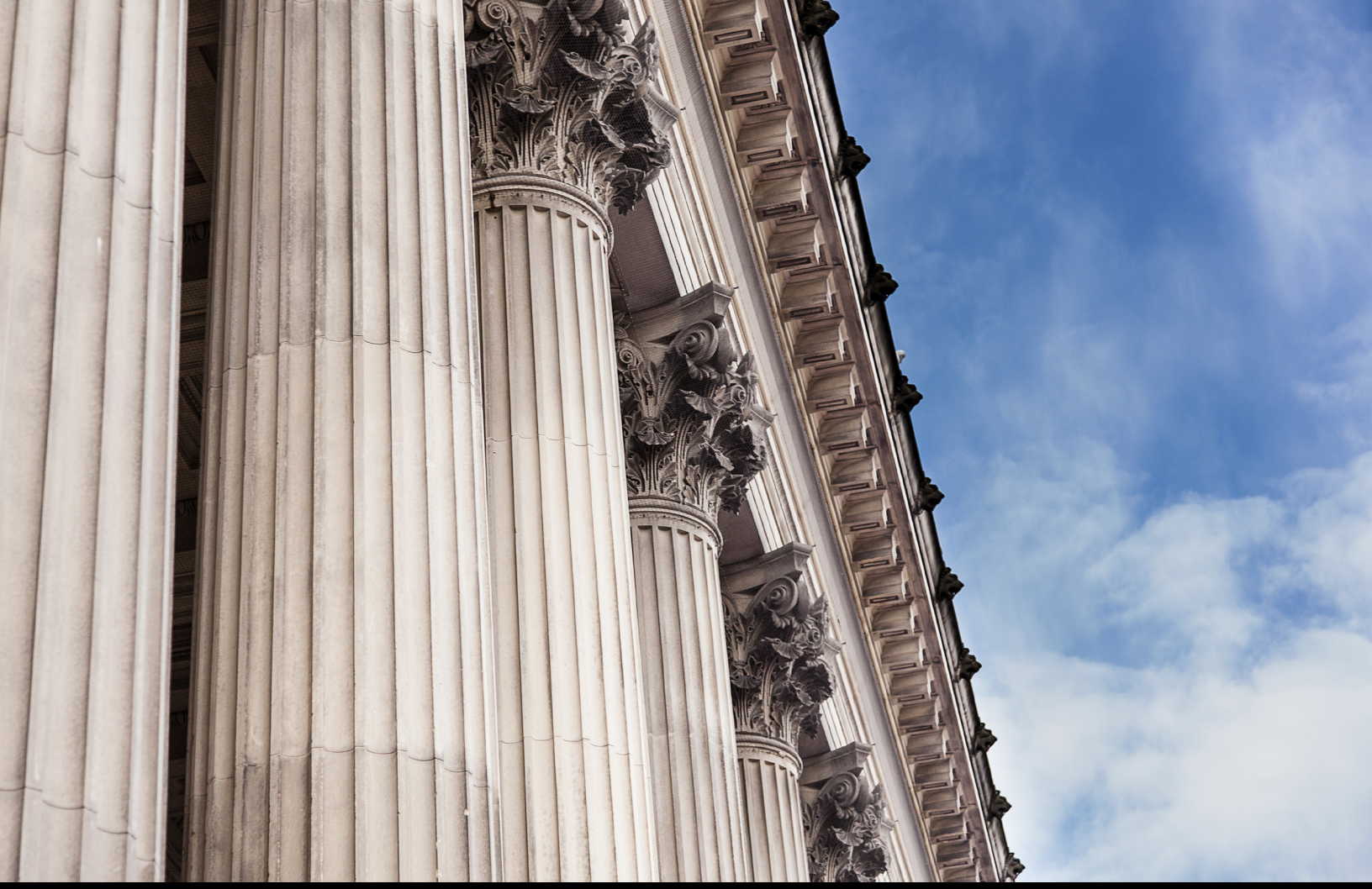


White paper

Best Practices for a Cyber Fortified Supply Chain.

