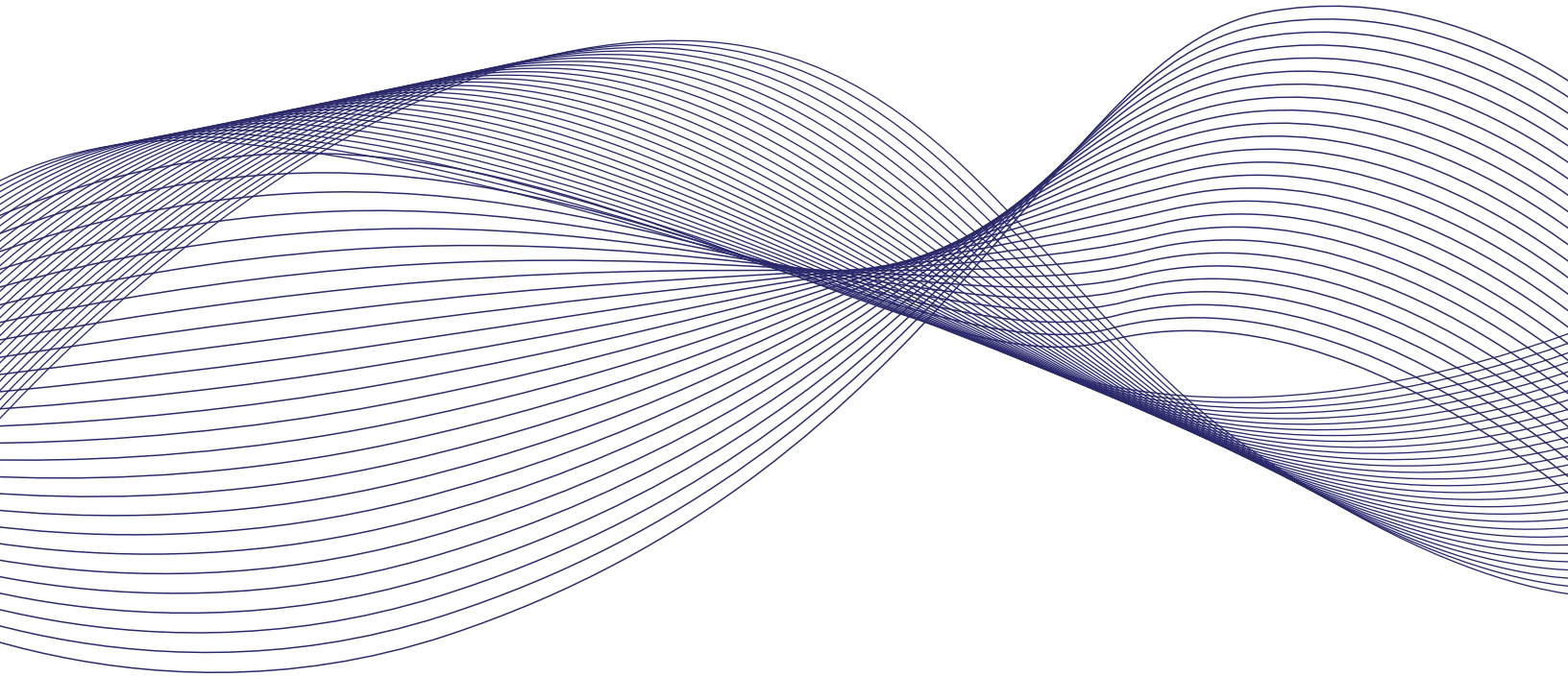
Visa
Economic
Empowerment
Institute

Fostering Digital
Equity and Inclusion

Demystifying cyber supply chain security and zero trust architecture
for small businesses

Jonathan Davis and Erin English



VISA

Synopsis

Software supply chain attacks have proliferated in the last few years. These attacks often have ripple effects given the growing complexity of today's digital supply chains, software, and services. Small businesses, many of which have adopted digital solutions to better weather the effects of the COVID-19 pandemic, are particularly vulnerable to these types of threats. This paper describes how small businesses can implement an effective cyber supply chain risk management system and offers a set of actionable steps that small firms can take to protect their supply chains and customers as they do business in the digital age.

Fostering Digital
Equity and Inclusion

Demystifying cyber supply chain security and zero trust architecture
for small businesses

Visa Economic Empowerment Institute

VISA

Acknowledgments

This paper is the second in VEEI's series on keeping small businesses secure, following *Keeping the lights on for small businesses: Safeguarding the payments ecosystem during the pandemic*. The authors gratefully acknowledge the contributions of Kristina Breen, Chad Harper, Marie Jordan, Barbara Kotschwar, and Megan Malone. We recognize with appreciation the editorial assistance provided by the team at Closeup Content and the design team from 451.

