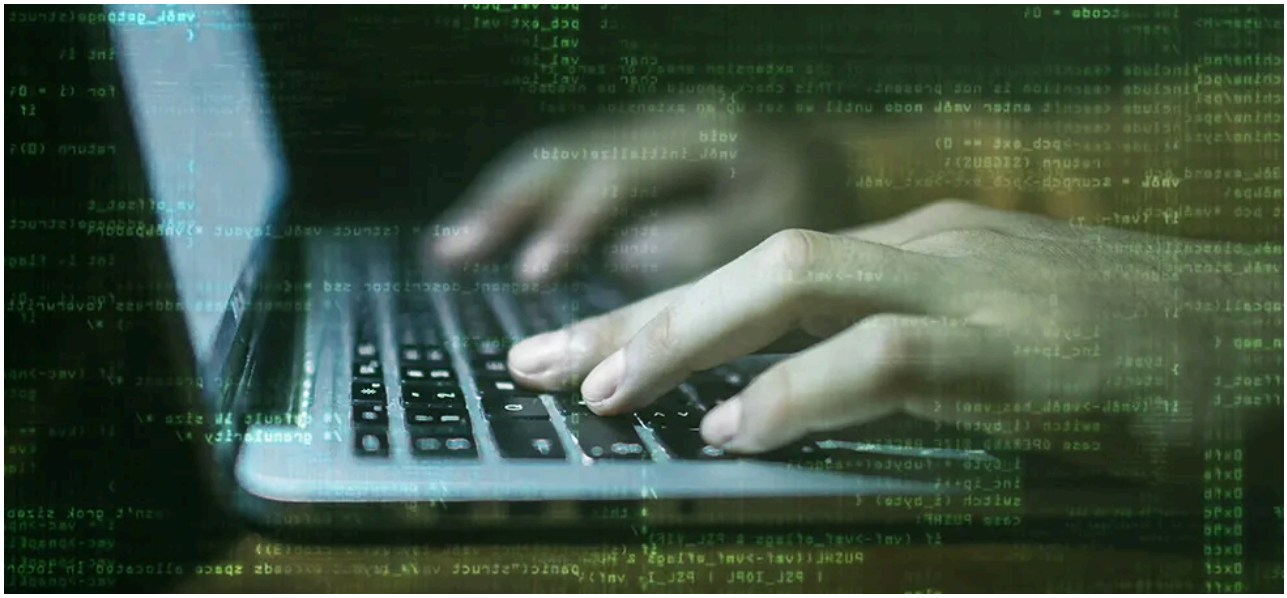
OPINION > CYBERSECURITY

THE VIEWS EXPRESSED BY CONTRIBUTORS ARE THEIR OWN AND NOT THE VIEW OF THE HILL

‘Software Bill of Materials’ — Not just good for security, good for business

BY SHANNON LANTZY AND KELLY ROZUMALSKI, OPINION CONTRIBUTORS - 07/26/21 11:00 AM ET



Getty Images

President Biden's May 2021 cybersecurity executive order raises the bar for product security with a mandate requiring — among other provisions — a "Software Bill of Materials" (SBOM) for all software sold to the federal government. This executive order formally recognizes that national security requires digital ecosystem defense. While this is a good first step, the U.S. should go further and mandate that all digital products be sold with an SBOM.

We require ingredient lists for our food packages, so why not the same for our digital devices?

Put simply, an SBOM is a list of software components in a digital product. Universally mandated SBOMs would empower all players of our digital ecosystem to reduce risk and increase security and competition. While many improvements are still needed to increase product security, a universal SBOM mandate is one step with the power to incentivize securing software. Product vendors should embrace this inevitable measure not just because it's good for security, but also because it's good for business.

SBOMs increase transparency for consumers

Universally mandated SBOMs would provide buyers new levels of transparency into what they are purchasing, which in turn helps consumers to better prioritize their security needs. While companies should always work toward maximizing their network security, they may need to make security tradeoffs due to limited IT resources, interoperability of connected systems, and their own risk assessments. To prioritize the most critical risk reductions on

For example, SweynTooth is a family of vulnerabilities in Bluetooth low-energy (BLE) communications that can bypass security features or crash the system. If a BLE-enabled product is used in patient care or pipeline operations, patching should be a priority; whereas, if used in a small test environment not connected to a network, it can wait. To make that determination, a company needs to know which products have BLE, and SBOMs would supply that information.

Universally mandated SBOMs would also provide consumers the transparency they need to comparison shop on the vulnerability of software components. Currently, consumers cannot determine what software is included with the products they buy. As a list of all components used to make a software product, an SBOM would reveal which open source or proprietary code objects are embedded in the software. Knowing this would allow end users to better understand how bad actors might target new software by attacking old code elements that harbor unpatched vulnerabilities.

SBOMs increase return on investment of securing software

In addition to the consumer transparency benefits of mandated SBOMs, they would also allow software makers to demonstrate to customers the return on investment (ROI) of security assets. Currently it's difficult to claim one product is more secure than another. According to a recent piece in The Economist, some say cyber is like magic amulets and the "market for lemons" — it's hard to prove to customers that a product is secure. By mandating disclosure of the software supply chain, software vendors could compete on the security features of their products. More secure components and patching programs would become a competitive differentiator.

Product offerings that are already secure-by-design will be able to command a premium price because consumers will be able to compare SBOMs.

Products with inherently less patchable components will also benefit. A universal SBOM mandate will make it easy to spot vulnerabilities, creating market risk for lagging products; firms will be forced to reengineer the products before getting hacked. While this seems like a new cost to the laggards, it's really just a transfer of future risk to a current cost of reengineering. The key to a universal mandate is that all laggards will incur this cost at roughly the same time, thereby not losing a competitive edge.

The promise of increased security and reduced risk will not be realized by SBOM mandates alone. Tooling and putting this mandate in practice will be required to realize the full power of the SBOM.

We should embrace an SBOM mandate — not only as a step forward for securing our national infrastructure and economy, but as a new opportunity to innovate, compete, and increase the ROI of building secure software by design.

Dr. Shannon Lantzy is chief scientist and regulatory innovation leader at Booz Allen Hamilton. Kelly Rozumalski is vice president at Booz Allen Hamilton and leader of the firm's secure connected health practice.

TAGS COMPUTER SECURITY CYBER HACKING CYBER VULNERABILITY CYBERSECURITY DATA SECURITY JOE BIDEN PATCH SOFTWARE BILL OF MATERIALS SOFTWARE DEVELOPMENT SUPPLY CHAIN MANAGEMENT