Foreign Affairs: Stop Passing the Buck on Cybersecurity

Why Companies Must Build Safety Into Tech Products

By: CISA Director Jen Easterly and Executive Assistant Director Eric Goldstein

Date: February 1, 2023

Despite a global multibillion-dollar cybersecurity industry, the threat from malicious cyber-activity, from both criminal and state actors, continues to grow. While many cyber incidents are never reported by their victims, Verizon's 2022 Data Breach Investigations Report noted that ransomware attacks rose 13 percent that year—more than the past five years combined. These breaches included attacks that threatened public health and safety, with several hospitals across the United States forced to cancel surgeries and divert patients because they were locked out of their systems.

Over the past decade, adversaries of the United States have developed increasingly sophisticated offensive cyber-capabilities. As cybersecurity expert Dmitri Alperovitch has argued, "We don't have a cyber problem. We have a Russia, China, Iran, North Korea problem." Although the focus on malicious actors—whether nation-states or criminals—is important, cyber-intrusions are a symptom rather than a cause of the continued vulnerability of U.S. technology.

What the United States faces is less a cyber problem than a broader technology and culture problem. The incentives for developing and selling technology have eclipsed customer safety in importance—a trend that is not unique to software and hardware industries but one that has particularly pernicious effects because of the ubiquity of these technologies. As Americans have integrated technology into nearly every facet of their lives, they have unwittingly come to accept that it is normal for new software and devices to be indefensible by design. They accept products that are released to market with dozens, hundreds, or even thousands of defects. They accept that the cybersecurity burden falls disproportionately on consumers and small organizations, which are often least aware of the threat and least capable of protecting themselves.

Widespread use of unsafe technologies is compounded by a common practice in many organizations and companies of relegating cybersecurity to the "IT people" or to a chief information security officer. They are given this responsibility, but not the resources, influence, or accountability to ensure that security is appropriately prioritized against cost, performance, speed to market, and new features. When cybersecurity is considered a niche issue, rather than a foundational business risk, organizations are not motivated to be part of a broader solution. As a result, victims of cyber-intrusions too rarely share information about malicious activity with the government or with other firms, allowing adversaries to reuse the same techniques to compromise countless victims.

Americans need a new model, one they can trust to ensure the safety and integrity of the technology that they use every hour of every day. Problems should be fixed at the earliest possible stage—when technology is designed rather than when it is being used. Under this new model, cybersecurity would ultimately be the responsibility of every CEO and every board. Collaboration would be a prerequisite to self-preservation. Such a culture shift requires the recognition that a cyberthreat to one organization is a threat to all organizations. To get there, incentives need to favor long-term investments in the safety and resilience of the cyberspace ecosystem, and the responsibility for defending that ecosystem must be redistributed to favor those most capable and best positioned to do so, as U.S. National Cyber Director Chris Inglis argued in Foreign Affairs last year.

Government can smooth the way by making clear its expectations that technology is designed and built with safety as a top priority, by advocating that cybersecurity be considered a CEO-level business risk, by providing opportunities for entities to share cyberthreat information, by holding itself accountable for being transparent and adding value, and by ensuring that regulatory frameworks encourage companies to comply. The Cybersecurity and Infrastructure Security Agency (CISA), established by the U.S. Congress in 2018 to serve as the country's cyberdefense agency, is focused on these goals. But government cannot solve the problem. Technology manufacturers need to take responsibility for the security outcomes of their customers as a fundamental issue of safety; otherwise, the critical infrastructure of the United States, its communities, and its way of life will remain at untenable risk.

UNSAFE AT ANY CPU SPEED

This is not the first time that American industry has made safety a secondary concern. For the first half of the twentieth century, conventional wisdom held that automotive accidents were the fault of bad drivers. Similarly, today, if a company suffers a cybersecurity breach, the company itself is blamed if it did not patch a known vulnerability. Such an approach neglects to question why the vendor that produced the technology needed to issue so many patches in the first place or why failure to implement a patch allowed a damaging breach to occur.

Any car manufactured today has an array of standard safety features—seatbelts, airbags, antilock brakes, and so on. No one would think of purchasing a car that did not have seatbelts or airbags, nor would anyone pay extra to have these basic security elements installed. With cars, however, customers can see for themselves if the proper safety features are included. That is not the case with insecure devices or software. The consequences of using unsafe technology are also harder to measure—school districts are shut down, food supply chains disrupted, chemicals manipulated at water treatment plants. The readily apparent safety issues with cars also led to a simple solution: government action to compel adoption of specific security measures with proven better outcomes. Whether automobiles or other sectors such as aviation or medical devices, it took crisis to force people to focus on the need for additional safety measures. Such a safety crisis is already here in the cyber-realm, and now is the time to address it.