About the Visa Economic Empowerment Institute

The VEEI is a non-partisan center of excellence for research and public-private dialogue established by Visa.

The VEEI's overarching mission is to promote public policies that empower individuals, small businesses, and economies. It produces research and insights that inform long-term policy within the global payments ecosystem. Visa established the VEEI as the next step in its ongoing work to remove barriers to economic empowerment and to create more inclusive, equitable economic opportunities for everyone, everywhere.

Visit: visaeconomicempowermentinstitute.org

Index

Introduction

Beginning in late 2020 and extending to the summer of 2021, a series of complex cyberattacks struck thousands of enterprises of all sizes. As in other cyberattacks, many of the victims were affected at approximately the same time. But the cyber criminals did not attack the victims directly. What happened was far more unsettling: The attacks came from businesses the victims trusted.

The cyberattacks against SolarWinds, Microsoft Exchange, and Kaseya that occurred during this period can be classified as software supply chain attacks (Higgins, 2021). In these types of attacks, cyber actors infiltrate a software vendor's network, employ malware that compromises the vendor's software, and then proliferate as the vendor deploys its software to its customer base (Cybersecurity Infrastructure Security Agency [CISA], April 2021). Software supply chain attacks like these rarely affect just one company; they often have ripple effects given the growing complexity of today's digital supply chains, software, and services. Many businesses, particularly small and medium-sized ones, work with a network of trusted partners and suppliers, including software providers. Those connections can present a security blind spot for business owners and chief information security officers charged with protecting these companies. For example, as cyber actors look for novel ways to attack, they are increasingly finding opportunities through third-party software and services provided by managed service providers (MSPs). The attackers' goal is to scale their reach by gaining access to other targets through a third party.[1]

These complex cyberattacks against software supply chains have received the right public response from the US government. First, President Biden issued an executive order to improve the nation's digital supply chains (White House, 2021). Then the US Commerce Department and Department of Homeland Security issued a report on how to improve the security and resilience of information and technology supply chains (US Commerce Department et al., 2022). And finally, in February 2022, the National Institute of Standards and Technology (NIST) began the process of updating and improving its Cybersecurity Framework (CSF).[2] In this instance NIST called for a public-private partnership to help launch a "National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains" (NIST, 2022).

Although the overall US response has been robust, more work needs to be done to build toolkits derived from cybersecurity standards, and to make them accessible to small businesses. Small businesses need to take steps immediately, and understand how those steps complement other checklists they may have already put in place, such as the CSF.

The purpose of this paper is to not only answer NIST's call, but also ensure this initiative includes, and provides solutions that are accessible for, small businesses. To defend against these types of attacks, businesses of every size can begin by applying two complementary NIST security approaches:

(1) A robust cybersecurity supply chain risk management (C-SCRM) program to secure the part of the digital supply chain *outside* an organization's direct control.

(2) A zero trust security architecture (ZTA) to secure resources within the company's control.

Many businesses, while realizing the criticality of ZTA, may still be uncertain about how to implement this approach due to the perceived costs of putting it in place (Ramel, 2021).

Cybersecurity is often referred to as a team sport. Each member plays a particular position in order to ensure the overall integrity of an ecosystem that benefits all participants, large and small. In addition to helping secure enterprises and value chains, team members share experiences and lessons learned. Visa, as a network of networks, maintains a unique perspective on the payments ecosystem. Connecting to so many issuers, acquirers, processors, financial service providers, merchants, individuals, and even governments has provided the company clear insights into the cybersecurity landscape. For Visa, this means ensuring the overall integrity and resilience of these networks by committing to drive best practices in cybersecurity—in the private sector and with governments—to make the shared infrastructures even more secure.

In a team sport, it is not enough to have all the participants on the field; they must also be following the same playbook. Cyber actors thrive on complexity and confusion, which means these best practices in cybersecurity need to be widely available, understood, and rehearsed.

Why small businesses are particularly vulnerable to digital supply chain attacks

Businesses increasingly have embraced digital solutions—often from third-party providers—in response to rising demand for online sales during the pandemic. Both small and large organizations depend on an agile but complex network of suppliers that provide critical services. Indeed, many businesses may not even be aware of the full extent of their dependency; as many as a third of businesses are uncertain how many suppliers they actually use (Muncaster, n.d.). As the cost barriers to starting a business are lowering, and the speed to market entry is rising, smaller organizations—often with less cybersecurity sophistication—are at greater risk from suppliers or subcontractors they know little about. Not surprisingly, cyber actors now try to exploit these complex systems because they likely know that enterprises put a large amount of trust in third parties to provide internet connectivity; manage or host critical services; and provide software, hardware, or other solutions. This weakness was well known to cyber-threat actors even before the pandemic. According to data from Marsh McLennan, supply chain attacks grew by a staggering 430 percent between 2019 and 2020 (Marsh McLennan, 2021). More recently, the European Union Agency for Cybersecurity (ENISA) said it was likely that the number of software supply chain attacks grew fourfold from 2020 to 2021 (European Union Agency for Cybersecurity [ENISA], 2021).

