Cybersecurity Risks in Software Supply Chains

A Medical Device Perspective

Robert L Schwartz
February 2025

Abstract

Supply chains are the lifeblood of commerce, enabling the flow of goods between economic agents domestically and abroad. They are increasingly global, accommodating cross-border trade amongst sovereign nations and their business entities. As illustrated during the global pandemic, supply chain disruptions can take the form of supply shocks, which can have a substantial impact on the economy. Despite their lack of press coverage, software supply chains are equally as important and, in some cases, more complex and fragile than traditional physical goods supply chains. As the proliferation of software persists at a rapid rate, industry practitioners have continued to critically analyze the cybersecurity of software supply chains to promote greater protections, internal controls, and resiliency alongside advancing technology. Through multistakeholder efforts led by the National Telecommunications and Information Administration (NTIA), Cybersecurity and Infrastructure Security Agency (CISA), regulators, and trade groups, a cybersecurity framework has been in development to minimize supply chain risk. This framework is especially relevant as it relates to industries of heightened importance, such as healthcare. Congressional legislators and regulators at the FDA have instituted meaningful new requirements for medical device manufacturers seeking pre-market clearance, an effort designed to minimize vulnerabilities in critical healthcare infrastructure and prioritize patient safety. These efforts have been well received, providing a strong value proposition for cybersecurity SaaS providers who can enable hospital IT professionals and asset managers to better secure their networks and device inventory.

The Role of Traditional Supply Chains

According to the U.S. Bureau of Economic Analysis, total domestic consumption of physical goods – both durable and non-durable – exceeded $6.2tn for the calendar year ending December 2024 [1]. Supplying over $6tn of physical goods is no small challenge. Domestic and international suppliers, manufacturers, wholesalers, and retailers must work in a coordinated ensemble to ensure the right products are delivered in the right quantities, to the right location, at the right time, with the right price, and in the right quality. As one can imagine, the coordination of so many independent but interdependent stakeholders is risky business, with the entire supply chain being only as strong as its weakest link. Business owners and consumers learned this lesson first-hand during the COVID-19 pandemic, as global supply chain disruptions led to goods shortages and higher prices charged to consumers.

Goods Supply Chains

In the world of manufacturing, companies that process and assemble finished products sold into the goods market are routinely concerned about their physical supply chains for intermediate inputs used in the production process. Vulnerabilities at any stage of the supply chain can result in serious detrimental business outcomes. For example, if one upstream raw materials supplier is the cause of shipment delays or an intermediate goods defect, the midstream manufacturing company will be

subject to throughput interruptions, idle capacity, and an overall decline in manufacturing output, leaving downstream wholesalers and retailers empty-handed. Needless to say, all of which manifests itself in the form of lower supply, lower revenue, higher costs, and lower corporate profits. It is no surprise that an entire labor market of supply chain managers has long been a staple in the manufacturing industry. Managers devote their time to arranging, monitoring, and ensuring optimized performance of their manufacturing supply chains. Toyota is a prime example, having led the adoption of the Just-in-Time (JIT) inventory management system. This often involves frequent touchpoints with entities all along the value chain and strategic management of supplier relationships.

Software Supply Chains

Supply chain concerns are also shared by those in the business of delivering intangible goods, such as software, in B2B and B2C transactions. Unlike in the world of physical goods, where supply chains are traditionally a linear pipeline from raw materials to end products, software supply chains are characterized by a complex web of software components, each typically dependent on its own web of other software components. This is because modern software development and usage are reliant on third-party code. Each of these third-party software components dynamically changes as each provider in the supply chain releases new versions, discontinues support of older versions, modifies software requirements and dependencies, and introduces new security enhancements and, potentially, vulnerabilities. Making matters worse, the commercial relationships between every member of the software supply chain are less direct and thus, weaker than those observed in a physical goods supply chain.

Scope of the Problem

Clearly, software development and distribution carries its own flavor of supply chain risks. The relevant question is, does the complexity and nature of software supply chains pose a significant enough risk – both in terms of scope and magnitude of impact – that it should be a concern to industry participants? I'd argue yes. Most software that is developed relies heavily on third-party frameworks, packages, and public libraries of code. On the one hand, third-party or open-source software components can speed up the development process, promoting efficiency gains and minimizing the amount of time necessary to get good software into the hands of end users. Further, assuming best practices are followed, open-source libraries can enable cross-platform compatibility and reduce redundancies. However, some disadvantages are worth noting, especially given they are the primary factor driving supply chain risk. First, by introducing third-party code, you effectively limit your control over aspects of the codebase. Think of it like outsourcing part of the development process where you don't have full oversight and control. Second, each third-party component has the potential to undergo future upgrades and/or modifications to its codebase and dependencies, leading to greater complexity of the software composition. While the proliferation of shared software components in the public domain is a major benefit to society, it undoubtedly introduces significant cybersecurity risks for both software providers and their customers.

