerabilities forever, so developers should plan for the safe and reliable installation of security updates.").
[22] Murugiah Souppaya, Karen Scarfone, & Donna Dodson, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," National Institute of Standards and Technology, SP 800-218, February 2022, https://csrc.nist.gov/pubs/sp/800/218/final.
[23] Microsoft, "About the Microsoft Security Development Lifecycle (SDL)," https://www.microsoft.com/en-us/securityengineering/sdl/about.

might be biased toward the Payment Card Industry Data Security Standard (PCI DSS),[24] and in health, security-by-design practices might be biased toward the Health Insurance Portability and Accountability Act (HIPAA).[25]

Google interviewees mentioned the use of product red teams, implementing "fuzzing" (automated software tests that inject random or bad data), and using vulnerability reports to inform future software design practices. Experts at CrowdStrike commented that policymakers should think about software cybersecurity problems from a risk mitigation standpoint and consider how authentication flaws, abuses of legitimate credentials, and other attack vectors fit into a security-by-design approach. The Schneider Electric interviewee focused on adherence to standards for operational technologies and conducting security assessment processes.

Interviewees at CISA and Google both mentioned the use of formal methods—mathematical techniques in computer science for designing and analyzing software—and how they could be used in conjunction with practical programming techniques to implement security-by-design principles. CISA officials stressed that security is not a binary and that the costs of security-by-design processes can vary depending on the technical issue at hand: Companies may find, one person mentioned, that if they only have the budget to pick one security-by-design measure to implement company-wide first, that implementing measures for a memory-safe programming language is more costly than secure database configuration at the outset. And several different interviewees, including at Google and at Microsoft, mentioned the importance of variation in how to implement security by design: when building internally facing vs. externally facing products, when building products in the latter case for a consumer customer vs. for an enterprise customer, and when building products for an existing customer vs. for a new customer. For example, an enterprise or government customer may have their own requirements they want custom built into a software product that requires the company to change its security-by-design process. An individual consumer, however, may not have the option of paying to get a custom-tailored version of the software product and would therefore buy the product off-the-shelf with whatever security-by-design process the company has in place.

At multiple companies, interviewees stressed that "security by design" is a useful term but that it could mislead organizations and lead them to focus on just software design, rather than on the entire software lifecycle (design, development, deployment, management, and retirement). This is a critical takeaway. Perhaps this perspective is missing the narrow objective—one could argue that the point, after all, of security *by design* is to focus cybersecurity investments on the product design phase, not anywhere else. But even so, policymakers, regulators, software vendors, and all organizations using software should remember that security by design may be focused just on the design stage, thus leaving questions about software updates, software

[24] PCI Security Standards Council, "Payment Card Industry Data Security Standard," https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf.
[25] U.S. Department of Health and Human Services, Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996.

sunsetting, and other important issues unaddressed. Technologists and policy specialists at multiple companies also praised CISA for its initial efforts to promote security principles and understandable guidance, but raised concerns about regulators' general tendency to pursue check-the-box approaches.

Finally, non-CISA interviewees suggested that there is little meaningful difference between the terms "security by default" and "security by design." Some individuals suggested the terms could be combined or integrated together. For example, if CISA's February 2023 definition of "secure by default" says that products have strong security features at the time of purchase, is that not captured by "secure by design," which says products must be designed, to then be sold, with security from the outset? Or if "default," one interviewee remarked, is meant to refer to the baseline security settings presented to a user—such as turning on end-to-end messaging encryption by default or restricting users' file downloads by default—is that not just designing security features into an application from the beginning of the product lifecycle?

In reading the documentation provided by CISA and a few related articles, we found it difficult to discern the difference between the two terms. CISA's April 2023 white paper, for example, describes "secure by design" as building products in a way that reasonably protects against malicious activity.[26] And it describes "secure by default" as building products that are resilient against exploitation out of the box, without additional change. The difference is not clear between reasonably protecting against exploitation by design and creating resilience against exploitation out of the box. Perhaps this is due to the newness of the U.S. government's security-by-design push for industry, and perhaps the distinction will become clearer over time or with future articulations of the concepts. For now, though, the distinction between security by design and security by default is quite unclear. Based on interviewees' consensus about what security by design means in terms of processes, using the term "security by design" may be the strongest way forward for government agencies and companies trying to "speak the same language" and use the clearest terminology.