Without rigorous cybersecurity and risk management practices in place, these interconnections can create a "weakest link" phenomenon that puts other participants, their clients, and customers at risk. According to the United States Cybersecurity Infrastructure Security Agency (CISA), "Customers often accept third-party software defaults without investigating further, allowing additional accessibility vectors." (CISA et al., 2021). An unsettling concern for small businesses is that their business partners may perceive them to be that weakest link. According to a January 2022 survey from the World Economic Forum, "Small and medium-sized enterprises (SMEs) are seen as a key threat to supply chains, partner networks and ecosystems. In our research, 88 percent of respondents indicate that they are concerned about cyber resilience of SMEs in their ecosystem" (Pipikaite, 2022).

Small businesses are hyper-aware of the risks cybersecurity vulnerabilities may pose, but they may not feel sufficiently prepared to counter these threats. As discussed in another recent report from the Visa Economic Empowerment Institute (VEEI), micro and small businesses placed cybersecurity capabilities at or near the top of their needs for weathering the pandemic (Harper, 2021). However, understanding cyber threats as a top risk concern is not the same as knowing how to effectively mitigate that risk. A 2022 PwC survey of global businesses found that only 40 percent of survey respondents understood the risk of data breaches from third parties, and more than half of the respondents had taken no actions to mitigate third-party cyber risks (PwC, 2022).

Implementing an effective cyber supply chain risk management program

ENISA describes software supply chain cyberattacks as having two main parts: "the attack on the supplier and the attack on the customer. Each of these attacks is usually complex, requiring one attack vector, one plan of action, and careful execution." In order to protect against cyber threats, organizations need to think critically about the security of their suppliers and conduct effective oversight. More to the point, small businesses need a manageable way to mitigate third- and fourth-party risk. With this understanding, security managers in small businesses should try to implement the principles detailed in the checklist below.[3]

- **Create collaborative roles, structures, and processes for your digital supply chain.** Cybersecurity is not the sole responsibility of the chief information security officer or head of technology. Every person in any organization, regardless of size, interacts with third-party products and services. Small-business owners need to understand which individuals come into contact with third parties, and then develop policies for how they manage these relationships. Beyond policy and defined roles, it is critical to establish trusted relationships and open communications with key third parties.

- **Determine supplier criticality by using industry guidelines and best practices.** There are several NIST and Federal Financial Institutions Examination Council publications that detail how to evaluate supplier criticality. Nevertheless, the first step in evaluating a supplier is to learn whether they have access to or store critical data for the small business—particularly regulated data, such as cardholder data, sensitive personal information, or health information. Businesses should plan for scenarios in which a supplier suffers a data breach, experiences a service outage or disruption, or otherwise introduces the risk of a cyberattack to the whole network.

- **Integrate cybersecurity best practices into the system and product life cycle.** As technology products and services age, they typically become more vulnerable to cyberattack. It's critical for small businesses to identify regular maintenance cycles and ensure they have installed the latest security updates and patches. Frequently, suppliers may terminate a product or service offering, or supply chains may be disrupted by other factors. Depending on the nature of the service, this could lead to business interruption or unacceptable levels of cyber risk, such as a situation where the product continues to work, but is no longer supported by the vendor. That's why it's important for small businesses to plan ahead and define product and service life cycles, including knowing what to do when products or services reach the end of their life.

- **Include key suppliers in contingency planning incident response , and disaster recovery planning and testing.** Nearly every business, regardless of size, has a cybersecurity response plan that includes how every employee will respond to a cyberattack. However, those plans should now include suppliers as well. This means proactively making the supplier part of the response plan, establishing rules for how information will be shared, and following protocols for how to share information about software vulnerabilities.

- **Use reputable third-party assessments, site visits, and formal certification to assess critical suppliers.** If practicable, businesses should also be able to visit their suppliers, or verify their third-party risk assessments. Businesses should prioritize these assessments or visits to suppliers that have access to critical network services (Boyens et al., 2021).

As a final consideration, it's important for small businesses to keep in mind that without well-written contracts, it can be very difficult to manage supplier risk. Wherever possible, organizations should ensure that minimum cybersecurity requirements clauses are included in supplier contracts. One of the most important requirements is the right to audit a critical supplier's cybersecurity risk management practices (Grance et al., 2011). If securing the right to audit isn't possible, it's still critical to agree on some minimum cybersecurity requirements or assurance. Other items to consider including in contracts are named cybersecurity contacts and cybersecurity key performance indicators (KPIs).

