



The Future of IT Operational Technology Supply Chains

Celia Paulsen

Most data breaches originate in the supply chain. This article seeks to identify policy, technology, and business environment changes that are shaping how organizations will source, buy, build, deliver, dispose of, and ultimately protect IT/operational technology goods and services in the next decade.

Supply-chain risk management has gained significant attention and momentum over the last few years. The supply chain (or value chain) is the network of designers, manufacturers, distributors, and others that work together to provide a product or service to customers. Supply chains are often considered a key component of a business's strategy, enabling an organization to leverage expertise in a different organization and focus only on its key capabilities. Risks to supply chains have traditionally focused

on disruptions and quality control. Over the last decade, as more digital (or cyber) technologies have been developed using complex supply chains, which are, in turn, managed by digital technologies, the idea of cyber supply-chain risk management has taken shape.

For IT and operational technology (OT), this concept was originally directed mostly at protecting against counterfeit products. However, as outsourcing became ubiquitous, it quickly became clear that the supply chain was often involved in every step of a system's lifecycle and represented a key weakness for many organizations. IT-based disruptions (for example, denial-of-service attacks), theft of intellectual property (IP), insertion of

Digital Object Identifier 10.1109/MC.2019.2951979
Date of current version: 15 January 2020

malicious code, inclusion of weak (from a cybersecurity perspective) software or hardware components in a product, or island hopping (using one organization's weak cybersecurity infrastructure as an attack vector to a more lucrative target) are some of the cyber risks impacting the supply chain. In fact, between 50 and 80% of data breaches originate in the supply chain.^{1,2} These risks are difficult to remediate due to the complex, ever-changing, and often proprietary nature of IT and OT. It is no wonder, then, that supply-chain cybersecurity is a top worry for many organizations.

Cyber supply-chain risk management exists in the unique space between many more well-established disciplines. It influences, interacts with, and connects silos such as logistics, inventory management, contract management, economics/accounting, cybersecurity, quality control, sociopolitical risk, business risk management, and potentially a host of other areas. As such, predicting the future of this emerging field relies on an understanding of how each of these intersecting factors is expected to change over the years. This article focuses on the future of technological solutions for supply-chain cybersecurity, but it also touches on the future of the business and political environments.

POLITICS

Nations around the world face the challenge of adapting well-established legal and acquisition frameworks to include the multifaceted problems of supply-chain cybersecurity. In the last year alone, dozens of government initiatives have sprouted in Australia, China, Israel, the United Kingdom, the United States, and others, all looking to address cybersecurity risks emanating

from a complex supply-chain ecosystem. These political efforts to manage or control cyber supply-chain risk are still in their infancy and could change significantly over the next 10 years.


However, because most political environments are notoriously slow moving, reactive, and risk averse, many of the policies we will see in the future will be traceable to what organizations and governments are currently doing. These can be narrowed down to three general concepts: implementing restrictions on purchases, imposing minimum cybersecurity requirements, and investments or incentives.

Several governments have or are developing a means whereby government and critical sector-specific entities will be limited as to what hardware or software they can use or which companies they can do business with. In

unclear how often these methods might be used in the future, but some have predicted that they will become as commonplace and politically charged as tariffs are today.

A related solution that several government entities have or are considering is the possibility of requiring that all or a subset of businesses prove compliance with a baseline of cybersecurity practices. It is an increasingly common practice in industry, but replicating the practice in governments with multiple agencies or entities with differing priorities and complex legislative limits is difficult.

Some suggest the future could mirror what has already been seen with safety. Government-mandated audits, certifications, reporting requirements, and penalties are possible, with different levels of oversight depending on the industry



THESE POLITICAL EFFORTS TO MANAGE OR CONTROL CYBER SUPPLY-CHAIN RISK ARE STILL IN THEIR INFANCY AND COULD CHANGE SIGNIFICANTLY OVER THE NEXT 10 YEARS.

some countries, such requirements are well established and considered part of doing business there. Other countries have only begun to experiment.

There are arguments about the efficacy of white- or black-listing organizations or the technologies they produce, and questions remain as to the criteria for making such decisions. But because they represent a very visible punishment that can potentially be used as political leverage, these methods are unlikely to disappear. It is

and regulatory environment. The first indications of heading in this direction have been seen with the European Union's General Data Protection Regulation and the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Both efforts utilize a model reminiscent of the safety regulations of the industrial revolution, before many data were available to incentivize volunteer compliance, and requirements were based, in part, on untested theories developed by research organizations.

