Supply Chain Trust

By: Nir Kshetri and Jeffrey Voas

Kshetri, Nir and Voas, J. (2019)."Supply Chain Trust", *IEEE IT Professional* 21(2).

Made available courtesy of IEEE: https://doi.org/10.1109/MITP.2019.2895423

Abstract:

Reports on supply chains as major sources of cybersecurity threats. Companies and organizations increasingly share data, credentials, software code, applications, networks, and infrastructures with “trusted” supply chain partners. Supply chains can be sources of cybervulnerabilities. One estimate has suggested that supply chains account for 80% of all cyber breaches. Insecure supply chains have fostered well-known cyberattacks. In a quest to break large organizations' networks, cyber-criminals may look beyond the first-tier supply chain partners.

Keywords: Supply chains | Companies | Blockchain | Computer hacking | Computer crime | Computer security | Software development | Malware

Article:

Organizations increasingly share data, credentials, software code, applications, networks, and infrastructures with “trusted” supply chain partners. Supply chains can be sources of cyber-vulnerabilities. One estimate has suggested that supply chains account for 80% of all cyber breaches (https://www.industryweek.com/supply-chain/can-t-turn-back-time-cybersecurity-must-be-dealt). Insecure supply chains have fostered well-known cyberattacks.

In a quest to break large organizations’ networks, cyber-criminals may look beyond the first-tier supply chain partners. According to Accenture’s Cyber Threatscape Report (2018), hackers have an increased focus on exploiting third- and fourth-party supply chain partners to infiltrate large organizations.[1] Another trend has been attacks on hardware products via backdoors and with malware insertion.[2]

VULNERABILITIES AND EXPLOITS

Supply chains are vulnerable and subject to exploitation. Table 1 provides examples.

Consider software development. By attacking smaller software providers, hackers have been able to infiltrate larger organizations that rely on software. For example, in a British Airways (BA)

case, hackers attacked third-party code that ran payment authorization by injecting their own malicious code into it. This meant that the hackers did not need to access or penetrate BA networks.[4] The hackers also obtained CVV numbers, however BA reported that it had not stored the CVV numbers. This suggests that the CVV numbers were intercepted when transactions occurred (https://www.bbc.com/news/uk-england-london-45440850). According to the cyber security company RiskIQ, the BA hackers employed a "cross-site scripting" attack. In such attacks, criminals exploit a third-party website to launch cyberattacks against other entities. Nation-states can also exploit supply chains for spying. For example, according to the cyber-security company Area 1, several nations may have collaborated to launch a cyberattack on 4the Saudi oil company Aramco in 2017 (https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/).

Table 1. Examples of cyberattacks involving supply chain partners

Organization	Reported in	Effect	Supply chain partner compromised
Equifax	2017	143 million people	Flaws in the enterprise platform (https://www.wired.com/story/equifax-breach-no-excuse/) that collected website performance data and served malicious content (http://www.latimes.com/business/la-fi-equifax-social-security-numbers-20171012-story.html).
Target	December 2013	40 million credit and debit-card accounts and 70 million people.	Started with stealing credentials of Target's HVAC vendor (https://www.csoonline.com/article/2601021/security0/11-steps-attackers-took-to-crack-target.html). The hackers then used the stolen credentials to gain access to Target-hosted web services that were dedicated to vendors.
Ticketmaster	Early 2018	40 000 U.K. users	Customer-service chatbot supplied by a third-party (https://www.bbc.co.uk/news/technology-44642567).
British Airways	September 2018	380 000 customers	Third-party software code used to run payment authorization.

CHALLENGES

Challenges exist in securing supply chains. For example, companies may assign a lower priority to supply chain risks than other types of risks. A survey conducted among the members of Consumer Packaged Goods Vertical Strategy Group revealed that while 100% of the respondents assessed IT risks, only 75% assessed supply chain risks. Likewise, only 75% considered minimizing supply chain cyber risks as a third-party risk management goal.[3] Furthermore, although most organizations conduct annual risk assessments, those may be insufficient to deal with the challenges facing supply chains (https://thehill.com/blogs/congress-blog/technology/403958-washington-to-finally-focus-on-threat-to-supply-chain-risk). Trust in any supply chain is a complex problem that is hard to measure and achieve. Supply chains of large organizations are often complicated and involve large numbers of partners and products. For example, one cybersecurity firm noted that one of its client's supply chains involved more than 5000 companies (https://finfeed.com/small-caps/technology/british-airways-data-breach-throws-whitehawks-us-government-contract-into-light/). Thus, it is challenging to monitor supply chains with so many stakeholders involved, and particularly in real-time. A survey found that 72% of companies lacked full visibility into their supply chains.[4]

While the problem has been recognized since the 1970s, the severity of this issue is compounded by the rapid internationalization of technology and the global division of labor

(https://krebsonsecurity.com/2018/10/supply-chain-security-101-an-experts-view/). Simply blocking foreign companies from being dominant suppliers may not be effective. For example, China controls of a large proportion of the global supply chain yet offers no guarantee that their products have security built-in since the designs of those products may occur in other countries (https://www.nytimes.com/2018/10/12/technology/the-week-in-tech-fears-of-the-supply-chain-in-china.html).