Checklist

Questions for security managers:

- ☐ Do you have a comprehensive list of all the third-party products and services your business depends upon?
- ☐ Do you have a policy to track and manage these relationships according to the risk or criticality of the service?
- ☐ Which vendors have access to the business's critical data? If a vendor's services went down, what would the impact to your business be?
- ☐ Have you prioritized your critical supplier relationships to understand the risks associated with each one?
- ☐ Do you have a contingency plan for supply chain interruption?
- ☐ Do you know which of your critical products and services are approaching the end of their life?
- ☐ How will you evolve your business processes to maintain adequate security and ensure continued availability for your own product and service offerings?
- ☐ Are you at risk of vendor lock or have you identified alternatives to help ensure resilience?
- ☐ Does your cybersecurity response plan include contacting your software suppliers and vendors?
- ☐ Conversely, do you know if your suppliers include your business in their own cybersecurity response plans?
- ☐ Does your cybersecurity plan include a communications protocol that clearly defines what incident information to share when, and with whom?
- ☐ Does the response plan include any regulatory obligations such as reporting timelines?
- ☐ Have you asked your suppliers if their cybersecurity posture has been assessed by an independent third party?
- ☐ Does your supplier have an industry-recognized assessment report or certification it can share with you?

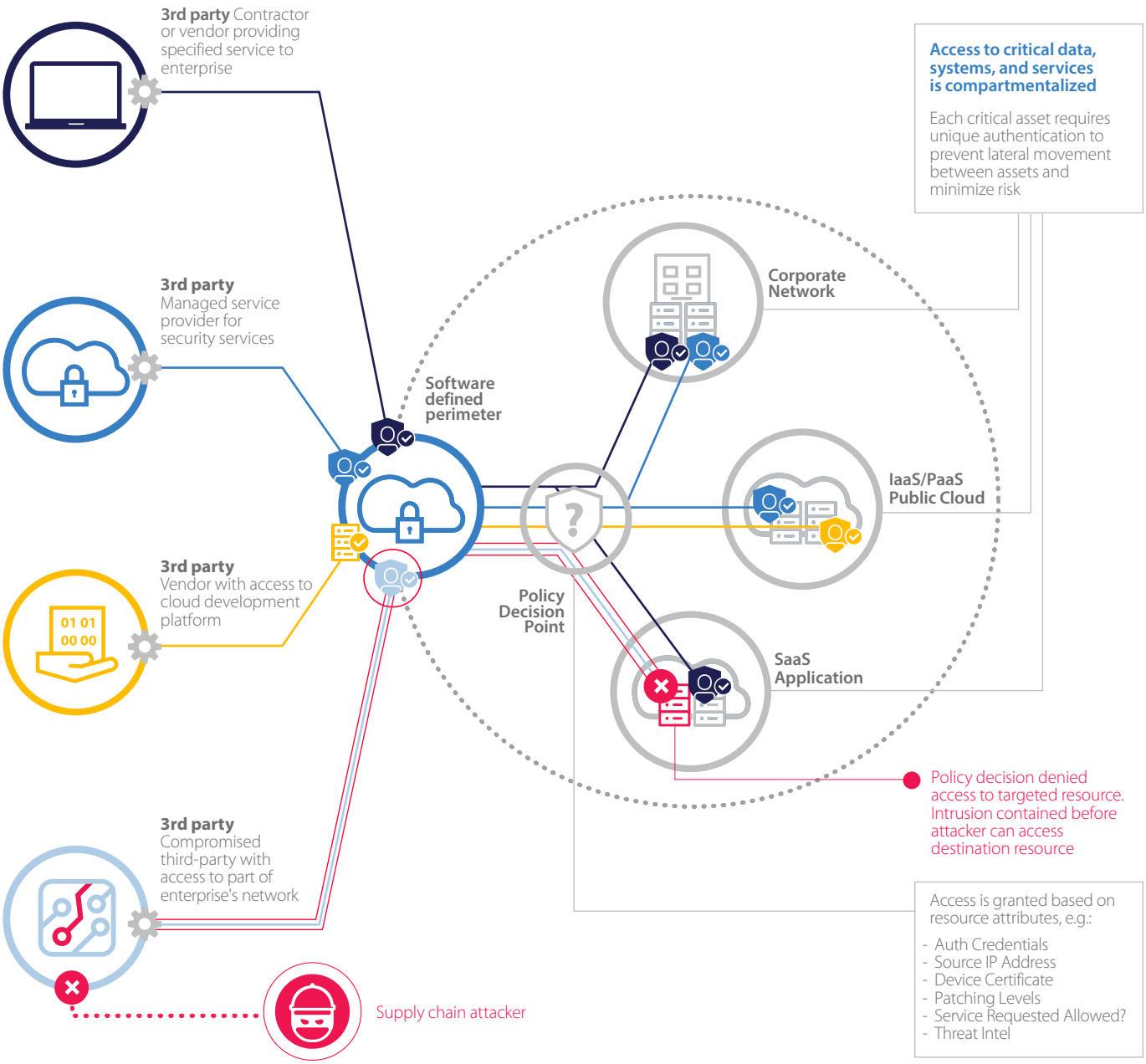
What a zero trust approach is and how it complements supply chain security