Cybersecurity Risks in Software Supply Chains

The problem faced by end users of software is that they traditionally have limited to no visibility into the underlying components or supply chain being employed. For contrast, consider grocery stores that are notified by a product supplier that their meat is being recalled due to a health safety concern.

Grocery stores across the country can quickly and effectively pull those specific items off the shelves. From a software perspective, if an open-source or third-party licensed piece of code used in the software itself becomes infected with a cybersecurity threat, the end user of the software may lack the necessary visibility into the software supply chain to know their level of exposure. A practical example of this is the healthcare industry. Ransomware distributors have been targeting healthcare providers for a number of years through software vulnerabilities within durable medical equipment devices and other critical healthcare infrastructure. The canonical example is WannaCry, which had a significant detrimental impact on hospital systems. Cybersecurity vulnerabilities embedded in healthcare infrastructure pose a substantial risk to patient safety and the lives of innocent civilians. If hospitals cannot use their digital systems, often the best-case scenario is that a facility must move patients elsewhere, redirecting them to neighboring organizations. If people cannot get the medical care they require quickly, the cost can be the difference between life and death. It is therefore critical that hospital administrators have visibility into the composition of software and hardware being deployed across their organization.

The Case for Software Transparency

Recognizing the legitimate need to mitigate cybersecurity risks imposed by software vulnerabilities that are hidden by a lack of transparency in software supply chains, several industry stakeholders have stepped up to address the issue. The National Telecommunications and Information Administration (NTIA) has been a leader in a multistakeholder process surrounding the promotion of software transparency. Through their efforts, the NTIA and industry stakeholders learned that many organizations have already been confronted with this issue and have made attempts to mitigate and manage associated risks through custom, organization-specific solutions. Therefore, it was prudent to document these existing solutions, taking note of the advantages and disadvantages of different methodologies. Further, it became clear that promoting widescale adoption of any solution should be grounded in a well-articulated set of guiding principles, frameworks, and tools. For example, one leading mechanism that has become essential to enabling supply chain transparency is the software bill of materials (SBOM).

Introducing the Software Bill of Materials (SBOM)

SBOMs are a list of ingredients for software and are valuable to software developers (producers), software purchasers, and software operators. For example, SBOMs enable producers to communicate the key components of their software to prospective buyers or licensees. For customers, SBOMs provide visibility into software composition, which is essential for mapping out potential cybersecurity risks were that vendor to be selected and software deployed. Finally, software operators can maintain awareness of software components so that if vulnerabilities arise, they can quickly assess their exposure and take corrective action. Given their multi-dimensional user base, the NTIA has worked to improve awareness and adoption of SBOMs, while collaborating with industry practitioners to enhance and solidify SBOM best practices. For example, the NTIA has recommended a minimum set of elements that every SBOM should contain. These elements include: (1) the name of the software supplier, (2) the name of the software components, (3) the version of the components, (4) other unique identifiers, (5) dependency relationship(s), (6) the author of the SBOM, and (7) a timestamp. Further, it is equally important that SBOMs adhere to one of the industry-accepted machine-readable formats, which include CycloneDX, SPDX, or SWID. By adhering to one of these formats, SBOMs can be generated, stored, and consumed in a scalable and

automated fashion. This will be especially important as SBOM clearinghouses and repositories become intermediaries between software producers and software consumers.

One final point worth noting is the level of depth SBOMs afford end users. At the very least, SBOMs should provide one degree of transparency into each software component and its dependencies. However, a more useful SBOM will offer many degrees of depth, allowing the end user the ability to see and track exposure to 'n'-level software components. The technical expression for this is "transitive dependency", which characterizes the fact that a single piece of software can be exposed to vulnerabilities in underlying software components 'n'-layers deep. Figure 1 and 2 illustrate how software can be exposed to threats nested in underlying software dependencies. For example, software 'A' is indirectly exposed to vulnerabilities in component 'C' by way of its exposure to component 'B'.

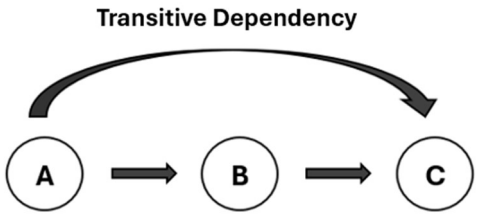

Figure 1

Transitive Dependency

Figure 2 illustrates that a cybersecurity threat in a piece of software can originate from a vulnerability three layers deep within the dependency tree. Thus, the value of an SBOM increases with the degrees of transparency into the underlying software components.