In some countries, electronic components produced in those countries are sold by various "white label" firms. If security flaws are identified in components that were "white labeled," it may be difficult to know which companies white-labelled a specific component, and it will be difficult to inform consumers about these flaws. In another scenario, when a security hole is found in a specific vendor product, that vendor may simply go out of business and restart under a different name (https://krebsonsecurity.com/2018/10/supply-chain-security-is-the-whole-enchilada-but-whos-willing-to-pay-for-it/). And when white-labeling occurs, the original manufacturer may have little incentive to increase trust in their products beyond what the rebranding companies require.

Another problem is related to the lack of regulatory and enforcement mechanisms. Some government methods for monitoring supply chain trust focus more on preventing counterfeit products than on espionage activities (https://www.techrepublic.com/article/5-tips-to-secure-your-supply-chain-from-cyberattacks/).

And finally, consumers are often more interested in price and functionality. Increased security often makes devices slower and more expensive. Moreover, security flaws may not directly affect device owners but affect others. Even if owners know that their devices are being used to launch cyberattacks, the end-victims are often unknown. Manufacturers have few incentives to make securer devices until customers demand it.

POSSIBLE APPROACHES

Table 2 presents four potential avenues for enhancing supply chain security and trust.

Governments

Regulatory measures are one approach intended to increase supply chain trust. Efforts to do this have already been undertaken. In September 2018, the Trump Administration released a National Cybersecurity Strategy that requires federal agencies to invest in more secure supply chain technologies (Feldman, 2018).[5]

There have also been attempts to introduce formal legislation to increase trust in supply chains. In September 2018, the U.S. Senate Homeland Security and Governmental Affairs Committee approved the Federal Acquisition Supply Chain Security Act. The Act is intended to improve information sharing within the intelligence community. It also establishes an inter-agency process to exclude companies from contracting with the federal government if it deemed that they may pose threats to the federal supply chain.[6]

Table 2. Possible measures at various levels to secure supply chains

Level	Mechanisms	Examples/Remarks
National/state	Increasing investment in technological and human capabilities. Introducing formal legislation to secure supply chains. Increasing awareness of supply chain risks and providing guidelines to strengthen security.	The U.S.: National Cybersecurity Strategy requires federal agencies to invest more in secure supply chain technologies. The Federal Acquisition Supply Chain Security Act. DHS guidelines that outline device manufacturers' roles and obligations surrounding IoT security.
Industry group/trade association	Fill the regulatory vacuum. Resource and expertise advantages.	Diverse networking, engineering, financial, electronics, cybersecurity, and blockchain businesses team to develop blockchain functionality to improve supply chain trust.
Manufacturers and service providers	Ensure that supply chain partners follow security standards. Continuously monitor supply chain cyber risks. Develop and implement new ways to assess and deal with supply chain risks.	Organizations employ Cyber Risk Frameworks to identify risks associated with subcontractors.
Consumers	Purchasing power.	Changing consumer mindset to require vendors to follow responsible security practices.

Government agencies have also taken steps to increase awareness of supply chain risks by providing guidelines to strengthen security. In 2013, the U.S. Department of Homeland Security (DHS) released guidelines that outline device manufacturers' roles and obligations related to IoT security. DHS urged companies producing IoT products to "build security in" at the design phase.

Government stakeholders can also consider teaming with private sector stakeholders to monitor vulnerabilities and share relevant information. This could lead to greater awareness and recognition of supply chain cyber-threats (https://www.weforum.org/agenda/2018/06/managing-risk-in-the-energy-sector-s-cyber-supply-chain). A recent report by MITRE on securing the U.S. Pentagon's cyber supply chain recommended the establishment of a National Supply Chain Intelligence Center. The report recommended that the Center be co-led by civilian and military agencies (Https://Advance.lexis.com/api/document?collection=news&id=urn:contentItem:5TG6-7771-JBHM-S2HW-00000-00&context=1516831).

Industry and Trade Associations

Industry groups and trade associations may also be able to play a role here.

One is an example of this occurred in January 2017; a group including Cisco, Bosch, Bank of New York Mellon, Foxconn, Dutch cybersecurity company Gemalto, and other blockchain startups came together to develop a team that plans to establish blockchain protocols for IoT devices, applications, and networks (bit.ly/2kNtm7w).

Note that blockchain has the potential to strengthen supply chain trust. Blockchain can facilitate the handling and dealing with crisis situations such as product recalls. Blockchain's public transparency offers traceability allowing for a backward trace to the origin of a final product's raw materials. Furthermore, transactions recorded in blocks might be able to predict and identify the end-users of vulnerable products.