Establishing a C-SCRM program at the same time as a ZTA provides an organization with the best opportunity to effectively manage against attacks from third parties. For a small business, a ZTA is not just the adoption of new security techniques and procedures, it is also a mindset change. According to NIST, a ZTA "assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)" (Rose et al., 2020). In other words, a ZTA assumes that attackers will breach an enterprise's security perimeter. That is why it reverses the order of the old adage "trust but verify," making the new rule "verify, then trust." An assumed breach mindset expects that every system, application, or process accessing the network could be compromised. Therefore, extra protections should be implemented for higher-risk resources at defined policy enforcement points, which should ensure that every interaction with other systems or application processes is authenticated.

Critically, a ZTA does not replace the principles of the CSF, but rather complements them. A ZTA approach examines the entire data flow and data life cycle of critical technology services. Then it identifies all the interfaces and handoffs among different organizations, processes, technologies, and environments. This can help uncover any potential weak links in the security posture or avenues of attack from each layer of the system architecture, and not just at the perimeter firewall. A security manager can then select additional controls, as appropriate, to lock down key moments in the data life cycle.

A useful metaphor to help illustrate where C-SCRM ends, and where ZTA begins, is to think of a house. Conceptually, someone following a ZTA would begin by not just locking the front door, but also locking the door to every room or cabinet, and perhaps every drawer containing valuables. Whereas a C-SCRM program can help secure the component software and services delivered by a digital supply chain that are *outside* an organization's (in the metaphor, the house owner's) direct control, a zero trust approach to cybersecurity can help an organization protect the resources that are within its own control, particularly at any connection points with supplier software and services.

How zero trust security defends an enterprise network



This figure illustrates the ability of a zero trust approach to mitigate the impact of software supply chain attacks, even after an attacker has initially penetrated an enterprise's security perimeter. In the figure, various third parties are displayed, each of which have trusted access to an enterprise's resources. These include a vendor providing a specific service with access to a corporate network, a managed services provider performing security functions, a vendor who has access to a cloud-hosted development platform, and an additional third party who has been compromised by a supply chain attack. In this case, the attacker has compromised a third-party service provider, who has access to the enterprise's network. Although the security service provider has granted the attacker entrance to the security perimeter, the attacker is denied access to the targeted resource. This is all thanks to the enterprise's decision to implement a zero trust approach, which results in the attacker's denial based on certain resource attributes.

Putting NIST's past work into context

The CSF was originally intended to be a voluntary framework designed to help critical infrastructures better understand, manage, and reduce their cybersecurity risk. However, since its original publication it has expanded to become a toolkit helping organizations of every size better manage their cybersecurity risk. NIST even published a "Quick Start Guide" of the CSF for small businesses (National Institute of Standards and Technology [NIST], 2021). Critically, the CSF was always intended to be a "living" document, in order to keep pace with emerging technologies and threats. Moreover, the authors wanted to ensure the CSF provided a "common language to address and manage cyber risk in a cost-effective way based on business needs, without placing additional regulatory requirements on businesses" (NIST, 2014).

It's heartening to see NIST treating the CSF as a living document and updating it to respond to new threat environments. Instead of treating C-SCRM and ZTA as new frameworks, NIST sees them as complements of the NIST CSM: "The process of migrating to a ZTA is not a unique process and is similar to other cybersecurity upgrades, improvements, etc. Existing frameworks such as the NIST Risk Management Framework (RMF) and Cybersecurity Framework (CSF) can help an enterprise discuss, develop, and implement a ZTA." (NIST, 2021).

Nevertheless, the C-SCRM and the ZTA are less familiar cybersecurity programs for most small businesses. They still need a workable checklist, or a toolkit, to start thinking about how to apply the two frameworks.

A checklist for small businesses implementing a zero trust security architecture

Once business leaders understand a ZTA, the next step is providing a checklist that information security managers can put into practice. The following recommendations are actionable steps that enterprises of all sizes can take to improve the cybersecurity and risk management of their digital supply chains. These recommendations may not work for every small business, but it is important to understand them. As the NIST CSF states: There is not a "one-size-fits-all approach to managing cybersecurity risk" because "organizations will continue to have unique risks—different threats, different vulnerabilities, different risk tolerances—and how they implement the practices in the [framework] will vary."

