VULNERABLE SOFTWARE SUPPLY CHAINS ARE A MULTI-BILLION DOLLAR PROBLEM

JUNIPER RESEARCH

Vulnerable Software Supply Chains Are a Multi-billion Dollar Problem

Juniper Research estimates that, without a paradigm shift in software supply chain cybersecurity management, cyberattacks targeting software supply chains will cost the world economy an estimated $80.6 billion in lost revenue and damages annually by 2026.

Contents

VULNERABLE SOFTWARE SUPPLY CHAINS ARE A MULTI-BILLION DOLLAR PROBLEM

1. Defining the Software Supply Chain & Its Cyber Risks

JUNIPER RESEARCH

1.1 Introduction to the Software Supply Chain

As with many things in today's world, supply chains have become more and more digital. From digital stockkeeping to the use of blockchain technology to record the movement of goods, supply chains are increasingly software based. The ability to connect everything from phones and cars to the Internet means that delivery and improvement of services can happen beyond the traditional point of sale and into the life of the product.

Modern businesses, governments, and individuals leverage an element of a software supply chain on a daily basis. Suppliers provide everything from connectivity to information, representing all the ingredients necessary to achieve the result that each organization or individual seeks in today's digital world.

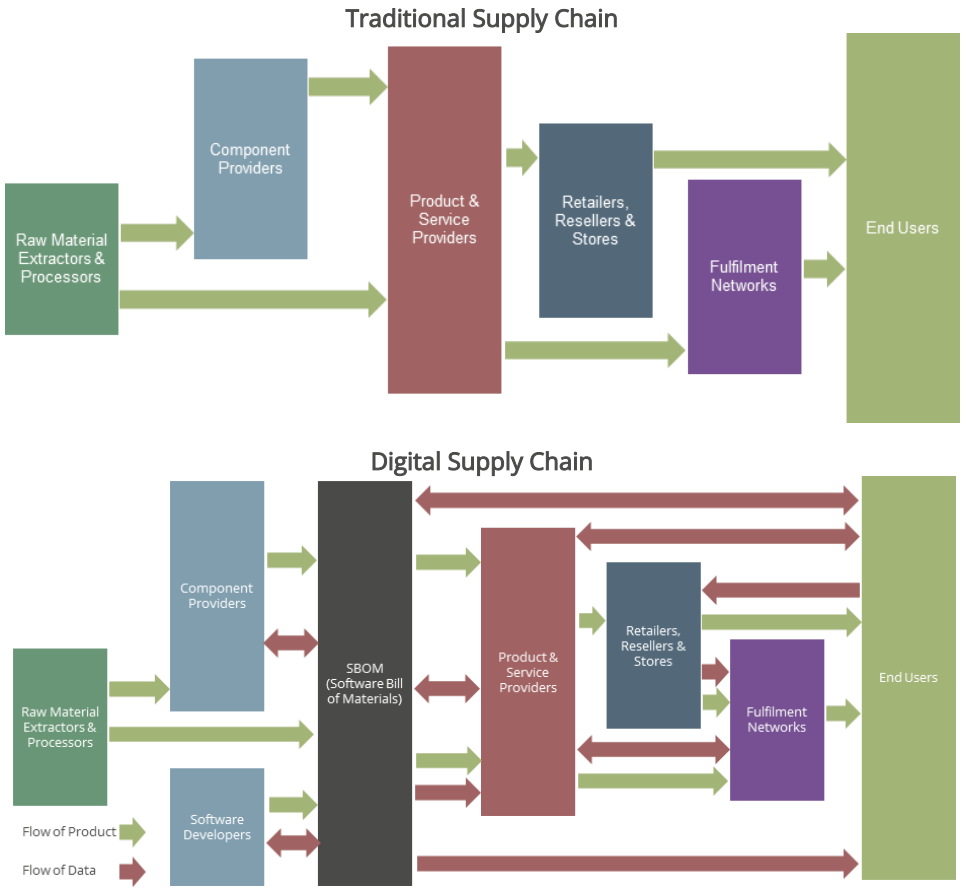
However, digitizing elements of the supply chain means that these areas are increasingly vulnerable to disruption from cyberattacks. In addition, the introduction of digital elements to both product delivery and the traditional supply chain means that areas not usually considered part of the supply chain now need to be assessed when companies are looking to secure their sources of products and services.

This paradigm gives rise to the need for a comprehensive strategy that leverages a wide range products, solutions, and regulatory compliance strategies to ensure the security and the resilience of the supply chain.

1.2 What Is the Software Supply Chain?

Much of the additional complexity digitization brings to the supply chain is embedded in the transfer and delivery of data, which creates relationships that are not traditionally seen as part of the supply chain (see figure 1.1).

Figure 1.1: Traditional & Digital Supply Chains



Source: Juniper Research

As a result of this expansion, the scope of what is considered a supply chain — and how to defend it against cyberattacks — needs to be not only revised but expanded.

This report proposes that a supply chain must be understood as the products, systems and services that are utilized by a product vendor to produce and deliver a product or service to the end user.

Supply chain security does not only involve ensuring the supply and movement of goods, but also the supply of systems used to monitor and coordinate goods and services that are provided during the production of a product. This includes hardware and software systems that are used in the provision of a service. In addition, software updates or other services after a product's sale can also constitute part of the supply chain. Finally, the software itself can be used as a component included in the delivery of finished goods, as in connected devices that may contain hundreds or even millions of lines of code, much of which may be sourced from a supplier.

This software supply chain is the combination of the ecosystem of resources needed to design, manufacture, and distribute a product.

1.3 Why Do We Need Software Supply Chain Cybersecurity?

Cybersecurity is an essential consideration for businesses today and in the future. In our recent Cybersecurity report, we highlighted that enterprise spend on cybersecurity solutions would reach $226 billion by 2027, from $179 billion in 2022, fuelled by rising awareness of vulnerabilities and targeted threats, such as ransomware and DDoS (Distributed Denial of Service) attacks.

The increased digitization of every part of modern life, including digital transformation in the context of smart cities, means that the cyberthreat landscape is wider than ever. Data breaches are frequent, with insecure practices leading to valuable data being lost or leaked, which can cause additional downstream cybercrimes, including extortion, fraud, and identity theft.

In this context, the software supply chain is attracting increased scrutiny, leading to several imperatives for affected organizations:

- Cybersecurity vendors must keep pace with cybercriminals: Successful cybercriminals are constantly innovating to derive increased financial returns from their crimes. As such, it is critical for cybersecurity vendors to match criminal ingenuity with aggressive innovation and improved capabilities of their own. Tested and trusted cybersecurity vendors will be essential in ensuring that organizations and individuals are protected.
- Enterprises and governments must focus on tracking the evolving threat landscape: As the cyberthreat landscape expands, so do the skills and requirements needed to meet the challenges it presents. Key stakeholders must stay informed about cybercrime trends and adjust their business practices as necessary to ensure they are secure. In many cases, this can be achieved by working with an appropriate cybersecurity vendor that can combine product solutions with support, reinforced with up-to-date CTI (Cyberthreat Intelligence), to deliver the maximum level of protection.

1.4 Exploring Cybersecurity in the Supply Chain

1.4.1 The Role of Software, Hardware & Data in the Supply Chain

Supply chain cyberattacks can occur at any stage in the production or maintenance of a digital product or service, and supply chain security now must be as much about the flow of data as it is about the flow of goods. When the delivery of a product or service relies on data, any portion of that data that could disrupt product performance or service delivery must be considered part of that product's supply chain.

This means that there are two broad areas outside of traditional product delivery that should be considered part of the digital supply chain:

- Software, firmware, and data — including software components and updates, and data feeds/APIs (Application Programming Interfaces)
- Third-party (including supplier) handling of data

Any compromise of these areas can have a severe impact on product delivery and performance, as well as potentially endangering the security of the enterprise or its customers due to the threat of lateral movement through the supply chain via an exposed vulnerability somewhere else in the chain. Data theft or leakage can also have regulatory and reputational implications.

To mitigate these risks, organizations must acquire visibility and a thorough understanding of the security measures embedded into their own supply chain, premises, and products, as well as those adopted by their suppliers. This includes transparency on security protocols implemented into their suppliers' platforms used to deliver software, updates, and additional services after the initial sale of a product. This is especially important where software updates include portions of code from open-source libraries and other third-party software tools. This recognizes that not all software code from a given developer shares the same point of origin, which makes keeping track of code's origins, and the potential vulnerabilities it may contain, much harder.

i. Hidden Vulnerabilities

While vulnerabilities to cyberattack are inherently software based, they are amplified due to the possibility of compromised hardware or OSs (Operating Systems). These function as the basis of many services but can be leveraged to disrupt the operation of anything that uses them. This is the case where services are the primary end product, such as in banking or stock trading. Vulnerabilities in hardware or at the OS level are among some of the most dangerous, due to their high levels of privilege in the overall system (relative to the standard application layer). While software companies typically become aware of these vulnerabilities and endeavor to provide patches and guidance on securing hardware, other types of hardware-centric organizations are frequently far less likely to consider this aspect.