The third political trend can be seen in the investments that governments have and will make into research and development incentives. Investments into technologies, such as artificial intelligence (AI), 5G, advanced manufacturing, cybersecurity education, and sustainable solutions, will continue to have a long-term impact on cyber supply-chain risk well into the future. Unfortunately, this is the polit-

tion for tracking provenance. Although blockchain is incredibly valuable for providing traceability for transactions in a strictly digital realm, the benefits begin to dissipate as it is translated into the physical universe. Questions related to interoperability, speed, privacy, obfuscation, reliability, and completeness have been the focus of much research and standardization efforts but remain unanswered.

ship, all of which will provide data to each other in a standardized, concatenated format to create a kind of metadata-like, hash-chain history of the life of the product and its components. When a product is delivered, a customer will be given a key to decrypt and access all the associated data. The sensors can then be removed, or they can be used to provide additional data back to the manufacturer or for internal inventory management.



THE DEMAND FOR A RELIABLE, BLOCKCHAIN-LIKE SOLUTION FOR TRACKING GOODS THROUGH THE SUPPLY CHAIN IS DEAFENING.



INVENTORY MANAGEMENT

Although technological opportunities around provenance and supply-chain visibility have received a lot of attention, inventory management is an area that has been largely ignored; without it, however, all other solutions fail. The famous adage (often misattributed to Peter Drucker or W. Edward Deming) states, “you can’t manage what you don’t measure,” but how can you measure or manage what you don’t know you have?

Problems associated with obsolete hardware and software—failing parts, unpatched vulnerabilities, and lack of institutional knowledge—highlight the fact that many organizations do not know what they have. The problem is not limited to obsolete products, though. Software often reuses code and takes advantage of libraries. Hardware combines multiple components and seals them into a box. With the Heartbleed vulnerability, it became clear that many end users did not know that OpenSSL was integrated into the software packages they used nor did they know how to find out.

Two efforts have risen in recent years aimed at encouraging software and hardware developers to provide information on what is in their products, or their *bill of materials*. The concept is that developers should provide

ical trend that varies the most among nations and over time, so it is the most difficult to predict.

TRACK AND TRACE

Much attention has been given lately to increasing visibility into the hardware supply chain. Numerous tools have sprung up advertising that they will map a company’s supply chain, track a component as it is integrated and delivered, or monitor suppliers’ compliance with established agreements, among other things. Only a few years ago, knowing a product’s provenance was considered nearly impossible and certainly cost prohibitive. Now, more organizations have processes and tools in place that enable them to document the provenance of at least the critical technology they buy and use.

Blockchain solutions are possibly the most hyped technology advancement in the last several years, and they have been touted as the premier solu-

Still, the demand for a reliable, blockchain-like solution for tracking goods through the supply chain is deafening. As researchers have modified and reframed existing blockchain products to meet the needs of organizations, those solutions have led to something entirely new. In as close as five years, a solution will be developed that is not blockchain but builds on many of the lessons learned from the blockchain hype. Some researchers have considered how related concepts, such as a hash chain, cryptographic audit logs, or Merkle trees, could be a more appropriate solution for a physical world of constantly moving, untrustworthy parts.

It is easy to imagine a future in which manufacturers and distributors around the world will use vendor-agnostic, integrated, standardized, automated, non-blockchain distributed ledger solutions. Companies could have sensors on components, robots building the products, and boxes in which the products will

an ingredients list, similar to what is found on food containers, so that a customer can take appropriate precautions. Both efforts have strong support, but many companies are apprehensive about participating for fear of disclosing their IP or providing information a malicious actor would need to craft an attack.

Over the next several years, many systems used around the world will reach a point where they have not been supported by the original manufacturer for 20 years. There are no authorized replacement parts, and there are no patches to protect the systems from well-known vulnerabilities. However, replacing these systems with newer versions would require an investment that many organizations simply cannot afford. Unless a concerted effort is made to address these issues, there is strong potential for the news to become full of incidents in which obsolete hardware or software failed or was exploited and caused massive disruptions.

COMMUNICATION

Both future provenance and inventory management efforts, along with efforts to automate the manufacturing, warehousing, and delivery processes using self-driving vehicles, drones, and robots, rely on the abilities of devices and organizations to communicate. To secure the supply chain, a data communication protocol or standard set of specifications would be valuable if it supports both anonymity and identity verification and is secure, fast, and reliable.