Consumers and businesses alike expect that cars and other products they purchase from reputable providers will not carry risk of harm. The same should be true of technology products. This expectation requires a fundamental shift of responsibility. Technology providers and software developers must take ownership of their customers' security outcomes rather than treating each product as if it carries an implicit caveat emptor. To achieve this, every technology provider must begin by creating products that are both "secure by default" and "secure by design."

These concepts are related but distinct. Secure-by-default products have strong security features—akin to seatbelts and airbags—at the time of purchase, without additional costs. Strong security should be a standard feature of virtually every technology product, particularly those that underpin critical infrastructure such as energy, water, transportation, communications, and emergency services. Attributes of strong security by default will evolve over time, but at a minimum, software sellers must include in their basic pricing features that secure a user's identity, gather evidence of potential intrusions, and control access to sensitive information rather than as added expensive options.

A cyberthreat to one organization is a threat to all organizations.

Equally important is technology that is secure by design. This is the 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. Achieving this outcome will require radical changes in how technology is produced, including in the code used to develop software. Flaws often wind up in technology products because creators rush to release them to customers and are often more focused on feature expansion than security. This places the burden of security on millions of organizations and individual end users, who are the least prepared to deflect cyberthreats.

It will not be easy to make these changes and convince companies to build and deliver more secure products, but the U.S. government can start by defining specific attributes of technology products that are secure by default and secure by design. It can also call out companies that continue to introduce insecurity into the fabric of the U.S. economy, and it can encourage companies that are making progress. Indeed, a number of technology providers, including Google, Amazon, and Salesforce, are moving in this direction, providing strong security measures by default for their customers and introducing innovative advances toward security by design.

Every organization should demand transparency from its technology providers about whether they have adopted strong safety practices. One way to push technology companies to adopt such practices is for every organization that buys technology to include safety requirements as basic, easily understood criteria before procurement or use. The Biden administration has taken important steps toward this goal in establishing software security requirements for federal contractors. It is also advocating for development and voluntary adoption of labels that would clearly and simply convey basic security information about Internet-connected consumer devices, such as baby monitors and webcams.

Building on this progress will require U.S. agencies to impose increasingly stringent secure-by-default and secure-by-design requirements in the federal procurement process, which will help prompt market changes toward creating a safer cyberspace ecosystem. U.S. President Joe Biden's 2021 cybersecurity executive order is spurring these efforts, but change must come from all angles: organizations across sectors should commit to requiring strong security practices when purchasing or upgrading technology, and technology providers should commit to taking responsibility for the security outcomes of their customers. Every technology provider must consider it a duty to ensure that its products are safe for use and to warn customers when that is not the case.

Such requirements may pose challenges for smaller technology companies and new entrants to the market. To ensure that innovative and disruptive companies can thrive in an environment where heightened security investment is the norm, development of stronger security practices must focus on outcomes rather than on prescriptive, doctrinaire requirements, allowing new market entrants to introduce creative ideas in which security is a positive differentiator rather than a cost.

THE BUCK STOPS HERE

Although the transition to safer technology is a longer-term endeavor, every organization can take steps today that will improve its cybersecurity. First and foremost, in every business, the responsibility for cybersecurity needs to be elevated from the IT department to the board, the CEO, and the senior executive level.

The trends here are encouraging. In a National Association of Corporate Directors 2019-2020 survey, 79 percent of public company directors indicated that their board's understanding of cyber risk had significantly improved over the past two years. The same study, however, found that only 64 percent believed that their board's understanding of cyber risk was strong enough that they could provide effective oversight.

To improve those numbers, shareholders must make CEOs and board members personally accountable for managing cyber risk. This is largely a cultural change: where cybersecurity is considered a niche IT issue, it is intuitive for accountability to fall on the chief information security officer; when cybersecurity is considered a core business risk, it will be owned by the CEO and the board.