For example, Avanti Markets, a supplier of kiosks for vending machines, suffered a severe malware cyberattack (likely PoSeidon or FindPOS) in July 2017. The breach was one of several similar high-profile POS (Point of Sale) cyberattacks that year. POS terminals have been a frequent target of malicious cyberattacks over the years as the information targeted for theft is highly monetizable. These breaches pointed to an urgent need for retailers to adopt more effective security solutions designed to mitigate the risk of theft of their customers' data, such as biometric information and credit card details, and constant encryption of sensitive customer data, especially in transit.

In 2020, SolarWinds (a US developer of software for managing networks, systems, and information technology infrastructure) was subject to a sophisticated cyberattack on its systems. In this incident, hackers inserted a vulnerability (SUNBURST) code within the developer's Orion Platform software, to compromise the server on which Orion products run. The code was then replicated across the software provider's customer base, compromising thousands of organizations in both private and public sectors. This attack reflects how expansive, disruptive, and damaging just one successful software supply chain attack can be. It also illustrates the unprecedented risk that accompanies the shift to a digital and knowledge-based economy in much of the world, as so many of our products and systems become almost entirely digital in nature. Companies and governments need to adopt a new mindset to conduct businesses and offer services as securely as possible.

More recently, in February 2022, researchers of Tel Aviv University discovered significant security vulnerabilities within Samsung smartphones (including the popular Galaxy S21, S20 and S8 models), whereby attackers can extract cryptographic keys from specific hardware elements of the phone. Once compromised, cybercriminals can downgrade the software of these devices to versions with less security provisions and make them more prone to hacking — otherwise known as IV reuse attacks.

Hardware, and the system-level software that runs on it, has a crucial role to play here, from the systems used to design and monitor products to the servers that provide many "as-a-Service" offerings — from streaming providers to cloud infrastructure. While these servers are vital to the service being delivered, they are often "out of sight and out of mind" to those procuring and using the digital services. Thus, they are unlikely to be scrutinized from a cybersecurity perspective, despite their vulnerability to compromise.

This means that software supply chain cybersecurity is of vital importance to many different types of organizations. However, this whitepaper will focus on the nature of the supply chain for the following specific verticals:

- Automotive —Consumer and commercial vehicle production and.

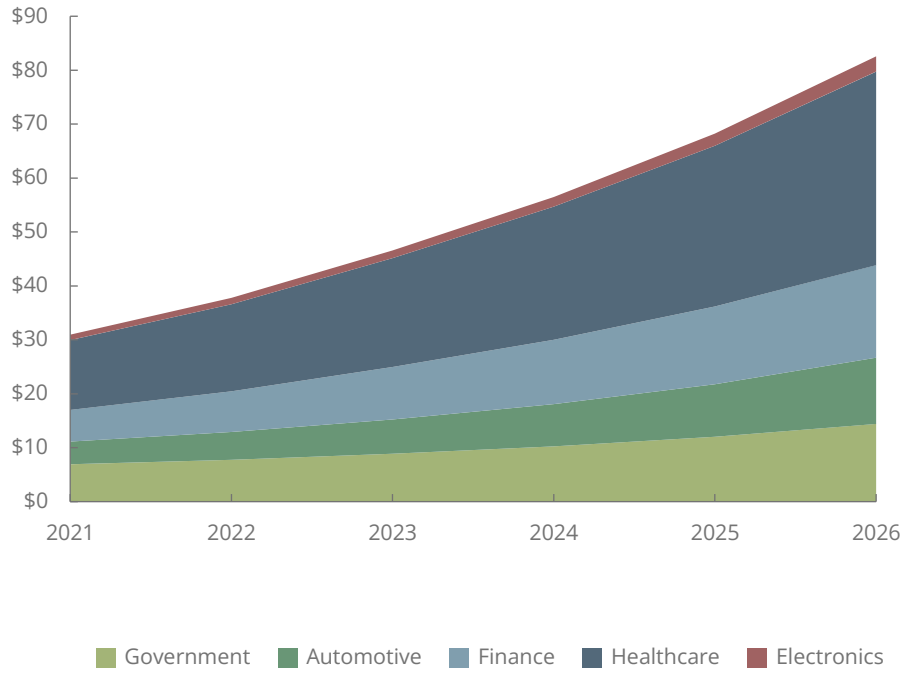
- Consumer Electronic Devices — The production and upkeep of electronic devices that generate and process data; simple electronic devices (such as hairdryers, alarm clocks, etc) will not be considered.
- Finance — All financial services, including banking, payments, investments, stock trading and insurance.
- Government — Information systems that are used to administer and secure digital government services; these can include systems for national defense, taxation, government licensing, criminal justice, and other state functions, including the military.
- Healthcare — Institutions concerned with primary healthcare delivery, whether provided by the state or private companies.
- Smart Cities — Locations where traditional networks and services are made more efficient with the use of digital solutions for the benefit of inhabitants and business; smart cities may utilize advanced technology to support urban transport networks, upgraded water supply and waste disposal facilities, more efficient ways to light and heat buildings, etc.

1.5 The Cost of Insecure Software Supply Chains

The prevalence of digital systems in the supply chain, coupled with a lack of awareness of the problems in many companies and industries, is likely to result in significant cost. Juniper Research estimates that, without a paradigm shift in software supply chain cybersecurity management, cyberattacks targeting software supply chains will cost the world economy an estimated $80.6 billion in lost revenue and damages annually by 2026.

Fundamentally, many businesses and industries lack sufficient cybersecurity resources to adequately harden their software supply chain today. In many cases, this is due to inadequate access to effective cybersecurity training, or failure to recognize the value of data they work with or process. In other cases, they may understand that cybersecurity is a threat, but not what that threat constitutes. This is particularly true with respect to the software supply chain.

Figure 1.2: Revenue Losses Attributable to Supply Chain Cyberattacks ($ billion), Split by Sector, 2021-2026



Source: Juniper Research

1.6 What Needs to Be Done

To secure their software supply chains against cyberattacks, companies and governments need to undertake the following measures:

- Make a concrete decision on what a strong security posture looks like. This requires quantifiable metrics, and interpretation of required standards. These standards often do not give quantifiable means of assessing a company's individual security posture, so cybersecurity vendors, companies and governments need to determine how to make those standards measurable, enabling a proper method of evaluation for changes and improvements to secure work practices.
- Providing a full account of software update management for any products, verifying each step of the process to be tamper-free and from an authenticated source. This can be done through an SBoM (Software Bill of Materials), tracking what changes have been made to software. However, robust verification must be completed in addition to just tracking ingredients and changes. This includes any software provided by a third party, even where it is integrated into a company's own products. The responsibility for security that is built into products not bolted-on must be shared between all parties within the software supply chain.
- Ensure suppliers and third-party data handlers have secure data processing practices, so that organizations are not compromised by a supplier's insecure practices. This includes ensuring that third-party data storage systems are properly encrypted, patched, and have robust authentication procedures.
- Raise awareness among executives that a company's supply chain is not just about the provenance of physical goods, but also about where and how the software and hardware systems it uses to produce its end products are managed.
- Consider cybersecurity as a component of safety. Companies must fundamentally realize that cybersecurity concerns are as important as physical safety concerns. The ramifications of cyberattacks in the supply chain — from cessation of operations to fines imposed for data breaches, or passing risks onto customers by supplying digitally contaminated goods — demand a strong focus on supply chain cybersecurity as a vital component of doing business, rather than an optional extra.

There is no silver bullet for supply chain security management, but using these steps can help organizations become more security conscious regarding the origins and handling of their software, and reduce risks associated with a software supply chain compromise.

2. Current State of Software Supply Chain Cybersecurity

JUNIPER RESEARCH

2.1 Introduction

Historically, the supply chain for each industry has had its own specific characteristics, thanks to the unique requirements and elements of each vertical. However, there is a set of common best practices for improving supply chain cybersecurity that can be employed across diverse industries. This section will discuss how various verticals — from digital products to cars to farming — handle cybersecurity today, including a variety of case studies documenting current processes. These will be critiqued, showing where improvements are most needed.

It should be noted that regardless of vertical, any system that relies on computer networks is vulnerable to attacks targeting that network. It is therefore vital that companies, regardless of the industry in which they work, take steps to secure the storage and transfer of data. As discussed in the previous section, this should be considered part of supply chain security, if such systems are needed to deliver a company's products or support ongoing operations.

2.2 Automotive: Increasing Cybersecurity Risks for OEMs Will Lead to the Need for External Cybersecurity Expertise in Managing Vulnerabilities

We expect 360 million vehicles globally to have embedded connectivity by 2027, covering multiple systems, from information and entertainment systems to vehicle management. These features are introduced into vehicle design and production at many points in the production process. This is one reason why the automotive supply chain is so complex, with a wide variety of companies providing individual components and portions of the vehicles, which are then combined by the automaker. This wide array of suppliers, often with limited visibility into what other suppliers for the same vehicle are doing, provides fertile ground for unintended software interaction. This in turn multiplies opportunities for cybercriminals to exploit digital elements of vehicles during production — and indeed their ongoing use. This has serious implications, given that many vehicles do not currently have the capacity to be upgraded. However, with the number of connected vehicles growing by the day, this represents both a vulnerability and an opportunity for updates to be provided.