Secure and reliable information sharing between supply-chain partners has been coveted by industry and government organizations alike for the last 40 years. Everything, from inventory levels, purchase requests, design specifications, bills of materi-

als, and threat indicators, is valuable information in friendly hands; but in unfriendly hands, it could result in significant risk. There is a strong demand for the ability to share this type of information more comfortably and quickly than is possible with existing models based on email, web browsers, or even Bluetooth.

As we move toward automation of processes, leveraging drones, robots, and the Internet of Things (IoT) devices, the need for fast, secure data-sharing protocols, standards, or models becomes obvious. Unfortunately, research into this area has been extremely limited and focused on modeling supply chains, the development of collaboration tools, communication between driverless vehicles, and some initial research on the leveraging X509 certificates for supply-chain data exchange. For future supply chains to fully leverage all of the possibilities associated with the automation of manufacturing and distribution technologies, automated and secure communication techniques will be key.

ZERO TRUST AND ASSUME COMPROMISED

A security concept first articulated in 2010 asks if we can create a secure environment when we don't trust any of the technology that makes up that environment. In September 2019, Bruce Schneier lamented that "we don't even really know how to build secure systems out of secure parts, let alone out of parts and processes that we can't trust and that are almost certainly being subverted by governments and criminals around the world."³

Current zero-trust architectures center on determining how much access a user or device should have, beginning with the assumption that the answer

is none. They are mainly identity- and access-management solutions that integrate continuous monitoring techniques. Using AI or machine-learning techniques, these tools can become sophisticated at identifying anomalous activities. Although these tools have been shown to reduce the potential attack surface and identify new attacks, their usefulness in an already compromised or rapidly changing environment, such as in IT/OT supply chains, is unproven.

One promising conversation in this area is founded on an age-old defense-in-breadth solution: redundancy. Historically, the concept of true redundancy has meant duplicative systems using different suppliers and different components to provide resiliency to a network. Unfortunately, outside of data storage, it is often a cost-prohibitive solution that requires a level of interoperability between technologies not always available.

However, full redundancy may not be necessary. Redundancy in a few key data points will be sufficient to allow a zero-trust AI architecture to know that a system or its supply chain has been compromised. For example, redundant checks on the basic input/output system of a computer can mitigate a significant number of high-impact cybersecurity risks. Data from multiple sensors in an industrial control system can be used to determine if a command received from the control unit might be spurious.

Solutions with these kinds of integrated, zero-trust, and self-monitoring techniques are only beginning to be developed. The next five or 10 years should prove enlightening as we learn where data redundancy can most cost-effectively be used to support zero-trust and self-monitoring solutions. It is not likely that we

will ever be able to completely distrust a supply while being able to trust the products and services it provides. If this were possible, 99% of cyber supply-chain risk-management problems would become null and void. However, any improvement in this area represents a significant step forward.

DIGITAL TWINS

The antithesis of zero trust is designing for security. Poor system or intentionally vulnerable designs can do more to damage an otherwise secure environment than nearly any other hazard. It is impossible to test for all possible weaknesses and unreasonable to expect most organizations to do the kind of advanced testing necessary to discover undisclosed vulnerabilities. Even asking organizations to patch their systems regularly is a major hurdle to cyber supply-chain efforts.

Although there are several movements and trends related to designing for security, one in particular has special implications for the supply chain: digital twins. The concept of a digital twin is that a digital replica of a system exists simultaneously with its physical counterpart. Any change to the physical system is replicated in real time in its twin. Although in its infancy, several companies, such as General Electric, Volkswagen, Tesla, and PTC have experimented with digital twins over the last two years, with positive outcomes. The purpose has generally been to increase efficiency and quality control, but the applications for cyber supply-chain risk are obvious.

Current digital twins are simplified data representations or abstractions of the original product. However, if the idea were expanded and organizations could create an accurate, real-time digital simulation of a product or its supply

chain, the possibilities are tremendous. Some examples could be a “twin” that is able to show when a supplier accesses a specific design file, when a supplier is purchased by another company, or something closer to home such as being able to simulate what will happen to a system if a patch or upgrade is installed. This would be an extremely difficult idea to achieve, but we will likely see many more companies invest in research over the coming years, exploring the digital-twin costs and benefits for the IT/OT supply chain.

ACCOUNTABILITY

Enforcing accountability in cybersecurity has been a challenge since the beginning, but interesting ideas spawning from the open source software realm have the potential to change the conversation. One idea is a merit-based certification system for programmers. This is not a new idea, but it is receiving new life as configuration management systems—and even word-processing applications—are better able to track what changes a user makes to a file.