Board members have special power to develop a culture of corporate cyber responsibility. They should ensure that they and other senior executives are well educated on cyber risk, that cybersecurity considerations are appropriately prioritized in every business and technology decision, and that decisions to accept cyber risk are scrutinized and revisited often. They should ensure that the thresholds for reporting potential malicious activity to senior management are not set too high; "near misses" should be reported along with intrusion attempts that succeed. They should ensure that adequate long-term security investments are available to address the safety consequences of antiquated technology. Most important, board members should see that chief information security officers have the influence and resources necessary to make essential decisions on cybersecurity. Decisions to prioritize profits over security must be made transparently, with clear ownership by CEOs and boards. The practice of blaming the chief information security officer or the IT department for organizational failings must end.

Key to advancing corporate cyber responsibility as a matter of good governance is the development of a common set of practices that businesses can use to determine their exposure to cybersecurity risk. The Cybersecurity Framework developed by the National Institute for Standards and Technology is considered an exemplar for building and evolving a firm's cybersecurity program. Many organizations, however—particularly small and medium businesses that comprise the supply chains of larger entities—find it difficult to meet those standards, often because they lack resources. To address this problem, the Cybersecurity Performance Goals, released by CISA in late 2022 in partnership with NIST, can help businesses determine which security measures most needed to reduce risk. Encouragingly, rating agencies have begun incorporating cybersecurity into their models for assessing creditworthiness, action that can further inspire companies to embrace cyber responsibility as a matter of institutional governance.

ALL TOGETHER NOW

Sustainable cybersecurity will also require rethinking how governments and industries interact with one another. When most companies detect a cyber-intrusion, too often their default response is: call the lawyers, bring in an incident response firm, and share information only to the minimum extent required. They often neglect to report cyber-intrusions to the government for fear of regulatory liability and reputational damage. In today's highly connected world, this is a race to the bottom.

General Paul Nakasone, head of the U.S. Cyber Command, wrote a few years ago about the doctrine of persistent engagement, in which U.S. forces compete with foreign adversaries on a proactive and recurring basis. From a defensive perspective, the U.S. government must instead move to a posture of persistent collaboration. Such a culture shift requires sharing becoming the default response, where

information about malicious activity, including intrusions, is presumed necessary for the common good and urgently shared between industry and government. Government and industry must work together with reciprocal expectations of transparency and value, where industry does not have to be concerned about punitive sanction. Finally, interactions between the government and the private sector should be frictionless, so that collaboration emphasizes scale, shared platforms, and data-driven analysis.

In 2021, Congress established the Joint Cyber Defense Collaborative to advance this posture by creating one U.S. government platform for cyberdefense planning and operations. It is still early days for the JCDC, but since its creation, for the first time, the government, the private sector, and U.S. international partners came together to develop joint cyberdefense plans and enable real-time information sharing on issues from the U.S. response to Russia's criminal invasion of Ukraine to efforts to help safeguard the 2022 midterm elections. Over the coming year, CISA will continue these efforts, which will include building resilience to ransomware attacks in coordination with the Joint Ransomware Task Force and the International Counter Ransomware Initiative and will address the root causes of incidents as identified by the Cyber Safety Review Board. As the JCDC continues to evolve, CISA and government partners will strive to uphold their end of the bargain by being transparent, responsive, and adding value, but the JCDC will only succeed if partners across the country, in every sector of the economy, join the effort.

WITH A LITTLE HELP FROM MY FRIENDS

Even as the cybersecurity community takes steps to build a sustainable approach to cybersecurity through the widespread adoption of safe technology, corporate cyber responsibility, and persistent collaboration, it must continue to help individuals and small businesses protect themselves, recognizing that everyone has a responsibility to maintain a safe cyberspace environment, just as drivers still bear responsibility for driving safely, even with seatbelts and airbags are included as standard features.

The philanthropist Craig Newmark has recently called for focused investment in "cyber-civil defense" to raise public awareness of online safety. Along similar lines, CISA has been engaged in building cybersecurity into K–12 curricula; working with "target rich, cyber poor" entities such as small businesses, school districts, water facilities, hospitals, and local election offices to ensure they have the tools needed to improve their cybersecurity; and leading a nationwide cyber hygiene campaign to help all Americans from "K through Gray" stay safe online by taking simple steps such as turning on multifactor authentication. The ultimate goal, however, is to dramatically improve product safety, so technology customers rarely need to secure their systems on their own. Although some safety measures will become as easy to use as a seatbelt, most organizations should be protected before they even "buckle up." This basic level of security will not be achieved under today's failing model. It is time for a new approach, and if the government and the private sector can build trust and work together, cyberspace can become safer for everyone.