The software deployed as part of car manufacturing varies; some systems, once established, will remain essentially the same for years — if not a decade or more. Several software packages used by automotive component suppliers either contain standard code or code provided by subcontractors, which is implemented without change or analysis by systems integrators and automotive OEMs. In addition, third-party code implementation can add elements that have not yet been screened during either software development or final assembly of the vehicle. Thus, in certain vehicle assembly cases, the vehicle manufacturer may have limited knowledge and an incomplete assessment of a vehicle's entire source code during the final assembly stage. Frequently, automakers will only do functionality analysis at this stage, to ensure the absence of software conflicts, rather than carrying out a full examination of all software components to assess the cybersecurity risks posed by each software component.

Model variants of cars also pose a challenge. Different safety features, as well as cruise-control options and varying degrees of automation mean that the software and hardware components required for each variant can differ widely. This makes both stock management and control of inventory highly challenging. If a resource-heavy model becomes popular, there may even be a need to shift suppliers during vehicle production, impacting efforts to ensure each supplier operates with acceptable levels of cybersecurity.

The automotive industry is aware of these challenges. The ISO/SAE 21434 standard, currently under development, is intended to address cybersecurity for the industry, as are requirements in WP.29, published in June 2020. These will necessitate a security-by-design approach, across both hardware and software design, for all vehicles produced on or after July 2024. We are also seeing moves internationally to require a software bill of materials, alongside software update management systems, which would simplify update processes. However, this has yet to reach all applicable segments and verticals of the industry. It is also arguable whether WP.29's requirement for a variety of cyberthreats to be "adequately considered" in risk assessment is sufficient. While it is laudable that WP.29 requires automakers to maintain a cybersecurity management system to keep vehicles secure while on the road, the extent of that monitoring is not totally defined.

Most importantly, ISO/SAE 21434 is a unifying standard that is intended to be applied to both automakers and their suppliers, guaranteeing a common standard of security to make sure that supply chain cyberattacks are no easier to perpetrate than attacks on the automakers themselves. The current automotive standard, ISO 26262, does not require secure supply chain management, instead merely that that automaker ensures the security of the vehicle and their own processes. This leaves the possibility of supply chain attacks much more open, which will remain an issue for the space while vehicles that are designed according to ISO 26262 standards are active. The implementation of ISO/SAE 21434 at a later point will bring some degree of security to these vehicles, but hardware-based flaws will still remain, unless general recalls are issued, which will be too expensive for automakers to realistically consider.

While the onus for enforcing these standards may fall on automakers, very few are likely to have enough in-house knowledge to manage cybersecurity across many disparate systems themselves, even as their cars require more technology. As a result, many will need external help in managing the vulnerabilities this increased digitization is introducing.

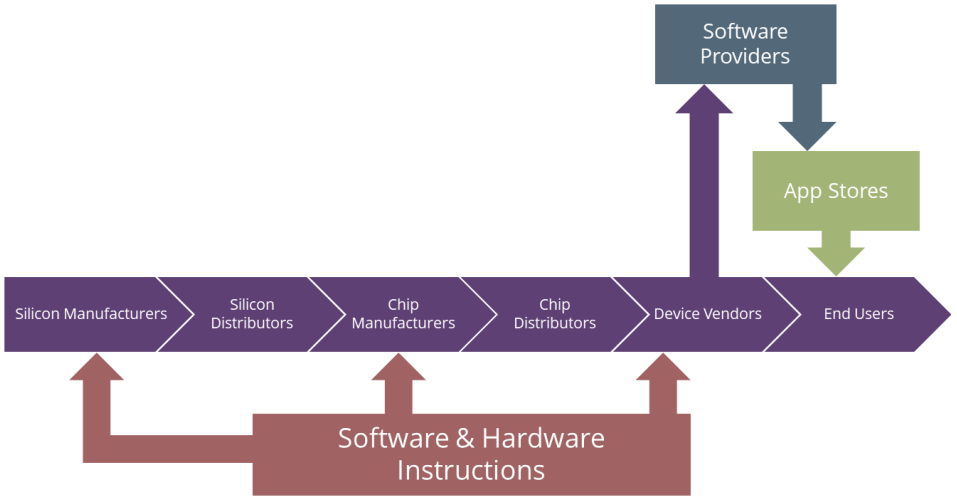
2.3 Digital Devices: Certification Required to Ensure Authentic Products & Secure Updates

2.3.1 Design & Production Cybersecurity

Any electronic device which is used for a specific function will require specific capabilities, such as the many different types of sensors involved with smart city transformation, including smart intersections, smart street lighting and others. This means that the sum of any digital device contains components from many different suppliers and distributors, even before device OEMs are involved. For example, where OEMs are not big enough to order in bulk directly from silicon wafer and board manufacturers, they instead rely on distributors to source their components, which can introduce malicious or defective elements into the production process, if the supply chain is not properly secured. Given that sensors will be needed in vast bulk for smart city transformations, this can be a major problem.

Indeed, in the smart cities context, if a sensor system is compromised during the production phase, this could lead to safety issues, for example, with a smart intersection not responding to traffic levels correctly or even failing completely. As such, the stakes are high for getting this fundamental security issue covered.

Figure 2.1: Digital Devices Supply Chain



Source: Juniper Research

i. The Importance of Certification

Component certification forms an important part of this process, but is not universally practiced. It is frequently seen as a useful tool for resource management or for CSR (Corporate Social Responsibility) purposes, to prove the provenance of the components as free from conflict minerals or similar. Component certification and provenance is not necessarily required as part of any national compliance standard. However, the EU's European Cybersecurity Act has provided a regulation that requires IT product providers to adhere to the various standards of a variety of cybersecurity certification schemes, and it is expected other governments will mandate further regulation.

This means that some vendors may even be unaware of the underlying components and firmware of the SoCs (Systems-on-Chip) that they are using, especially if they involve third-party designs. As a result, particular components may contain unaccounted for software interactions that may not be properly inventoried. These can cause design failures (most famously the Samsung Note 7), but also leave the devices open to potential cyberattacks.

These devices are therefore potentially open to the incorporation of either unauthorized components that a distributor or chip manufacturer includes but does not necessarily include in a specification, or of unauthorised hardware that neither party is aware of. This is the kind of attack that Bloomberg first suggested in October 2018 was perpetrated against Super Micro by Chinese state actors; if chips can be introduced onto SoCs without the OEM's knowledge and incorporated into the board's BIOS, they can potentially compromise an entire device.

Another significant threat in the current environment is the global chip shortage. While some industries have begun to catch up in terms of chip availability, there are still major shortages within certain industries, especially in the automotive space, with orders being delayed and features being scaled back. As distributors struggle to fulfil orders and to cut waiting times, the temptation to cut corners and take on silicon that is not properly verified and quality-checked is increasing. This desperation means that device vendors' own designs may not be being carried out to specifications, introducing unknown vulnerabilities that can be exploited.

For this reason, device manufacturers need to be able to inventory their hardware and software accurately to assess the full scope of what vulnerabilities need to be addressed in their products. This is currently not done in many cases, where the ODM's (Original Design Manufacturer) or distributor's parts are taken as trusted simply by virtue of their source. Security by design has been the mantra of various portions of the industry (most notably the IoT) for some time. However, this must be paired with the ability to review the actual content of the devices to ensure that those secure design principles have been carried out in execution.

This is difficult to achieve internationally, balancing different regulatory requirements. Producing products that comply to differing national compliance standards is a logistical challenge, which is not helped by a lack of international standards in this space.

2.3.2 Software & Update Cybersecurity

The majority of supply chain cyberattacks come not from a threat to hardware, but to software, in the process of providing software updates. If a cybercriminal can compromise the ongoing delivery of software, then any device requesting a software update can become a vehicle for malware. If a device base is large, this can lead to thousands or millions of compromised devices.

A key layer of software here is firmware. Firmware-level commands have broad authority to alter system configuration, as well as issuing commands, making them damaging and hard to root out as firmware updates are not usually carried out on a regular basis. In the case of these forms of compromises, servers that provide OTA (Over the Air) updates can be compromised and can send backdoors or malicious instruction sets to a device as part of a trusted update framework.

Companies will have a quality assurance and assessment process during the build stage and may check over the source code for any updates if they make the software themselves. However, this will exclude any threats or vulnerabilities introduced during the software compiling stage, as well as anything introduced post-build. Companies need to be aware of the security of distribution of their software, as well as the security of the software itself. This requires robust security procedures for checking software both pre- and post-build, and a knowledge of how any software updates for the device will be administered. At present, companies rely on reputational information or one-time third-party assessment of their suppliers, which is not enough to fully assess the security of the update mechanisms. These mechanisms can be altered and changed by the third party to suit their needs, incorporate new acquisitions or inventory, and other techniques that may introduce new vulnerabilities into their procedures, unbeknownst to the device manufacturer.