- **Build an inventory and perform threat modeling to understand the pathways that attackers could use to gain access to your data and technology assets.** Security managers should begin by building a comprehensive inventory of data, systems, and applications; where these reside; and how they connect to, or depend on, other resources. Then they should prioritize these assets by criticality. Once a prioritized inventory has been captured, the data flows associated with critical systems and applications should be mapped (Open Web Application Security Project, n.d.). Security managers should also vet who has access to these assets (including any suppliers or third parties), and determine whether that access includes administrative privileges, or the ability to make major changes to a network or operating system. When the environment is clearly understood, threat modeling—or the process of imagining yourself as the attacker—should be performed to identify the likely paths an attacker could take to gain access to resources by traversing various layers of the environment. After this exercise is complete, controls can be placed at key locations and policy enforcement points.

- **De-emphasize the dependence on "perimeter" controls and assume network defenses have already been breached.** Historically, the perimeter was demarcated at the enterprise's firewall and typically protected everything running inside this strictly controlled and self-managed environment. Everything "inside the castle walls" was perceived to be safe and friendly. Today, however, companies have a growing reliance on complex hybrid architectures. Local infrastructures managed from inside traditional enterprise data centers now connect with multiple cloud and partner platforms and services, remote offices, and mobile workers. This complexity makes it increasingly difficult to effectively define where an enterprise's "perimeter" begins or ends. Firewalls are still critical, but it's dangerous to assume that assets inside or behind a firewall are safe by default. Organizations need to train their attention on protecting individual end points and data to prevent unnecessary access, even within the same network. It is vital to select and place policy enforcement points or gates to prevent unnecessary traffic between environments and individual end points. Penetration testing and red team[4] exercises are essential activities in testing security controls and mapping out any avenues for lateral movement.

- **Apply a least privilege access model.** Once critical assets and workloads are identified, access should be granted only on a "need-to-know" basis and should be limited to those people and systems with a legitimate business need. Even then, permissions should be limited to the absolute minimum set required to perform each business process and should enforce segregation of duties where appropriate to prevent malicious insiders from making harmful changes.

- **Build extra protection for the most important assets using micro-segmentation.** A least privilege model doesn't apply only to people, but also to system-to-system communications. Micro-segmentation isolates resources and workloads from one another and secures them individually, implementing security controls to prevent lateral movement, based on a zero trust approach (Palo Alto Networks, n.d.). This way, even if an authenticated (i.e., verified) system has been compromised, it can perform only a discrete set of activities and will not necessarily be able to cause more serious harm or further propagate an attack. ZTA assumes there are no "safe zones" where one can access every resource in a shared environment. Think of a ship that can seal its compartments to prevent flooding in the event of a breached hull. Each compartment of the ship represents an individual system, application, or data object. Each of these resources is sealed off from the others and can be accessed only via explicit permissions to perform the absolute minimum set of required tasks associated with that object or function.

Checklist

Questions for security managers:

- ☐ Do you have a comprehensive inventory of your data and technology assets?
- ☐ Have you identified the most critical systems, applications, and services?
- ☐ Have you mapped out their data flows, dependencies, and connections to other systems?
- ☐ Do you know who has access, particularly privileged access, to your critical systems?
- ☐ How would an attacker be able to gain access? Where are your defenses weakest?
- ☐ How much emphasis have you placed on data- or system-centric security controls?
- ☐ Is everything "open" behind your firewall? Have you compartmentalized your network and key service components to help you limit the impact and contain any potential security incident?
- ☐ How often do you stress-test your network security by running penetration tests or red team exercises, or by rehearsing cybersecurity incident response plans?
- ☐ Do you have insights into the network activity and security of all your remote employees, and the devices they use to access your network?
- ☐ What data do remote employees have access to, and what types of network privileges do they have?

- ☐ Do you have policies in place to authorize and track each access request to your systems, applications, and data? Is that current process automated?
- ☐ Is access currently limited to one part of the network and narrowly defined to meet only the needs of the request, or does the requestor gain access to a broader set of resources?
- ☐ Are your network architecture and business processes designed to support a least privilege model?
- ☐ Have you identified areas where segregation of duties is appropriate to prevent rogue actors from doing damage or covering their tracks?
- ☐ Have you configured your systems to allow only those services and connections necessary to perform the minimum required activities to deliver business functionality?
- ☐ Have you enforced authentication for system-to-system communication?
- ☐ Do you monitor your systems and applications for anomalous activity?
- ☐ Are there vendors or suppliers that you trust implicitly, simply because you have worked with them for years?
- ☐ How do your different software systems and cloud providers intersect?
- ☐ What policies, or governing principles, do you have in place to limit access from one activity to the other?
- ☐ Are those processes automated, and in the event of a cyberattack, will they help contain the damage by preventing further spread?