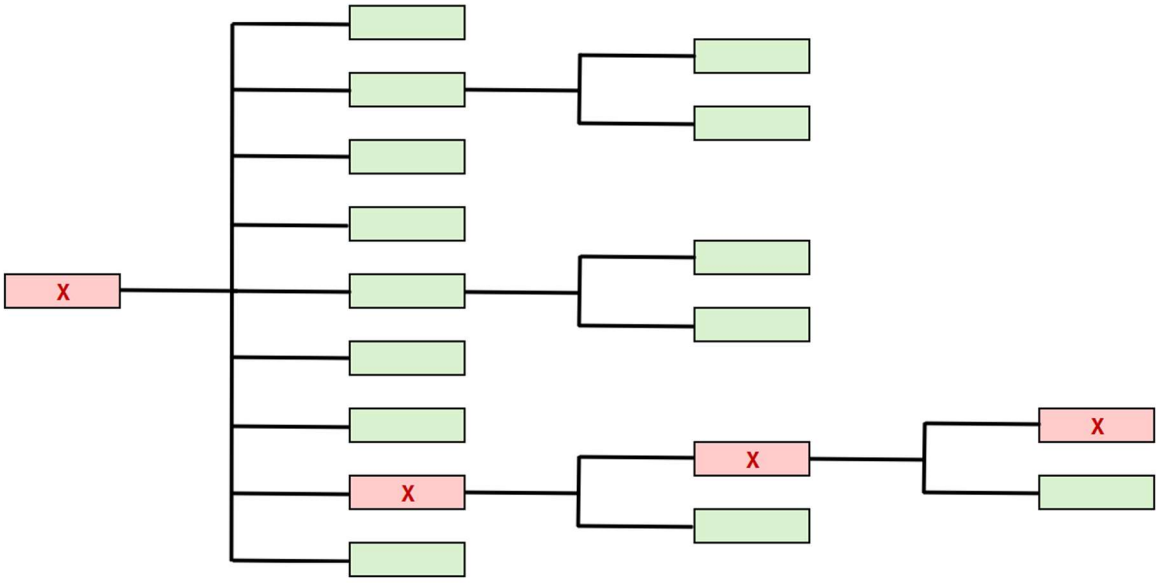

Figure 2

Regulatory and Statutory Requirements for Medical Devices

In parallel with the NTIA's programming efforts, legislators and regulators have worked to not only encourage the use of SBOMs but mandate their use in certain industries and under certain conditions. A terrific example is the Food and Drug Administration (FDA). Historically, for medical device manufacturers to be awarded go-to-market approval by the FDA, manufacturers were required to submit a "pre-market submission" to the FDA. The FDA would review the submission to ensure the manufacturer provided sufficient evidence and assurance of product safety and effectiveness. The FDA would assess whether the medical device manufacturer had adequately proven that the device was safe and effective and that it was expected to remain so throughout the entirety of its useful life. Historically, this was the safety and effectiveness mandate that device manufacturers had to meet or exceed for the FDA to feel comfortable that the device would not jeopardize patient safety. As FDA Senior Cyber Policy Advisor Jessica Wilkerson has publicly acknowledged, "if you do not have a cybersecure device, then you don't have a safe device" [2].

Despite success under this legacy process, the FDA determined they should explore a more thorough mechanism that further institutes strong cybersecurity controls. In doing so, the FDA worked with Congress on new legislation that expanded and improved cybersecurity requirements for medical devices. Their objective was to amend and extend existing laws, rather than introduce new regulations. Under that objective, the Consolidated Appropriations Act of 2023 was signed into law on December 29, 2022, which included the Food and Drug Omnibus Reform Act (FDORA) within it [3].

Section 3305 of the Omnibus Act made amendments to Section 524B of the existing Food, Drug, and Cosmetic (FD&C) Act [4]. The amendments, titled "Ensuring Cybersecurity of Medical Devices", modified the submission requirements for medical device manufacturers seeking pre-market FDA approval. More specifically, any future submissions for "cyber devices" (as defined in the Act) that are pursuing 510(k), de Novo, HDE, PDP, or PMA pathways to regulatory approval will require the inclusion of an SBOM, along with a comprehensive plan to monitor and address post-market cybersecurity vulnerabilities, which includes an obligation to disclose such vulnerabilities and provide patches for them in a timely and orderly fashion. If submissions are incomplete, insufficient, or lacking the newly required SBOMs, the FDA can "Refuse to Accept" (RTA) medical devices submitted for approval. The new requirements became effective 90 days after the signing of the Act on March 29, 2023, and are only applicable to future submissions. In other words, there is no retroactive application of the requirements for past medical devices already approved by the FDA.

The major evolution in medical device oversight is that cybersecurity requirements are no longer just regulatory, they are now statutory. To help explain the new requirements, the FDA offers guidance to medical device manufacturers seeking pre-market approval and post-market regulatory compliance. The FDA also provides guidance to other stakeholders, such as the suppliers of non-medical device software and hardware and healthcare organizations and their network administrators and IT personnel. Figure 3 provides examples of FDA guidance documents that industry stakeholders might find useful.