Device manufacturers also need to ensure that their software distribution channels, frequently a third-party provider, are secure. This paradigm is why many consumer devices only provide update through certified app stores. However, other environments, such as enterprise software, must handle update distribution through arrangements with a dedicated service provider. Device manufacturers need to be able to certify that their updates are provided securely, and thus have an awareness of the cybersecurity practices of their distribution partners.

Case Study: Gigaset

Gigaset

German smartphone maker Gigaset was the target of a software supply chain cyberattack in April 2021.

The attackers exploited a weakness in a third-party update provider's server to install adware and message and social media hijacking capabilities on infected phones. Gigaset said that only its users who received firmware updates from the compromised server were impacted. It is not clear whether the updates containing the malware were unsigned or whether the private keys to sign the updates were stolen. The malware was able to affect smartphones out of the box, because it came as part of the smartphones' system apps loadout and would reinstall malware apps and carry on its activities so long as the system app level commands were still present.

The malware did not impact all Gigaset devices because of the limited penetration the criminals were able to gain into the third party's servers, only compromising a single server.

Juniper Research's View: The Gigaset breach is a perfect example of how the update process can be compromised through involvement of a third party. Device manufacturers need to ensure that they have a way to measure what has been installed to what is produced from the company. This can most easily be done through the implementation of cryptographic hashes to verify the size of updates, to ensure no tampering, as a form of digital signature. This would have prevented this form of tampering, if the update service provider never had access to the private keys to sign the updates, but instead placed a verification call to the manufacturer's own servers.

2.4 Finance: High-target Industry Opening Up but Needs to Watch its Tech Partners & APIs

The finance industry relies on software for its fundamental operation, and as such, it has had standards for data management in place for many years, with the PCI DSS (Payment Card Industry Data Security Standard) being established in 2004, following the SOx (Sarbanes-Oxley) legislation of 2002. SOx has been recently expanded to include cybersecurity provisions, meaning that FIs (Financial Institutions) are now required to have "cybersecurity systems standards and practices" in place. This is increasingly necessary as it has been noted that the financial industry is 300 times more likely to be the target of a cyberattack than other industries.[i] However, the focus of such cybersecurity efforts has been on detecting fraud and other customer-facing cybersecurity issues and data transfer, with only cursory regard given to the security of FIs' supply chain in many regulations, with risk disclosure being the extent of many FIs' regulatory need with regard to suppliers, although best practices do exist for vulnerability management, such as in the framework outlined in NIST SP-1800-5.[ii]

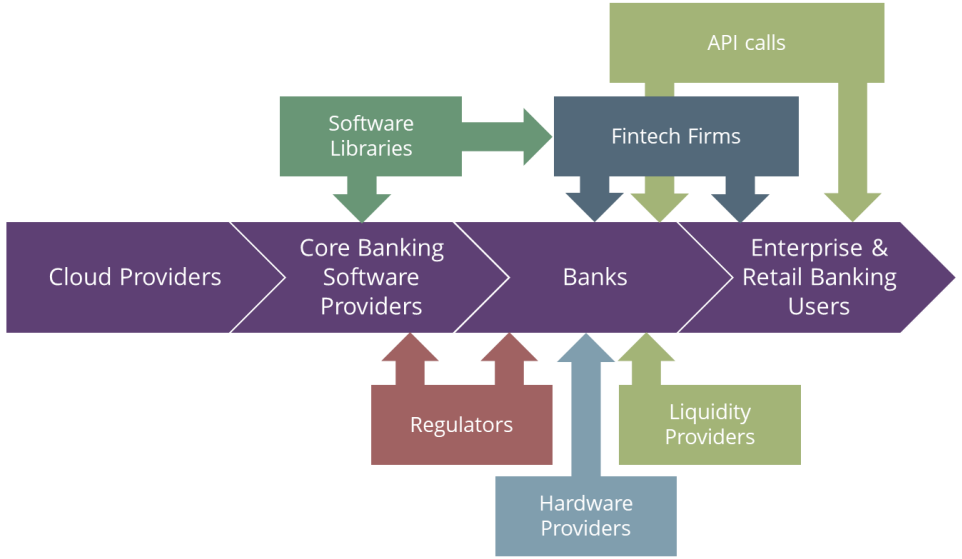
With many banks and other financial firms now partnering with fintech companies to offer a wider range of software services and interacting through API platforms, the software that accesses and manipulates that data is frequently outside of banks' control, and needs to be secured.

The distance between banks and the software they leverage is often by design, as fintech firms often do not want to be burdened with the high levels of compliance that come with being a bank, but still want to offer banking services. This means that companies do not necessarily have visibility on the activities of other companies that deal with their data, presenting security risks.

Although such companies are still regulated by the PSD2 (Second Payment Services Directive), the emphasis of this is in providing guidelines for authentication requirements to make payments, rather than on more general cybersecurity requirements being enhanced.

FIs also need to consider their underlying software providers – for smaller institutions, third-party provision of financial management software for core functions is common. This means that the core operations of some of the most crucial companies in any economy are frequently outsourced to third parties, over which the financial institutions have little control, but often shield from liability, thanks to tight regulatory frameworks. This is the case for the banking industry, where core banking software providers have long been a part of banks' standard practices and have flourished where there is a plurality of banks that require their software.

Figure 2.2: Banking Industry Supply Chain



Source: Juniper Research

Case Study: Prospect Capital

PROSPECT CAPITAL

In March 2020, in New York City, physical offices of all non-essential businesses were closed by order of the Governor, including that of Prospect Capital Management, a private debt and equity investment advisor to Prospect Capital Corporation and Priority Income Fund, each with thousands of shareholders across the US.

Only three days before the shutdown, BlackBerry Security Services consultants had completed onboarding BlackBerry CylanceGUARD and begun actively monitoring and defending Prospect's endpoint security infrastructure. This was highly fortunate timing, given surges in cybercriminal activity during the pandemic. Due to the deployment of CylanceGUARD, Prospect Capital was unaffected by this upsurge in cybercriminal activity, showing the importance of using the right systems at the right point, while being shielded from the alert, fatigue or exacerbated threat activities. In June 2017, Prospect formally selected BlackBerry CylancePROTECT as its new endpoint protection platform. The deployment launched shortly thereafter. In Fall 2019, Prospect Capital began assessing BlackBerry CylanceOPTICS and three other EDR solutions and concluded that CylanceOPTICS had the most flexible detection and response framework, which would allow them to fine-tune detection rules to minimise false positives. The subsequent upgrade from CylancePROTECT to CylanceGUARD went smoothly for Prospect Capital and left it well protected when the threat of pandemic-related cybercriminal activity came around.

Juniper Research's View: Prospect Capital has clearly taken a proactive approach towards its cybersecurity risk management and has reaped the rewards of this in remaining secure during a difficult time. Proactive assessment and the tuning of what capabilities are required at different points in time are critical to ensure security within the financial services space and the wider enterprise environment.

Software providers are a key, but often invisible, part of any bank's business. Both providers and fintech firms can rely on third-party software libraries, as many developers do.

Unless correctly audited, these third-party components may contain compromised code, leaving FIs' end software vulnerable to compromise through exploits of that shared software.

Open Banking may cause problems for the bank's software supply chain. For counties that have legal requirements for Open Banking (Europe), this means mandatory interactions with API platforms, which have been sharply on the rise, noted in Salt Security's latest report on the issue.[iii] With the need for third-party involvement due to Open Banking, API security is a software supply chain issue for banks, one that will only increase in complexity over time.

In addition to the criticality of the data that they carry, banks' systems are highly interconnected; a study by the Federal Reserve Bank of New York notes that, if one of the "big five" banks were to fail, 38% of assets held in other banks would be at risk due to the reduction in payment flow.[iv] The 2017 Equifax breach affected not only Equifax customers directly, but the credit bureau's supply chain, including Visa and Mastercard. This means that, in effect, large FIs (banks and payment networks) form part of the supply chain for other FIs, and if they are compromised, then large portions of the financial system may be vulnerable to supply chain cyberattacks. To properly secure their supply chain, FIs need to understand how their cashflow operates regarding third-party involvement, and to understand not only their own cybersecurity risk, but potentially that of their competitors as well.

Despite this interconnected nature, there are few thoroughgoing requirements for cybersecurity other than principle statements, and few authorities that oversee general cybersecurity standards for the industry even at the national level. This means that the industry is at risk of losing sight of more general cybersecurity needs thanks to an industry that is focused on securing transactions, to the detriment of the elements that inform that security.

Hardware has a key role to play here, as defective hardware can circumvent even the most secure software provisions. Hardware components installed onto servers can give attackers access that can negate software-based security, as it can give commands to override particular software at the OS level. As a result of this, financial institutions need to be aware of where their hardware comes from, including those aspects of hardware used by non-industry players, such as unspecialised use of cloud hardware. Many of these providers aim to keep the data they store outside of the scope of financial regulation using encryption, tokenization, and other technologies, but in the event of a hardware compromise, these measures may be insufficient.

2.5 Government: Complex Supply Chains Should Look to the Top & Set the Standard for Other Sectors

Of all the forms of organizational supply chain, those supplying government bodies are among the most complex. The need to meet a variety of requirements to ensure interoperability of data between different government bodies means that the supply chain for government agencies is both wide reaching and subject to changing requirements and structures. As a result, the supply chains connecting them are equally excessively complicated, covering everything from state pensions administration and city governance to military procurement.