Thinking about the path forward

It is possible for small to medium-sized businesses to benefit, securely, from the use of third-party providers of software and other digital infrastructure solutions. These providers make it easier for businesses to lower costs, provide greater services, and scale faster into new markets. However, in light of software supply chain cyberattacks, businesses can dramatically improve their cyber-resilience by applying a robust C-SCRM program to secure the digital supply chain outside an organization's direct control, and by implementing a zero trust architecture to secure resources that are within its own control. The US government has taken the right steps in the wake of the recent software supply chain attacks by providing two complementary standards for enterprises to follow.

In order for these programs to work successfully, however, all businesses must expand their security focus from just the enterprise to the entire supply chain. Such a shift would recognize that businesses of every size are networks consisting of multiple participants that share responsibility for cybersecurity. When a small business asks one of its suppliers—which may be a much larger business—if it is following these NIST standards, the answer should be "of course." Software supply chains often extend beyond borders, which is why the US government promotes these standards to other countries and other international standards bodies. Finally, with software supply chain attacks that can impact thousands of victims at the same time, sharing information is even more critical. Implementing a C-SCRM and a ZTA is most effective when an enterprise has the most up-to-date threat information. Governments should encourage transparency and information-sharing regarding threats, vulnerabilities, and controls between government and private industry, among government agencies, and between governments of different nations.

References

Baksh, Mariam (2022, February 22). *NIST Refreshing Voluntary Cybersecurity Framework Amid Push for Mandates. Nextgov.* https://www.nextgov.com/cybersecurity/2022/02/nist-refreshing-voluntary-cybersecurity-framework-amid-push-mandates/362278/

Boyens, J., Paulsen, C., Bartol, K., Winkler, K., Gimbi, J. (2021, February). *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

Cimpanu, C. (2020, December 14). S*EC Filings: SolarWinds Says 18,000 Customers Were Impacted by Recent Hack. ZDNet.* https://www.zdnet.com/article/sec-filings-solarwinds-says-18000-customers-are-impacted-by-recent-hack/

Computer Security Resource Center (n.d.). *Glossary. National Institute of Standards and Technology.* https://csrc.nist.gov/glossary/term/red_team

Conger, K., Frenkel, S. (2021, March 6). *Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China. New York Times.* https://www.nytimes.com/2021/03/06/technology/microsoft-hack-china.html

Cybersecurity and Infrastructure Security Agency (2021, April). *Defending Against Software Supply Chain Attacks. Cybersecurity and Infrastructure Security Agency.* https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

Cybersecurity and Infrastructure Security Agency (2021, September). *Operationalizing the Vendor Supply Chain Risk Management Template for Small and Medium Sized Businesses.* https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force_smb-operationalizing-vendor-template_508.pdf

European Union Agency for Cybersecurity (2021, July 29). *Threat Landscape for Supply Chain Attacks.* https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Grance, T., Jansen, W. (2011, December). *Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology.* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

Harper, Chad. (January 8, 2021). *Small Business in the Digital Age: Recommendations for Recovery and Resilience. Visa Economic Empowerment Institute.* https://usa.visa.com/content/dam/VCOM/global/ms/documents/veei-small-business-in-the-digital-age.pdf

Higgins, K.J. (2021, August 5). *Why Supply Chain Attacks Are Destined to Escalate. Dark Reading.* https://www.darkreading.com/vulnerabilities---threats/why-supply-chain-attacks-are-destined-to-escalate/d/d-id/1341588

Kaseya (2021, July 7). *Kaseya Responds Swiftly to Sophisticated Cyberattack, Mitigating Global Disruption to Customers.* https://www.kaseya.com/press-release/kaseya-responds-swiftly-to-sophisticated-cyberattack-mitigating-global-disruption-to-customers/

Koziol, J. (2021, October 20). *The Most Common Cyberthreats Facing SMBs and How to Prevent Them. Forbes.* https://www.forbes.com/advisor/business/common-cyber-threat-prevention/

Lemos, R. (2021, July 6). *Cyberattack on Kaseya Nets More Than 1,000 Victims, $70M Ransom Demand. Dark Reading.* https://www.darkreading.com/attacks-breaches/cyberattack-on-kaseya-nets-more-than-1000-victims-$70m-ransom-demand/d/d-id/1341476

Lemos, R. (2021, July 7). *Attacks on Kaseya Servers Led to Ransomware in Less Than 2 Hours. Dark Reading.* https://www.darkreading.com/vulnerabilities---threats/attacks-on-kaseya-servers-led-to-ransomware-in-less-than-2-hours/d/d-id/1341496

Marsh McLennan (2021). *3 Best Practices to Reduce Supply Chain Cyber Exposure.* https://www.marsh.com/us/services/risk-consulting/insights/best-practices-to-reduce-supply-chain-cyber-exposure.html