Scalability of Solutions and Processes

Once organizations have defined or conceptualized "security by design," they have to look beyond their cybersecurity teams and implement it across their organizations, all of their employees, and all of their products. Security by design already creates friction with tech cultures that favor innovation speed over cybersecurity, business models that demand minimum viable products (MVPs)[27] pushed out as quickly as possible, and more—all tensions covered in the next section. Making secure design a reality across an entire organization and its software ecosystem is an even greater challenge than implementing security by design into a

[26] Cybersecurity and Infrastructure Security Agency, "Shifting the Balance of Cybersecurity Risk."
[27] Product Plan, "Minimum Viable Product (MVP)," https://www.productplan.com/glossary/minimum-viable-product/ ("a product with enough features to attract early-adopter customers and validate a product idea early in the product development cycle").

single process or product. This is the idea of "scalability." We asked interviewees about scalability in all of our conversations.

To scale security by design across an organization, cybersecurity professionals must articulate why security by design matters across all the component sub-organizations and processes. Therefore, scalability includes making the case for why all code templates used by developers must have baked-in security, why product managers must have some understanding of company cybersecurity policies and considerations, and so forth. For example, some interviewees mentioned that industry's general emphasis on MVPs can make security, reliability, and related considerations feel like a "tax" on organizations that only grows exponentially with the organization; in other words, if security by design is maintained, the bigger the organization, the bigger the necessary security infrastructure, and thus the bigger "tax" on product development and rollout. No one, of course, was suggesting that larger organizations should halt implementation of security by design. Rather, the discussion underscores the importance of baking it into processes so that it's as efficient as possible and the value to the organization is clearly articulated.

With respect to efficiency, scalability also depends on the idea—and practice—of minimizing friction for developers. Interviewees at CISA, Google, Microsoft, and other organizations gave many examples of how to make security scalable with minimal friction, or without imposing an "undue burden" on developers, as one interviewee put it. Some experts pointed to the 2017 report from the New York Cyber Task Force on the concept of "leverage" in cyberspace and the importance of identifying security measures, such as encryption, where the benefits scale easily and are especially helpful for defenders.[28] Others pointed out examples of how companies can set internal policies and access controls to mandate that their developers use only memory-safe programming languages; predefined web templates; code templates with built-in preventions of cross-site scripting attacks; prescreened application programming interfaces (APIs); and other code, tools, and technologies that allow developers to build secure software from the start. Setting defaults is powerful here. For instance, a default to scale up security with minimal friction could be a company giving its developers access to memory-safe programming languages in their integrated development environment and blocking access to using any unsafe language (except with specific, defined, and authorized approval). The default is therefore to use a language that is memory-safe.

How this works—and how well it works—in practice depends partly on an organization's technical expertise, resources, internal architectures, and product base (software mainly for consumers vs. for enterprises vs. for both). No two companies are going to look exactly the same. As interviewees at Google put it, each organization has to figure out how to set invariants—properties that must remain true no matter what—and engineer developer tool sets and development processes around them to ensure it's impossible to negate those invariants. A

[28] New York Cyber Task Force, "Building a Defensible Cyberspace," Columbia University School of International and Public Affairs, 2017, https://www.sipa.columbia.edu/global-research-impact/initiatives/cyber/nyctf/defensible-cyberspace.

large corporation could be building software for enterprise clients and have much more experience with security at scale and how to alter development processes across thousands of workers; it may also have to contend with years-old legacy code, riddled with security vulnerabilities, and overcome entrenched processes. A smaller business creating software for consumers' home devices may face more challenges in growing out a security-by-design program and identifying which policies to set and technologies to require by default, but it may not have a legacy code problem and therefore be able to build out the program at a much smaller scale.

By identifying a small group of security criteria, baking them into software development technologies and processes, and then scaling that broadly across the entire company, organizations can begin to prioritize specific security outcomes that can be achieved without unduly burdening programmers and product managers. Those outcomes can then inform evaluation criteria and metrics used to track progress and adjust course over time.

Market Incentives, Disincentives, and Corporate Culture

Security by design is not just a technical challenge. There needs to be corporate buy-in that security is worth the allocation of resources. This is because of the many reasons the market does not already prioritize design security: The market does not offer enough of an incentive to businesses to invest in cybersecurity, there are several other principles and goals that need to be taken into account (such as software's ease of use and interoperability with third-party products), engineers are not properly trained on the importance of security, and there's often little to no market or regulatory consequence for pushing unsafe products. All these factors shape a company's corporate culture and the role secure software has to play. And even when a company has developed a policy and has procedures in place, there is the potential for a mismatch between policy and practice. We wanted to understand how our interviewees have adopted and encouraged security by design internally.