The variations in requirement for the security of government systems will depend on the states in question, so only a few will be the focus of this whitepaper. A recent US executive order has required extensive changes in how the US federal government secures its supply chain.[v] This includes moves towards Zero-trust Architecture for cloud facilities, and a requirement for data encryption and multifactor authentication. For the supply chain, it has required the development of practices that require a software bill of materials to be provided by all suppliers to the federal government, alongside vulnerability disclosures and requiring secure software development practices. Preliminary guidance is already available on what constitutes a suitable SBoM, and final guidance should be in place by early February 2022. The Executive Order follows the IoT Cybersecurity Act of 2020, which is similarly intended to make government devices less vulnerable to hacking and may eventually become a *de facto* standard for the private sector. The Executive Order is already spurring

greater awareness of supply chain cybersecurity elsewhere, with fresh guidelines published for businesses by the UK government, in the light of the US executive order. However, to date, the standards have not been fully revised, and the existing NIST standard (SP 800-161, published in 2015) still stands as the legal benchmark for government supply chain compliance.

As they currently stand, the SBoM requirements mandate that software elements' dependencies are disclosed, allowing for the identification of the source of software used from places like open-source libraries or companies' existing catalogues. These could introduce vulnerabilities not immediately obvious from a functional security analysis, as well as potentially being invisible to source code analysis.

The executive order, and pronouncements surrounding it, indicate that the US federal government is taking its software supply chain seriously. However, those areas that have autonomy in determining software, such as state and local governments, may not require such rigorous security standards. In addition, there is some evidence that smaller and discretionary purchases may not be subject to the same standards as larger items.

In addition, security standards vary wildly at endpoints for government service delivery, meaning that zero-day threats may remain and disrupt the ability to deliver needed services. Departments without inherent security awareness as part of their job role may be unaware of the critical role that such software plays in their ability to remain secure and deliver their services. Areas handling sensitive data may be more aware of this, but even personal data is often left exposed when these platforms are not updated regularly.

The EU has launched a review into supply chain cybersecurity in member states that may have far-reaching consequences beyond the confines of its governing bodies, but will have the biggest impact there first. However, there is little cybersecurity regulation that is specific to supply chains within the EU at present.

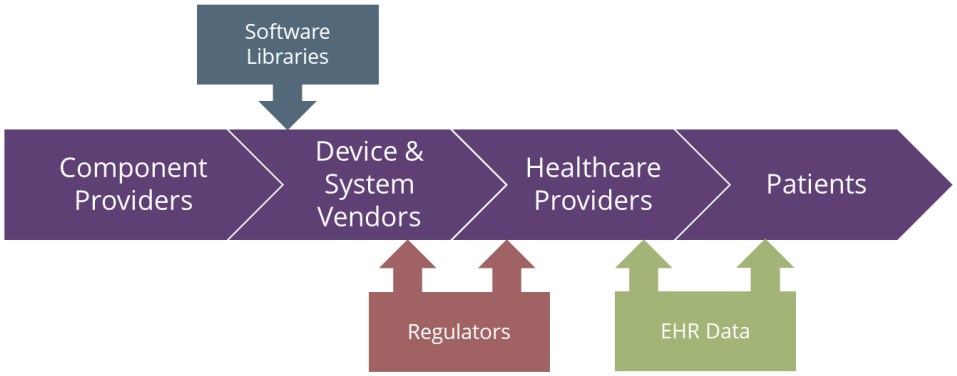
2.6 Healthcare: Disconnected Device Monitoring Is Vital, as the Ecosystem Brings More Digital Gateways

The healthcare industry has a complex supply chain, dealing with the supply and management of both general electronics and specialized medical devices and software, which potentially has to be disclosed to a range of healthcare stakeholders, from other healthcare organizations to patients and, increasingly, data from consumer-grade products as wearables manufacturers start to leverage their biometric data for healthcare purposes.

The industry handles a large amount of sensitive personal data in the form of medical records and treatment details, which means that the industry is very aware of threats to patients' data and its management. As a result of this, there has been a focus on making data transfer interoperable while also requiring that data is secure. This is managed by the HIPAA (Health Insurance Portability & Accountability Act) in the US, and the GDPR in the EU. The industry also uses the DICOM (Digital imaging & Communications in Medicine) and HL7 (Health Level 7) standards that facilitate encryption of medical imaging data.

However, there is almost no acknowledgement in regulations of more general cyberthreats. FDA regulations in the US recommend NIST cybersecurity practices as standard, but there is little emphasis in this on the industry. Standards relied on medical device providers and medical system software providers to provide secure software, something that is often specified in regulations on devices and software used for medical purposes. However, there is little requirement for ongoing software security, beyond the basic words in these frameworks. The management of devices is often left to technicians, and updates if required are often *ad hoc* and expensive, meaning that vulnerabilities can be left unaddressed for large periods of time. This may be less of an issue than in other verticals as medical devices' Internet connections are often intermittent, instead relying on a healthcare provider's intranet, but both updates and the lack of them can still pose a threat.

Figure 2.3: Healthcare Industry Supply Chain



Source: Juniper Research

The lack of connection has meant that healthcare providers and their management bodies have paid little attention to ongoing device management, even as their systems become more digitised and able to connect to wider networks. The data flow for both EHR (Electronic Health Record) updates and device software updates is therefore not subjected to the same scrutiny as data storage and transfer. This lack of oversight leaves the proliferation of older devices and mis-managed devices being exploited and creating a gateway for lateral movement.

The COVID-19 pandemic has brought about a boom in remote monitoring and telehealth technologies, which have been rapidly put into place. This has brought a new element into the supply chain that few healthcare providers were ready for: that of third-party connectivity and data service providers. These players may or may not store healthcare data themselves, but also require linking to existing data storage systems that can give cybercriminals a larger attack surface to access and disrupt healthcare IT systems. Although the medical supply chain for software can have the same benefits and pitfalls of updating devices where consumer hardware is used (such as tablets or, in some cases, wearables), other forms of medical devices are intended for use with only intermittent connectivity, but still have some level of cybersecurity provision. Software providers and healthcare organizations therefore need to implement cybersecurity measures that perform well offline, and are not reliant on the traditional hash-based endpoint protection, which will quickly become outdated without regular connectivity.

This is coupled with the long lifespan expected of medical devices, heightened within emerging economies. Due to this, devices need to remain secure even after a manufacturer has discontinued active support for a device, particularly in the case of specialized equipment. This means that all elements of the device need to be geared towards that longevity, including its security. The technology required to secure healthcare systems and modern medical devices is beyond the scope of traditional signature-based products. BlackBerry's embeddable technology, CylanceOEM Engine, allows manufacturers to leverage machine learning technology that quickly and accurately identifies malware, without relying on network connectivity. This resilient and lightweight technology bridges the gap between long and potentially offline device lifespans and increasingly complex threats to healthcare and IoT security.

Device identity is the one area where healthcare has a strong regulatory framework in the EU. With IoT connectivity increasing across many healthcare facilities, device identity is a key part of management of these and will be vital to make sure that updates are properly managed and maintained. However, it is only a single piece of the puzzle.

VULNERABLE SOFTWARE SUPPLY CHAINS
ARE A MULTI-BILLION DOLLAR PROBLEM

3. The Way Forward

JUNIPER
RESEARCH

3.1 Introduction

Evidently, current cybersecurity practices are inadequate for much of supply chain management in many industries. This is due to a combination of a lack of realization of how far the supply chain extends (the software supply chain), and a lack of awareness about what should be done to keep that supply chain secure.

There have been numerous calls to update NIST SP 800-161 with provisions to track and verify the security of software, to secure this digital element of the supply chain.

We believe the following principles should be implemented by businesses and as part of regulation, in excess of current standards, in order to ensure more secure supply chains.

3.2 General Supply Chain Cybersecurity Principles

There are several general principles that can be applied across all industries in order to improve organizations' supply chain cybersecurity. While some elements will apply more to those organizations that directly engage with elements of their supply chain,

- Supply chain cybersecurity is important for everyone. Some of the biggest supply chain cyberattacks have impacted industries not traditionally associated with cybersecurity. In some cases, such as the SolarWinds attack, the impact ran across industries, with more than 30,000 public and private organizations, including local, state and federal agencies, using the comprised Orion network management system.[vi] This has implications for how organizations consider cybersecurity internally (where all employees need a level of cybersecurity awareness), but also in terms of industry regulation. Standards in many places need to be tightened and the responsibility for cybersecurity broadened to make industries more concerned about the security of their supply chain.
- Security needs to be Security by Execution, as well as Security by Design. Many supply chain cyberattacks can subvert or undermine Security by Design practices; these are intended to protect against attacks from outside the design process, and if the design process is compromised then securing systems from the outside does not matter. Companies that produce digital products need to guarantee that secure procedures are followed.
- Verifiable bills of materials are needed for both software and hardware. With supply chains for many industries relying on many different third parties, secure bills of materials are needed at all stages of production, so that at-risk elements can be identified and either removed or mitigated. Software verification has received much attention recently, but hardware verification is also necessary, to avoid defective products that can undermine software-based security measures. As such, certification of what hardware elements are or are not present on a given device is necessary.