The reason that blockchain holds promise here is that the blocks can register the time of transaction, the location of transaction, price, parties involved, and other information as an item changes ownership and moves through a work flow or manufacturing process. Blockchain's distributed ledger technology can also track raw materials as they move through a supply chain over time. Blockchain can also register updates, patches, and part replacements applied to end-products throughout their lifetime. This offers tracking of vulnerabilities and notifications for end-users.

MANUFACTURERS AND SERVICE PROVIDERS

Manufacturers and service providers can leverage their buying power to strengthen trust in supply chains. How? They can evaluate the security practices of supply chain partners and insist that applicable security standards are followed. Furthermore, compliance can sometimes be mandated through contracts (https://www.cbronline.com/solutions/us-organisations-not-battle-ready-in-war-against-cybercrime-4280918/), however, determination of compliance is often elusive.

Manufacturers and service providers may also consider developing new ways to assess and mitigate supply chain risks. For example, artificial intelligence and machine learning may be able to fight specific types of malware attacks in software supply chains. Over time, such tools "learn" to detect unusual patterns in various supply chain environments (http://www.cioandleader.com/article/2018/02/22/india-invest-heavily-ai-based-tools-counter-cyber-attacks-cisco). IBM's AI platform, Watson, is being used to provide predictive analytics to minimize disruptions and risks (https://www.forbes.com/sites/andrewarnold/2018/05/26/how-the-internet-of-things-impacts-supply-chain/).

Solutions that focus on risks associated with supply chain partners, subcontractors, and vendors can also be employed. WhiteHawk's 360 Risk Framework evaluates software vendors and service providers. The first customer of WhiteHawk's product was a U.S.-based financial institution whose goal was to identify the institution's exposure to cybersecurity risks induced by its 50 most important subcontractors. The identified subcontractors were expected to address their cyber risks (https://finfeed.com/small-caps/technology/whitehawk-wins-us325k-first-sale-cyber-risk-product/).

And finally, it may be useful to contract for the external services that will continuously monitor the cyber risks associated with third-party vendors (https://threatpost.com/five-weakest-links-in-cybersecurity-that-target-the-supply-chain/137453/). Realize that if only an annual risk assessment is performed, security problems may be discovered too late for mitigation and after damage occurs. More frequent assessments should provide a fuller picture of supply chain risks so that more timely mitigation measures can be applied.

CONSUMERS

Consumer buying power can also be leveraged to strengthen supply chain trust. For instance, consumers could add pressure to manufacturers to incorporate security "best practices" into development life cycles. If consumers demanded more secure products and services,

manufacturers might be more likely to source their components from contractors with known and demonstrated levels of security.

An encouraging trend here involves consumer mindset. Recent surveys have suggested that consumers expect businesses to follow responsible security practices. According to the RSA Data Privacy & Security Report that was based on a survey of 7500 consumers in France, Germany, Italy, the UK and the U.S., 62% of the respondents said that they would blame the company, not the hacker, if their data is breached.[7] Likewise, a survey of 1000 U.K. consumers commissioned by FireEye indicated that 72% of consumers would stop purchasing from a company if a security breach was found to be linked to the company's failure to prioritize security and privacy (http://www.itproportal.com/2016/05/11/high-profile-data-breaches-affecting-consumer-trust-in-big-brands/).

SUMMARY

Supply chains are increasingly vulnerable and threatened. Trust in supply chains is a difficult proposition. Adversaries can inject malware and other malicious defects anytime during manufacturing and design. And it is hard to assess trust for international supply chains.

The problem of trusting supply chains is unlikely to go away soon. It is an analogous problem to that of drug smuggling—smugglers continue to find new ways to hide their illegal products during transport while law enforcement tries to catch up. So, in closing, let us revisit our title: *Supply Chain Trust*, a topic that is both timely and timeless. Is trust here possible? "Yes," but with caveats, and probably many.

DISCLAIMER

The authors are completely responsible for the content in this paper. The opinions expressed here are completely their own.

REFERENCES

1. J. Ray et al., "Cyber threatscape report 2018", 2018, [online] Available: https://www.accenture.com/gb-en/insights/security/cyber-threatscape-report-2018.

2. L. Newman, "There's no good fix if the supply chain gets hacked", 2018, [online] Available: https://www.wired.com/story/supply-chain-hacks-cybersecurity-worst-case-scenario/.

3. "Consumer packaged goods sector needs decisive unified action in the face of third party risks", Oct. 3, 2018, [online] Available: https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:5TD9-23N1-J9XT-P0J4-00000-00&context=1516831.

4. P. Myerson, "Can't turn back time: Cybersecurity must be dealt with", Jan. 2017, [online] Available: https://www.industryweek.com/supply-chain/can-t-turn-back-time-cybersecurity-must-be-dealt.

5. V. Feldman, "Trump administration moves to address cybersecurity concerns congress funds cyber programs" in Nat. Law Rev., 2018.

6. Oct. 4, 2018, [online] Available: https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:5TDG-6NR1-DY0P-G376-00000-00&context=1516831.

7. M. Nadeau, "General data protection regulation (GDPR) requirements deadlines and facts", 2018, [online] Available: https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html.