The National Cybersecurity Strategy's objective of shifting responsibility from individuals and small organizations to software manufacturers assumes that there are market failures that need to be addressed by government action. It states that "[t]oday's marketplace insufficiently rewards—and often disadvantages—the owners and operators of critical infrastructure who invest in proactive measures to prevent or mitigate the effects of cyber incidents."[29] There was broad consensus during our interviews that the demand for security is limited. The biggest disincentive was the rush to market. That, paired with the focus on shipping MVPs (discussed in the previous section), is a significant barrier to a security-by-design approach over a bolt-on approach. The latter approach allows the company to reach the market sooner, without the delays that testing and incorporating security features would cause.

The trade-off between priorities was another common theme throughout our interviews. Some of the other principles that individuals mentioned include privacy, interoperability, reliability,

[29] The White House, *National Cybersecurity Strategy*.

performance, backward compatibility (making sure that new software can function and communicate with older versions), resiliency, and usability. It was clear that ensuring the usability of the product is a priority for both Microsoft and Google. A product that is not user friendly is not long bound for this world, regardless of how secure it may be. And a product that is not compatible with other products becomes less useful.

A company's internal decision-making will be shaped by the market forces and the resources available to its team to deliver the product. Unfortunately, so far the market has not put a premium on security. That security is not top of mind is reflected in the skill set that engineers are expected to have when joining the workforce.[30] Our interviewee from Schneider Electric considered investing in cybersecurity training to be the most effective way to move the needle in promoting a security mindset among engineers.

This brings us to the need for a corporate culture that values security and encourages all its teams to center it. CISA calls this "leading from the top," and it is the third principle the agency espouses in its white paper on security by design.[31] In the explanation of the principle, CISA argues that security is not simply a technical issue but, rather, needs to be first embraced as a business priority. Both Google and Microsoft spoke with us about their understanding of security by design as a constant choice, a process of iteration. At Google, the "well-lit path" benefits from integrating threat intelligence analysis and attack behavior into the development teams. At Microsoft, the Security Development Lifecycle is often adjusted to respond to changes in technology and threats. The expert from Schneider Electric described it as a constantly moving goal post.

An interesting facet of the challenge of adopting security-by-design principles is that the resources available to different-sized companies are fundamentally different. We heard from some experts that most of the concerns about security stem from the practices of less mature organizations, rather than those of the big software developers. A startup or a small or medium enterprise is not only more pressed to launch a product rapidly but will also have to rely during development on external tools, over which it has limited control. It might be on this point that some of the differences in understanding of security by design become most salient. The experts from Google focused on the high cost of secure infrastructure, nothing that most companies don't have the necessary resources to produce it. By contrast, our interviewees from CISA were more skeptical of the idea that security by design depends on size. While some investments are certainly expensive, they argued, there is plenty of low hanging fruit that would harden a smaller organization's security.

The conversation about size and the ability to implement a secure development ecosystem led to a discussion regarding responsibility. Experts from Google argued that bigger companies

[30] Jack Cable, "We Must Consider Software Developers a Key Part of the Cybersecurity Workforce," Cybersecurity and Infrastructure Security Agency, January 2024, https://www.cisa.gov/news-events/news/we-must-consider-software-developers-key-part-cybersecurity-workforce.
[31] Cybersecurity and Infrastructure Security Agency, "Shifting the Balance of Cybersecurity Risk."

should bear most of the burden for security outcomes and "have no excuse not to be on the bleeding edge" of security. Microsoft and Schneider Electric shared the different ways in which their companies try to support a security mindset in their dealings with third-party vendors.