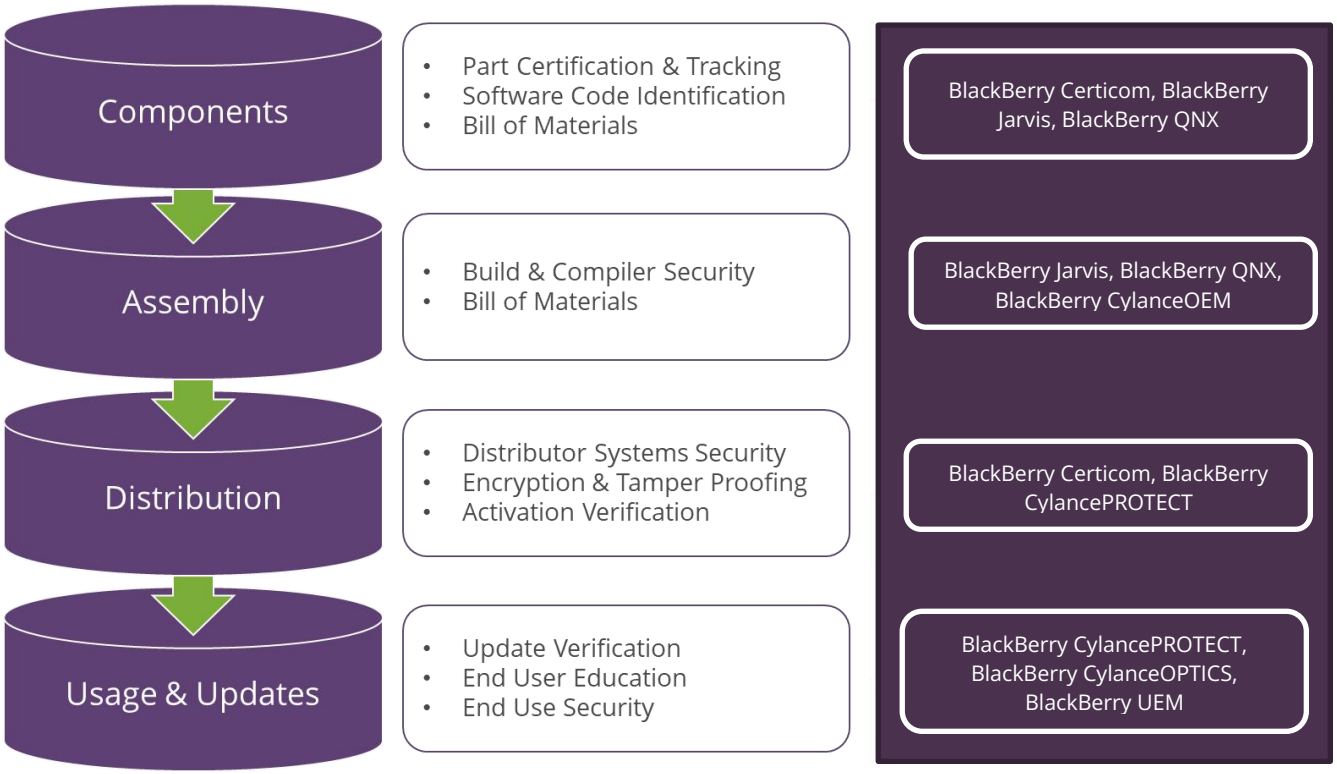
A standard framework for SBoMs has been proposed by MITRE, which would leverage elements such as common metadata, code signing and assurance levels so that both product providers and end users can analyse elements of any given product for vulnerability.

The recent MITRE research noted that the global supply chain environment lacks systematic integrity and recommends a series of actions by the software development community and IT sector to reduce the risk of compromise from software supply chain attacks. They propose that the NIST update its existing supply chain standard (NIST SP 800-161) to include a new framework for securing software supply chains and that the federal government require vendors/resellers/integrators to implement this framework. With any shift in standards, organizations will need to consider how to meet these while maintaining operational efficiency.

3.3 Securing the Supply Chain Technology Stack

Many of these measures can be expressed as having an awareness of the provenance of elements in each stage of the supply chain, but this has different manifestations throughout.

Figure 3.1: Supply Chain Stages & Security Measures



As a well-established cybersecurity vendor, BlackBerry is well-positioned to help organizations secure their software supply chain and meet new regulatory standards. Source: Juniper Research

i. Component Supply Chain Security

Proving the identity of components is key, whether as part of anti-counterfeit measures for hardware, or tracking the source of third-party code bundles, in the case of software. These identities can be maintained through the assignment of cryptographic hashes in most cases, assigned to chips or portions of code. However, where code is consumed from open-source libraries, these stakeholders need to become more vigilant at maintaining metadata that can be understood by the end users.

This will require some form of automated identification and certification process. Initial consultation results for the SBoM requires that component names and versions are maintained, alongside any other identifiers available.[vii] They will require a large degree of automation to keep up with the requirements, as managing software of this sort by hand will rapidly become impractical.

As with any bill of materials, this will need to be matched with verification tools to be fully effective. The prevalence of software updates means that there will need to be a steep change in how organizations think about the software they use, at least those looking to comply with the US Executive Order in the first instance.

Case Study: Jaguar Land Rover

Originally developed in 2018 for the automotive industry, BlackBerry Jarvis is a cloud-based binary code scanning solution that provides an assessment of the code base of software provided to it. It goes beyond source code analysis by providing breakdowns of packaged software used as part of an application.

Jarvis' insights into the software it analyses are taken from a range of sources. It fulfils the requirement of the recent US Executive Order and goes beyond it in highlighting known vulnerabilities in need of remediation. This can be machine read and used in tandem with a vulnerability remediation system to fix any vulnerabilities, errors, and other areas of concern in a software build.

The tool can be deployed to help inform cybersecurity actions and form part of a measurable level of vulnerability for a company. The tool does not fix vulnerabilities itself but allows other software or a human analyst to see what action is needed.

The tool can also make the task of code analysis much less time consuming. Jaguar Land Rover ran a comparative study using Jarvis and a cybersecurity analysis team to analyse the software contained in a vehicle under production, and Jarvis produced the same results in seven minutes that two analysts had taken 30 days to produce.[viii]

Software verification tools will themselves have to be secured, which means that they need to be prepared now for quantum computing. Many critical devices most in need of supply chain security are expected to be in service for many years or, at times, decades, and so need to be ready for the possibility of quantum computing cyberattacks, and go beyond basic cryptography.

ii. Assembly Supply Chain Security

Several manufacturers stop at the stage of analyzing code, often either purely to check functionality or analysing the source code for a product. This leaves the possibility of flaws being introduced when software is compiled, or when different software interacts within the same system. Build environments can also be compromised and introduce deliberate vulnerabilities into the software it is producing. As a result, companies need to go beyond the SBoM minimum requirements outlined by the US Chamber of Commerce, and track the name and version of the compiler as well as software code versions. In this way, errors or malicious code introduced as part of the compilation process can be identified.

This process has a mirror in the hardware side, that requires authenticated versions of each component to be tracked and certified, which is done through a key-based device and component provisioning process. To ensure that these are not compromised at any point on the lifecycle, these keys need to be encrypted using processes that are resistant to anticipated quantum hacking. Although several years away, devices need to be secured against quantum hacking if they are still in service when this becomes a reality. One of the most common ways to secure these in a quantum-resistant fashion will be through cryptographic hashing, verified through a public key infrastructure.

Case Study: BlackBerry Certicom

BlackBerry | certicom

BlackBerry Certicom offers a variety of solutions to ensure that components, devices, and software can be authenticated securely. The company offers specific services for the automotive, IoT and semiconductor industries, covering the use of PKI certification, hardware security modules and code signing capabilities. The solution uses hash-based signatures, which means that the system is ready to defend against quantum computing hacks.

BlackBerry offers specific profiles for V2X and ZigBee Smart Energy devices. The IEEE 1609.2 Standard for Wireless Access in Vehicular Environments and its ECQV certificates are based on BlackBerry's technology in this area, guaranteeing compliance.

The Managed PKI solution allows clients to utilise a fully customisable Certification Authority, including the ability to revoke credentials and provisioning privileges remotely, which ensures that contract manufacturers cannot produce authentic products without the consent of the OEM, limiting the ability of manufacturers to produce counterfeit devices. This allows for trusted outsourcing of manufacturing. The certification process can also be separated from device provisioning, checking upon activation that a device matches the manufacturer's specification.

A combination of Certicom PKI and Secure Code Signing allows valid device activation while checking that no unauthorised code or other modification has been applied to the device, utilising a distinct Code Signing Key Management capability, inclusive of quantum computing and cryptography capabilities.

Together, Certicom's capabilities work to mitigate many risks manufacturers face in dealing with component management in the supply chain.