The idea is that any time a programmer contributes to the development of a software application, he or she would receive points. If the software is well received, the developer receives more points. If specific code is found to contain a weakness (for instance, subject to a Structured Query Language inject), the programmer who wrote it loses points. Users would be able to award and deduct points from each other, but a moderator would be needed. Once a programmer receives a certain number of points, he or she would receive a badge (gold, silver, or bronze). Programmers could request payment for job requests based on their badges.

A similar idea has been proposed for technology manufacturers, but organizations would receive ratings based on how many weaknesses cybersecurity researchers find in their systems and how many known vulnerabilities are found. Both models require a federated approach where scores can be validated and verified and a significant user base before they become useful. Questions also remain related to how persons or organizations would appeal a rating.

Neither of these ideas will likely survive in their current form, but it is possible that some variation will be adopted, or, perhaps, there will be better ways for information about the quality of software and hardware devices to be measured and shared. Either way, whether access to such information would influence customer behavior remains to be seen.

THE SUPPLY-CHAIN ECOSYSTEM

Figure 1 shows a notional model loosely describing four types of supply-chain environments. This model has not been extensively validated, but it has initially proven valuable for discussing IT/OT supply-chain trends. The vertical axis relates to the number of tiers of suppliers involved or how many organizations exist between the raw materials and the end user. The horizontal axis shows how complex the product (hardware, software, firmware, service, or other IT/OT-related product) is. This complexity takes into consideration how many different components make up the product and how difficult it is to produce. The four resulting quadrants are creation (low complexity, few tiers), brokerage (low complexity, many tiers), assembly (high complexity, many tiers), and aggregation (high complexity, few tiers).

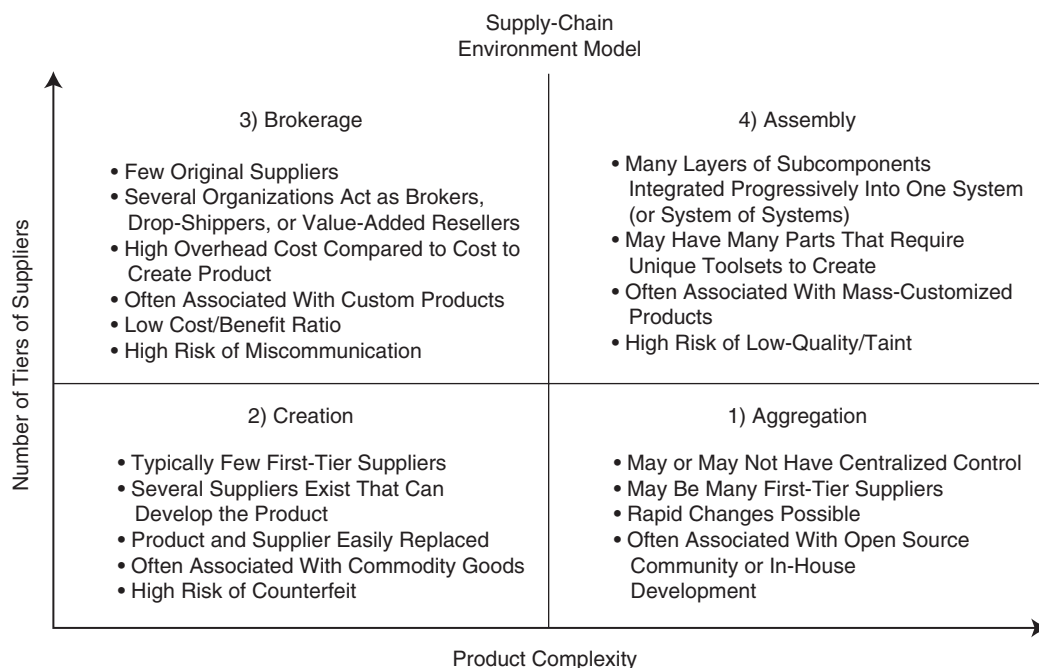


FIGURE 1. The types of supply-chain environment.

The technology industry supply chain as a whole has traveled through each of these quadrants. (Individual organizations may or may not have followed this path.) Early computers were relatively complex for the time but developed by a specialized team of engineers and programmers (quadrant 1, aggregation). As manufacturing processes for technology improved, computers generally became easier to make, and several manufacturers began developing computers or their parts (quadrant 2, creation). Then, the business model shifted to outsourcing and re-outsourcing; organizations became specialized, and low-cost contracting and drop-shipping models took shape (quadrant 3, brokerage).