We would be remiss when writing of corporate culture—its effects on security outcomes and how size affects organizations—if we did not mention the Cyber Safety Review Board's review of the Microsoft Exchange Online intrusion in the summer of 2023 and the aftermath of the report. One of the board's findings was that "Microsoft's security culture was inadequate and requires an overhaul, particularly in light of the company's centrality in the technology ecosystem and the level of trust customers place in the company to protect their data and operations."[32] While Microsoft has challenged this characterization of its security culture, the recommendation has not gone unheeded. A leaked memo from Microsoft CEO Satya Nadella urged Microsoft employees to prioritize security, even at the expense of other priorities.[33] At a hearing in front of the House Homeland Security Committee, Microsoft President Brad Smith offered a *mea culpa* and acknowledged the company should have done better.[34] Part of revamping the company's security initiative includes "changing our engineering processes, how we are integrating security by design, how we are changing the way employees review themselves, how we elevate these issues and reward people for finding, reporting and helping to fix problems."[35]

Since the intrusion took place, Microsoft has launched a new Secure Future Initiative—anchored in the three principles of secure by design, secure by default, and secure operations. The differentiation in this new initiative between the terms "security by design" and "security by default" marks an interesting departure from the company's posture during our conversation with the experts at Microsoft. In that interview, those from Microsoft had expressed slight skepticism at the idea of differentiating the concepts of "security by design" from "security by default," as we described earlier.[36]

CONCLUSION

Is there a conceptual alignment among different companies and governments about security by design? At a high altitude, we feel confident that there is, indeed, a relatively common understanding of what the term involves. Among other things, it refers to making cybersecurity

[32] Cybersecurity and Infrastructure Security Agency, "Cyber Safety Review Board Releases Report on Microsoft Online Exchange Incident from Summer 2023," March 20, 2024, https://www.cisa.gov/resources-tools/resources/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer-2023.
[33] Tom Warren, "Read Satya Nadella's Microsoft Memo on Putting Security First," *The Verge*, May 3, 2024, https://www.theverge.com/24148033/satya-nadella-microsoft-security-memo.
[34] House Committee on Homeland Security, "Assessing Microsoft Corporation's Cybersecurity Shortfalls & the Implications for Homeland Security," June 13, 2024, https://www.youtube.com/watch?v=kB2GCmasH4c.
[35] Gabby Miller, "TRANSCRIPT: House Committee Hearing to Assess Microsoft's Cybersecurity Shortfalls," *Tech Policy Press,* June 15, 2024, https://www.techpolicy.press/transcript-house-of-homeland-security-hearing-on-assessing-microsofts-cybersecurity-shortfalls/.
[36] Microsoft, "Microsoft Secure Future Initiative," https://www.microsoft.com/en-us/microsoft-cloud/resources/secure-future-initiative.

a core component of software design and deployment processes, leveraging technology tools and creating company policies to minimize friction for developers and to scale up security, and focusing on processes, rather than a single, specific end state. Simultaneously, there is plenty of variance at the granular level—regarding the specific technical systems, policies, and plans implemented by different software companies.

Since we started working on this paper, a lot has happened under the umbrella of security by design in the policy world. CISA has certainly been successful in creating a buzz around the term, which is being adopted widely by companies. CISA has also issued a voluntary pledge for security by design.[37] The scope (for unstated reasons) does not include "[p]hysical products such as [Internet of Things (IoT)] devices and consumer products," addressing one of the concerns around clarity of scope for the initiative we identified earlier—and at the same time introducing a gap between the definition and the billions of IoT devices deployed around the world in consumer, commercial, and government settings.

Looking forward, open research questions on the concepts of and possible approaches to security by design include:

- How will the "security by design" concept mature over time with developments such as the publication of additional CISA guidance documents and design principles, the creation of new cybersecurity regulations outside the U.S., and cyber incident reviews such as the U.S. Cyber Safety Review Board's report on the Microsoft Exchange hack and company security culture?
- Are "security by design" and "security by default" sufficiently differentiated and distinct for CISA to continue using both terms? Or is the presence of both terms simply creating unnecessary confusion?
- What dynamics and trade-offs could exist between organizations scaling up security across their development teams and product areas, and organizations remaining flexible to quickly change their development and security processes as threats evolve?
- How should the open-source software community mature and implement the concept of security by design? Or is security by design not the right framing for baking in security improvements outside of a corporate software vendor context?
- Are the principles of security by design substantial enough that they can be translated into articulable standards, which can then be imposed and applied by legislators, regulators, or the courts?
- Will there be sufficient alignment between the concept of security by design—as promoted by CISA and partner agencies in other countries—and how each country adopts these principles?

[37] Cybersecurity and Infrastructure Security Agency, "Secure by Design Pledge," https://www.cisa.gov/securebydesign/pledge.