This practice is already established in many industries, although there are instances where there is little awareness of key management and provisioning in devices. The biggest hurdle for device manufacturing and assembly at this point is ensuring the integrity of the process through the application of standards. Different industries will have different degrees of component verification required (dependent on how much a device's function may affect health and safety) and adhering to those legal requirements is more a priority than particular standards for a process applied to generalised manufacturing and assembly.

Post-build component checking is also a requirement, and one that cannot be simply tied to boot procedures and BIOS scans. Bill of materials verification is a vital part of this process, but must occur independently of the system itself, as malicious hardware can often compromise firmware to the degree that a device will not accurately report malicious content.

iii. Distribution Supply Chain Security

The path from manufacturer to consumer also needs to be considered a cybersecurity risk, especially for software. Software products and updates, including those that are offered by smaller companies, will not use their own servers to provide their products, but instead go through a third party. This introduces another set of risks as the distributors may have different security standards to the device vendor. In some cases, such as mobile app stores, these policies are relatively well disclosed, but others may not. Software vendors must verify the integrity of the software that is sent to their clients, rather than simply relying on pre-launch QA processes to catch any malicious code. This requires software certification, which can be provided through hash-based certification procedures.

This ability to confirm distribution through digitally signed components or other deliverables is one that is proliferating through many different industries, using a range of diverse technologies, from the use of RFID tags to blockchain. The biggest danger in using these methods, regardless of industry, comes from the lack of standardisation between points in the supply chain. This means that different portions of the supply chain may use different forms of validation, requiring each stage in the chain to be familiar with each form, which only escalates further up the supply chain. Only in markets where a stakeholder can exercise sufficient market power over others will this not occur. To prevent this, governments and industry organizations need to work alongside digital service providers to make certification and metadata standards broadly applicable to different forms of organizations within various industries.

iv. Usage & Update Supply Chain Security

For digital products, many of the same principles that apply to software component security also apply to the update process, where several vulnerabilities can creep in. This is because each update is essentially a build of the software in miniature and needs to follow the same secure procedures. A SBoM should be required for updates as well as initial builds. The base requirements released by the US Chamber of Commerce in the wake of the executive order on cybersecurity acknowledges this by requiring version numbers to be part of any committed update's details.[ix]

One element that is critical for updates is that of confirming that the update delivered to the end user matches that held by the company are the same as those developed internally, through means of a cryptographic hash, based on file size. This ensures that the code that users are receiving are the same as those that are being shipped out of the original organization. The security of any update channel, whether part of a company's own infrastructure or a third party (including servers and systems integrated through acquisition of companies), needs to be verified through such checks in order to protect against both compromise of the update service supplier and man-in-the-middle attacks through elements not controlled by the company supplying the software.

In the wake of SolarWinds, there also needs to be a decrease in automation of the update process. The SolarWinds attack is currently understood to have been a compromise of an automated build environment. At the very least, this indicates that the validation of updates and their components needs to be undertaken through a different system than develops the update itself. There needs to be a big enough break between build and validation to stop a single compromise from allowing malicious actors to both produce and distribute code, or even to produce authentic certification for the malware.

The ability to provide updates to patch security vulnerabilities is one that also needs to be critically considered. Devices that are only intermittently connected to the Internet also need to be able to withstand cybersecurity threats, whether from direct device tampering or infection via an intranet. Endpoint security for these devices needs to be adaptive without being online, as Internet connectivity cannot be guaranteed. In addition, many businesses have to run older software in order to do business, meaning that endpoint protection for many supply chains needs to incorporate protection of systems that receive only intermittent updates, and need wide-ranging compatibility to function.

Case Study: SSP

Insurance software provider SSP has an infrastructure of more than 7,000 endpoints and operations in four continents. This includes legacy software systems that are around a decade old and runs many bespoke software packages, as well as having many different online and offline operations. This mix of technologies and systems means that SSP requires an extensive and flexible cybersecurity posture, capable of running in multiple environments at low system resource cost. It also means that providing cybersecurity solutions to SSP is challenging, requiring the ability to protect different areas, technologies, and threat vectors.

In tests run by SSP, BlackBerry CylancePROTECT detected a range of custom malware and prevented simulated zero-day attacks, whether others failed. In addition, alongside advice from BlackBerry's cybersecurity consultants, BlackBerry CylancePROTECT incorporated custom executable identification to cover this older software, alongside a full discovery and coverage of SSP's endpoints. Following this initial survey, it was deployed on SSP's AWS cloud infrastructure in place of its older anti-malware solutions, resulting in a faster processing time that ultimately tripled cloud-based throughput.

Juniper Research's View: Being able to monitor large-scale software distributions, that are often automated, is key to the smooth running of many businesses. Infrastructure protection needs to be able to consider all forms of potential attack surfaces, including legacy systems that are often not able to be kept up to standard with the latest software. Protecting these legacy systems will often cover one of the weakest points in an enterprise's cybersecurity posture.

3.4 Secure Supply Chains by Industry

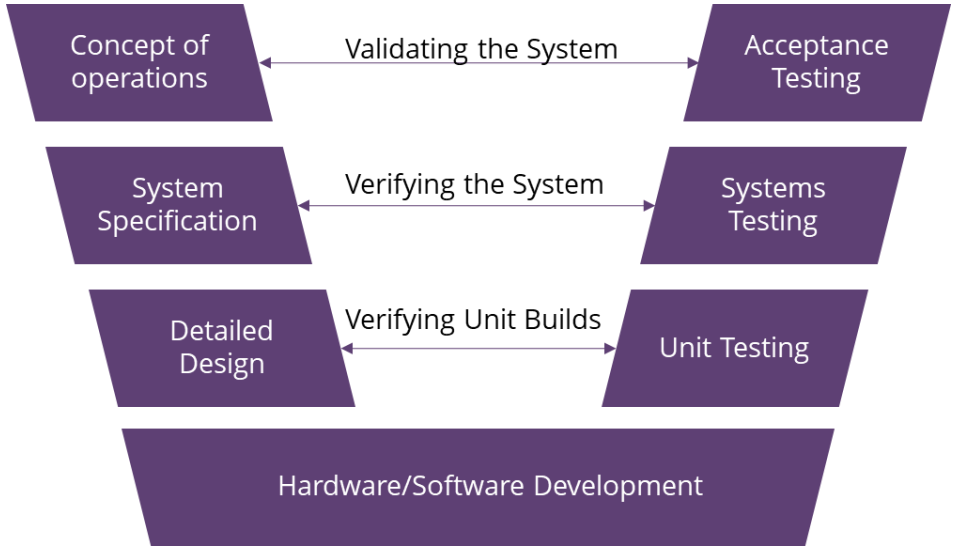
While many elements of the supply chain are similar across industries, there are several concerns that are vertical-specific, thanks to the individual requirements of different supply chains.

3.4.1 Automotive: Software Growth Requires Independent Software Expertise

The latest in standards for automotive supply chains, most specifically ISO/SAE 21434, is a positive step towards further securing the complex automotive supply chain. This new standard's collaboration with industry, including partners like GMV and BlackBerry, means that connectivity and security products that incorporate the standard's provisions will become more common in the coming years. In addition, harmonising the provisions of UNECE WP.29 / R155 with the standard means that automakers and their suppliers will not have to comply with multiple divergent standards, which could potentially undermine requirements for metadata and similar SBoM requirements.

However, these standards will require changes in working practices, as well as a broader range of new software tools to align with these practices. We expect automotive working processes to have to change to incorporate ISO/SAE 21434's required V-model of design. This will necessitate additional dialogue between software providers and all elements of the hardware supply chain, to ensure that both the component parts and systems work together as a cohesive whole. This has the potential to radically transform the design and build of vehicles in future.

Figure 3.2: V-model of Design for Software Development



Source: Juniper Research

In order to ensure that these practices are carried out effectively, automakers will need to bring additional cybersecurity and programming expertise onboard. This will generally mean relying on third-party suppliers for the process themselves, as cybersecurity is not a traditional core competence of vehicle manufacturing.

This will mean the expansion of professional services in automotive supply chain cybersecurity. Specialists onboard who can advise on software supply chain security and manage the required software testing requirements, while keeping the overhead costs of compliance low for the OEMs.

3.4.2 Digital Devices: Hardware Certification Secures Brand Image

For digital device manufacturers, the provision of a SBoM should be standard practice, regardless of a regulatory environment. In the United States at least, the executive order will bring some firms, who have not considered it to date, up to speed with the current practices.

Hardware certification takes on an additional level of importance for these vendors, as anti-counterfeiting measures are linked to brand reputation in a way that such certifications are not in other sectors. Independent verification of elements tied to device warranties and privileges that access to firmware can give a cybercriminal are of particular importance. Vendors should maintain verified and signed confirmations of all elements of their hardware, including the individual elements of a SoC.

This form of certification should be part of standard quality assurance processes if they are not already for certain firms. The absence of centralized standards bodies in this area means that there is little way to compel compliance on individual manufacturers. Instead, OEMs need to make a point of device security and secure manufacture as a selling point, especially in the B2B space, where such concerns often have commercial implications.