Beginning in the late 2000s, the industry largely moved to an assembly model (quadrant 4). The focus again turned to increasing the complexity

of products, partly to avoid IP theft or counterfeiting but also to satisfy a self-perpetuating demand for upgrades. This has created the perfect storm for cybersecurity risks. The large number of outsourcing tiers resulted in an opportunity for a malicious or unqualified entity to insert itself into the supply chain. Unfortunately, due to the high complexity of the product, any wrench thrown into the machine would not be seen immediately but could cause a lot of damage.

INDUSTRY 4.0

The amount of effort to maintain and ensure cybersecurity while at a high degree of product complexity and with many tiers of suppliers is untenable for many organizations. Already, there have been indications that the industry is moving to a different model, but it is not a new quadrant—it

is one we've seen before: the aggregation quadrant.

In the new version of this quadrant, organizations will have many first-tier suppliers able to develop complex machines, but fewer subassemblers and subsuppliers. This is driven, in part, by advances in system design and manufacturing technologies (Industry 4.0). Outsourcing was partially necessary to ensure cost-effectiveness in the use of specialized machinery. However, additive manufacturing and flexible factories allow a system where organizations can produce very few iterations of a part cost-effectively. Although these benefits have not yet reached into firmware and integrated circuit supply chains, there is a significant amount of research being conducted to remedy that.

The Industry 4.0 model has many implications for cyber supply-chain

ABOUT THE AUTHOR

CELIA PAULSEN is a cybersecurity researcher for NIST. She received an M.B.A. in information assurance and security management from California State University, San Bernardino. Contact her at celia.paulsen@gmail.com.

risk. Most obviously, the cybersecurity of the industrial control systems, IoT devices, and other technologies used to enable this new manufacturing model are critical. It is less obvious that this model has significant implications for the gray market. One reason organizations have struggled with obsolete hardware is because manufacturers could not justify making one-offs.


For many years, there have been organizations willing to reverse-engineer any part a customer might need replaced, but these organizations were either extremely cost prohibitive or untrustworthy. With the Industry 4.0 revolution, this will no longer be a major stumbling block. Currently, organizations scramble to find replacement parts for which manufacturers no longer even maintain designs. In the future, a model could be conceived in which, once a manufacturer decides it won't manufacture a part any longer, it would put the design into escrow. When a customer needs a replacement, he or she would contact the escrow organization, which would make arrangements for a part to be manufactured by a local, trusted flexible factory and pay the manufacturer, minus a service fee.

Some assume that the focus on supply-chain risk is hype and will subside eventually. A

new threat will emerge that will shift people's attention, and supply-chain risks will no longer be a priority, or a solution will emerge that will become commonplace, and board rooms will not be interested in a solved problem. Both are possible. However, the interconnected nature of the world is likely to only increase as technology becomes cheaper and more ubiquitous, and threats to technology will change as readily as the technology itself changes. Managing the risks associated with the interconnected nature of technology supply chains will be a challenge long into the future, requiring ever-changing technological, business, and government solutions.

As manufacturers embrace automation and other tenants of the Industry 4.0 technology revolution, the economic model surrounding supply-chain risk management will change. A move to fewer tiers of outsourcing will be incidental to other business decisions but greatly simplify the third-party attack-space risk professionals must manage. The political environment will move in fits and spurts in this area, according to national priorities. However, organizations can expect that governments will try not to reinvent the wheel if they do not have to.

Ideally, as technologies are developed that can mitigate supply-chain risks or aid in the management of such risks, organizations will be able to

move from manual oversight practices to automated monitoring and decision making. However, all of the technological solutions mentioned in this article rely on the ability to quickly, securely, and automatically communicate data between systems and organizations. This is a challenge due to technical limitations and conflicting political and business drivers. Still, the emerging technological solutions that could be used for cyber supply-chain risk management are promising. 

REFERENCES

1. "Quarterly incident response threat report," Carbon Black, Waltham, MA, Nov. 2018. [Online]. Available: <https://cdn.www.carbonblack.com/wp-content/uploads/2018/10/carbon-black-quarterly-incident-response-threat-report-november-2018-0119.pdf>
2. D. Shackelford, "Combatting cyber risks in the supply chain," SANS Institute, Bethesda, MD, Sept. 2015. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/analyst/membership/36252>
3. B. Schneier, "Supply-chain security and trust," *Schneier on Security*, Sept. 30, 2019. [Online]. Available: https://www.schneier.com/blog/archives/2019/09/supply-chain_se_1.html

DISCLAIMER

The identification of technologies in this article does not imply recommendation or endorsement by NIST or other agencies of the U.S. government. This article reflects the author's opinion and not that of the U.S. Department of Commerce or NIST.