Name of Publication	Date of Publication	Description
Cybersecurity for Networked Medical Devices Containing Off-the-Shelf Software	1/14/2005	Provides guidance on how existing regulation, including the Quality System Regulation, sets cybersecurity requirements for medical devices.
Information for Healthcare Organizations: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf Software	2/8/2005	Provides additional information to healthcare network administrators enabling them to better collaborate with medical device manufacturers, especially regarding cybersecurity vulnerability assessments, cybersecurity planning, and patchwork.
Post-market Management of Cybersecurity in Medical Devices	12/28/2016	Guidance on how to maintain cybersecurity over the medical device's useful life, including the identification of cybersecurity threats and dissemination of patches.
Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions	9/27/2023	Guidance on how to secure go-to-market approval by proving to the FDA with sufficient evidence that a medical device is cybersecure and has appropriate systems in place.
Select Updates for the Premarket Cybersecurity Guidance: Section 524B of the FD&C Act	3/13/2024	Guidance updates related to amendments to Section 524B of the FD&C Act, such as a new SBOM requirement.

Figure 3

Overcoming Hurdles in SBOM Utilization

Despite the new statute and FDA mandates, there are still major difficulties faced by healthcare organizations on the receiving end of SBOMs. These difficulties arise from the fact that SBOMs are simply nested, hierarchical orientations of software components. SBOMs alone provide no list of existing or potential vulnerabilities. Rather, SBOMs need to be used as a data input for the end user to research and identify cybersecurity vulnerabilities. Unfortunately, many hospital technologists lack the necessary tools to convert SBOM data into useful and actionable information. However, this problem is not isolated to the healthcare sector. Under Executive Order 14028, efforts were made to require companies bidding for government contracts, whereby they would supply government agencies with software, to also provide SBOMs [5]. Agency personnel receiving these SBOMs face similar challenges to those faced by healthcare organizations. They lack the necessary tools to interpret and derive actionable insights from the data within SBOMs.

Fortunately, this problem serves as the value proposition for several cybersecurity technology companies that offer SBOM lifecycle management solutions to both the private and public sectors. These SaaS companies enable organizations to continually monitor, identify, and patch cybersecurity threats presented in their technology assets. Users can generate and import SBOMs, proactively identify vulnerabilities through cybersecurity risk assessments, prepare cybersecurity readiness audits, institute vulnerability alerts for real-time notification, conduct threat modeling, and implement vulnerability monitoring and management plans. For example, cybersecurity teams, compliance teams, continuity planners, and other technology professionals can utilize cybersecurity risk assessments to inform the development of incident response and vulnerability response procedures. Further, hospital technology staff can conduct drift analyses on their entire suite of medical devices. That is, by working with manufacturer field techs, they can easily compare "build SBOMs" with "deployed SBOMs", identifying any notable differences in the software components, packages, and libraries. These supply chain differences can be explored, and vulnerabilities can be patched.

Conclusion

Over the last several years, tremendous progress has been made to foster greater software supply chain transparency for the benefit of various stakeholders, especially private sector industries such as healthcare, automotive, and financial services. Multistakeholder working groups have enabled the creation of a uniform framework for the implementation of SBOMs in the broader cybersecurity ecosystem. Federal law has been amended, and regulatory requirements and oversight have become more robust. Where the need has presented itself, technology service providers have also stepped in to provide the necessary tools to effectively utilize SBOMs and improve technology asset management. As the world's technology evolves and new cybersecurity risks emerge, productive collaboration between the public sector, the private sector, regulators, and lawmakers will continue to be essential.

References

1. U.S. Bureau of Economic Analysis, Personal consumption expenditures: Goods [DGDSRC1Q027SBEA], retrieved from FRED, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/series/DGDSRC1Q027SBEA, February 20, 2025.
2. Vigilant Ops Inc., "Demystifying FDA's Pre Market Final Guidance." YouTube, 20 Jan. 2024, https://www.youtube.com/watch?v=8hFat9PbHpc.
3. Text - H.R.2617 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2023. Congress.gov, Library of Congress, 29 December 2022, https://www.congress.gov/bill/117th-congress/house-bill/2617/text
4. U.S. Congress. *United States Code: Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301-392 Suppl. 5*. 1934. Periodical. Retrieved from the Library of Congress, https://www.loc.gov/item/uscode1934-006021009
5. Office of the Federal Register, National Archives and Records Administration. 3 CFR 14028 - Executive Order 14028 of May 12, 2021. Improving the Nation's Cybersecurity. Office of the Federal Register, National Archives and Records Administration, https://www. https://www.govinfo.gov/app/details/CFR-2022-title3-vol1/CFR-2022-title3-vol1-eo14028/summary