Threat Profile: 3CX DesktopApp Software Supply Chain Attack

In March 2023, a zero-day software supply chain attack leveraged the software of a popular phone system developed by 3CX that is used by more than 600,000 companies globally, and more than 12 million individuals. A Trojanized and digitally signed version of the desktop installer is part of an integrated cyberattack campaign that gives threat actors and interactive command shell on infected systems.

The infection starts with a Trojanized installer (MSI) of the 3CX VOIP software. The malicious code allegedly found its way into the release process via a compromised dependency. This means that the installer containing the malicious code was signed with their code signing certificate, so the installer appears perfectly legitimate.

BlackBerry customers were protected from this software supply chain attack for more than two weeks before its general proliferation. While some media reports indicate that this attack may have commenced on March 22 2023, BlackBerry customers using BlackBerry CylancePROTECT® reported convictions a week earlier on March 15. BlackBerry's internal threat intelligence data suggests an even earlier detection date of March 13 where their AI-driven defense models first began blocking malicious code injections (DLLs) associated with the compromised installer.

The Cylance® AI-driven defense model is a battle-proven solution that has been shown to stop more attacks — and earlier in the attack chain — than other models. This is due to the sophisticated algorithms that enable the system to detect and prevent threats before they have a chance to fully execute.

3.4.3 Finance: Third-party Data Moral Hazard Needs to End

The finance industry will remain one of the most compelling targets for cybercriminals, and while current regulations require a degree of due diligence for FIs in undertaking relationships with third parties, these often do not require checking the supplier's current cybersecurity posture, only evaluating its possible risks. FIs need to be able to assess the capabilities of those companies managing their data in more depth, evaluating how the platform they use stores and transmits data, as well as the status of the underlying hardware. This is important with a dispersed workforce as a result of the COVID-19 pandemic,

The industry in some territories has a reasonable framework for undertaking such an awareness, as NIST guidelines for finance (IT asset management, NIST 1800-5A) provides a strong framework for being aware and able to monitor devices and their vulnerabilities in the financial services supply chain. However, identification needs to be able to move into remediation, which is accounted for in current NIST publications, but not frequently emphasized. If this can be linked to fraud prevention then it will gain more traction among FIs, who in a unique take on the "security vs safety" debate, have long had an interest in preventing fraud.

To better practice cybersecurity within their supply chain, FIs need to insist upon greater access to suppliers' software management processes, to be able to better manage vulnerabilities in line with their requirements. On the side of the data management providers, these players need to be able to deliver assurances of precisely how regulations are being met, not just statements of compliance. The current legal frameworks could also be overhauled to lay more liability on third-party financial data handlers, which would incentivise greater levels of security on the supply side in these instances; currently, most systems penalise the FI for incorrect data handling, where it can often by the fault of other data providers. This moral hazard needs to be rectified to help secure the supply chain in future.

3.4.4 Government: Standards Setting Needs to Be Consistent

In many nations, the government's cybersecurity requirements of its suppliers often set the standard for other areas of business. Security is top-of-mind for secret or sensitive information but needs to be constant throughout all levels of government if breaches elsewhere are to be stopped. Smaller entities and smaller discretionary purchases often slip through this net but need to be included in more stringent procurement controls if access points are to be made wholly secure.

The diversity of device requirements and practices within different government bodies is the biggest challenge here. With many different forms of hardware and different requirements of that hardware, making standards more than guidelines a challenge. As a result, they often fall back onto general guides, like the NIST Cyber Supply Chain Risk Management program.

Governments can improve on this by requiring IT security to be more generally involved with IT management and procurement processes, mandating that suppliers provide requirements like an SBoM and device certification standards. Those departments that allow commercially bought devices need to have a robust device management platform in place, and an independent ability to secure a diverse range of endpoints.

Government software supply chains are complicated, with procurement processes also highly complex. Governments must actively work to define the software elements of their supply chain and ensure that vendors meet the standards required, or they risk the loss of highly sensitive data.

Case Study: Phoenix Children's Hospital

Phoenix Children's Hospital in Arizona, US has a wide array of different systems and devices to reconcile. From the data collected and stored in EHRs to sensitive payments information for billing, as well as a range of specialized devices that have to connect to the hospital's network to provide information where it is needed. BlackBerry CylancePROTECT was implemented to replace signature-based antivirus software.

BlackBerry CylancePROTECT provides AI-based endpoint protection, which resides at the OS level once installed, and evaluates files that are present based on an AI algorithm. Although updates to the algorithm are made available, the core function of the algorithm is effective against unknown malware because it evaluates file characteristics without needing to match files to a signature database in need of constant updates. During initial deployment, CylancePROTECT was run alongside the previous endpoint protection software, and detected and remediated multiple threat instances that the previous protection could not address.

This allowed Phoenix Children's Hospital's information security staff to be freed up from the process of constantly updating software to be able to work with BlackBerry's other support teams and strengthen the hospital's security posture further, as endpoint security was no longer an ongoing management process.

3.4.5 Healthcare: Supply Chain & Connectivity Standards Necessary as Digital Healthcare Devices Become More Common

The healthcare industry stands in a strong position to begin reform of its cybersecurity, thanks to an emphasis on device identity in many current standards, particularly within the EU. However, the standards themselves do not consider the software supply chain explicitly, so while the devices themselves can be effectively identified and isolated in the event of vulnerabilities being discovered, that discovery process needs to be strengthened in many cases.

Device access to healthcare networks is another point of vulnerability that needs to be better managed from a supply chain perspective. With many healthcare devices (including in some cases consumer hardware) connecting and providing data to healthcare services for EHRs, there are many possible points of entry for cybercriminals if devices can be compromised. While cellular connectivity is rare in these devices, limiting reach, automated threat creation from infected devices with hardware flaws remains a possibility. This will only increase as connected healthcare overall becomes a more common experience, especially in the wake of the COVID-19 pandemic. Healthcare organizations need to insist that only third-party devices and services that have a strong cybersecurity posture and ability to trace all their actions be permitted to access or contribute to healthcare data. Without this, the landscape will fragment and introduce a landscape of ever-growing healthcare cybersecurity threats.

One solution to this is AI-based threat detection at all healthcare device endpoints, that does not require virus signatures to be effective, but provides probabilistic assessment and remediation. In this way, devices can be left offline indefinitely and still be sure that any malicious compromise of the network (even at the intranet level) will not be able to compromise any devices in use. This will need specific partnerships between cybersecurity companies and device manufacturers, where consumer hardware is used in a healthcare context, but the benefits to both device manufacturer and healthcare provider will be an enhanced level of cybersecurity, ensuring that vital parts of healthcare supply chains and infrastructure remain protected.

3.5 Conclusion

Comprehensive exploration identifies that the software supply chain is a mission-critical entity which affects all organizations who rely on technology to carry out their day-to-day operations. Moreover, significant supply-chain-related cybersecurity risks exist posed by the expanded threat surface spanning both hardware and software, which must be addressed to ensure the *resilience* and *continuity* of those operations.

As such, it is important for all stakeholders to consider how to best approach cybersecurity within their software supply chains. This requires closely examining their current approach, what software and suppliers are involved, and ensuring that appropriate and necessary security mitigations are applied. This can be achieved by identifying and leveraging a cybersecurity partner with the correct set of tools, proficiencies, and expertise to augment existing internal resources. Further research determines that BlackBerry is a seasoned cybersecurity vendor, with the capabilities to secure the supply chain end-to-end and throughout the product lifecycle.

To best secure your operations, there are several software supply chain-related priorities for key stakeholders:

- Know your suppliers: Only by getting deeply involved with their suppliers can private and public-sector organizations determine the full breadth of their software supply chain, and identify risks associated with it. These organization should use the parameters of strict tendering processes that promote SBoM transparency to ensure suppliers are compliant.
- Consider immediate software updates: "Secure now" does not mean "secure later". Staying on top of software updates, throughout the entire software supply chain, is vital to ongoing security. These efforts should be paired with identifying resilient technologies (particularly security solutions) designed with security built in.
- Raise awareness internally: Software elements of the supply chain can "fly under the radar". Only through raising awareness and building hardened processes, can these secure needs be met.

Endnotes

[i] Thomas M. Eisenbach, Anna Kovner, and Michael Junho Lee (2021), Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis, accessed at https://www.newyorkfed.org/research/staff_reports/sr909 in September 2021

[ii] Michael Stone, Chinedum Irrechukwu, Harry Perper, Devin Wynne, Leah Kauffman (2018), NIST Special Publication 1800-5 IT Asset Management, accessed at https://www.nccoe.nist.gov/sites/default/files/library/sp1800/fs-itam-nist-sp1800-5.pdf in September 2021

[iii] Salt Labs (2021), State of API Security, Q3 2021, accessed at https://content.salt.security/rs/352-UXR-417/images/SaltSecurity-Report-State_of_API_Security.pdf in September 2021

[iv] Eisenbach, Kovner & Lee (2021), op cit.

[v] The White House (2021), Executive Order on Improving the Nation's Cybersecurity, accessed at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ in September 2021

[vi] https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

[vii] US Department of Commerce (2021), The Minimum Elements for a Software Bill of Materials (SBOM), accessed at https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf in September 2021

[viii] https://blackberry.qnx.com/en/products/security/blackberry-jarvis

[ix] Ibid.