Marsh McLennan (accessed 2021, November). *Defining and Uncovering Cyber Risks in Your Digital Supply Chain.* https://www.marsh.com/us/services/cyber-risk/insights/defining-uncovering-cyber-risks-digital-supply-chain.html

Marsh McLennan, Microsoft (2019, September). *2019 Global Cyber Risk Perception Survey.* https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

Muncaster, P. (n.d.). *Small Business Cyber Security: Protecting Against Supply Chain Attacks and Supplier Risk. Verizon.* https://www.verizon.com/business/resources/articles/s/protecting-against-supply-chain-attacks-and-supplier-risk/

National Institute of Standards and Technology (NIST), Commerce. (2022, February 22). *Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management. Federal Register.* https://www.federalregister.gov/documents/2022/02/22/2022-03642/evaluating-and-improving-nist-cybersecurity-resources-the-cybersecurity-framework-and-cybersecurity

National Institute of Standards and Technology (NIST). (2014, February 12). *NIST Releases Cybersecurity Framework Version 1.0.* https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10

National Institute of Standards and Technology (NIST). (2021, August). *NIST Special Publication 1271. NIST.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf

Open Web Application Security Project (accessed 2021, November). *Attack Surface Analysis Cheat Sheet.* https://cheatsheetseries.owasp.org/cheatsheets/Attack_Surface_Analysis_Cheat_Sheet.html

Palo Alto Networks (accessed 2021, November). *What Is Microsegmentation?* https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation

Pipikaite, A. (2022, January). *Global Cybersecurity Outlook 2022 Insight Report. World Economic Forum.* https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

PwC (accessed 2022, February). *2022 Global Digital Trust Insights Survey.* https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights.html

Ramel, D. (2021, December 16). *Survey Shows Zero Trust Confusion. Virtualization & Cloud Review.* https://virtualizationreview.com/articles/2021/12/16/zero-trust-survey.aspx

Rose, S., Mitchell, S., Connelly, S. (2020, August). *Zero Trust Architecture. National Institute of Standards and Technology.* https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=930420

Shackleford, D. (2021, September). *How to Create a Comprehensive Zero Trust Strategy. Sans.* https://www.sans.org/white-papers/39790/

United States National Institute of Standards and Technology (2021, April). *Defending Against Software Supply Chain Attacks. Cybersecurity and Infrastructure Security Agency.* https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf

United States Department of Commerce, Office of Public Affairs (2021, August 25.). *US Secretary of Commerce Gina M. Raimondo Joins White House Cybersecurity Summit.* https://www.commerce.gov/news/press-releases/2021/08/us-secretary-commerce-gina-m-raimondo-joins-white-house-cybersecurity

United States Department of Commerce, United States Department of Homeland Security (2022, February 24). *Assessment of the Critical Supply Chains Supporting the US Information and Communications Technology Industry.* https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf

The White House (May 12, 2021). *Executive Order on Improving the Nation's Cybersecurity.* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Williams, J. (2020, December 15). *What You Need to Know About the SolarWinds Supply-Chain Attack. Sans.* https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/

Notes

[1] Immediately after the 2021 REvil attack, Kaseya announced that 50 of its customers were affected. Those affected customers then infected somewhere between 800 and 1,500 additional victims with the ransomware (Kaseya, 2021). In other words, Kaseya and its MSP partners became distribution channels for the malware that struck mostly small and medium-sized businesses. It took less than two hours from the moment the first Kaseya servers were affected by the attack for the ransomware to reach the downstream victims (Lemos, 2021).

[2] The NIST CSF consists of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to reduce cybersecurity risks. It is used widely by private- and public-sector organizations in and outside the United States and has been translated into multiple languages, signifying its success as a common resource (NIST, 2022).

[3] The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency published a vendor supply chain risk management template for small and medium-sized businesses that can serve as an expanded checklist.

[4] Also known as cyber red team. NIST definition: A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The red team's objective is to improve enterprise cybersecurity by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the blue team) in an operational environment.

About Visa Inc.

Visa Inc. (NYSE: V) is the world's leader in digital payments. Our mission is to connect the world through the most innovative, reliable, and secure payment network—enabling individuals, businesses, and economies to thrive. Our advanced global processing network, VisaNet, provides secure and reliable payments around the world, and is capable of handling more than 65,000 transaction messages a second. The company's relentless focus on innovation is a catalyst for the rapid growth of digital commerce on any device for everyone, everywhere. As the world moves from analog to digital, Visa is applying our brand, products, people, network, and scale to reshape the future of commerce.

For more information, visit About Visa, visa.com/blog and @VisaNews.

Visa Economic Empowerment Institute