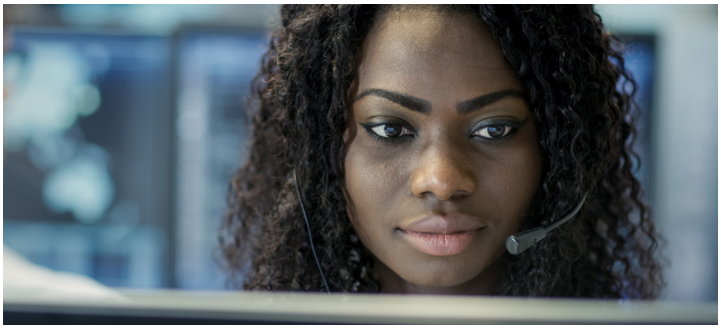
verizon

verizonenterprise.com/federal

Executive summary.

Regardless of the industry, the supply chain is one of the most overlooked and yet most critical components of any Cyber Security fortification plan. Although we often think of cyber security related to a network edge attack or an internal personnel breach; devices and software coming in the backdoor may possess the same level of disruptive capability to your network or data security. As our adversaries have become increasingly more sophisticated finding vulnerabilities, so has their approach to creating vulnerabilities. This white paper discusses cyber risks through a supply chain and the need for a private-public partnership to truly secure our nation from supply chain vulnerabilities.

In 2012 the White House published the "National Strategy for Global Supply Chain Security". This document was designed to be an Executive Overview and a general statement about the need for a unified approach to the global supply chain risks. From a security perspective it fell short of outlining the tactical methods needed to combat a rising cyber problem facing our country. In fact, most efforts by the government to address supply chain security have focused on the Customs and Border Protection container shipping programs outlining what individual companies can do to verify their own supply chain. Programs such as Customs-Trade Partnership against Terrorism (C-TPAT) and "10+2" Carrier requirements support the government's efforts in monitoring and securing the physical shipping process. What remains open is a cohesive supply chain approach addressing unintended or intended cyber outcomes.



Industry experience.

Who better to ask about a cyber secure supply chain than an industry leader protecting a network with hundreds of thousands of network route miles reaching more than 2,700 cities in more than 150 countries; or a nationwide 4G LTE wireless network covering over 2.4 million square miles. The fact is consumers, businesses, large enterprises, and the federal government, all rely on Verizon to provided dependable and resilient services for their data and voice communications.

Every day, Verizon's global network is tested for resiliency against adversaries. As such, Verizon has developed best practices for properly vetting the equipment we install on our own network, including suppliers and their 3rd party component manufacturers.

First and foremost, equipment going into the Verizon network requires a strong relationship with our suppliers/technology partners. Our technology partners have a long and collaborative history backed with a track record of strong security practices. Just like the recommendations below, our technology partner supply chains have been well vetted, and periodic reviews of manufacturing best practices help us understand and vet changes within our partners' supply chain.

In order to adequately address the supply chain cyber issue, a variety of techniques, processes, and technologies are used to detect vulnerabilities and anomalies. The following is a list of best practices that Verizon recommends any government agency consider when evaluating their total supply chain security posture.

Overview.

Supply Chain Cyber Security can be broken down into manufacturing, shipping and receiving, installation, network and monitoring. Each area of focus should be accompanied by a corresponding risk score, which can be weighted with customer-specific, environmental considerations, which will go into the overall decision of if/how a partner should be integrated into your ecosystem.

Manufacturing.

In Verizon's view, a Cyber Fortified Supply Chain starts with the manufacturing ecosystem and influences that can affect the outcome of the product. Although we do not address all of the cyber security factors, below are items and learnings we include within our supply chain processes and help us determine an organization's risk score.

Financial review.

Each agency should perform a yearly financial evaluation of their suppliers. Validating a supplier's stability and dependability should be part of protecting your financial investments, your business, and your security. A risk assessment that includes capital resources, experience, personnel, and time in the market all contribute to their longevity and their potential susceptibility to supply chain vulnerabilities. Instability in these areas can lead to cost cutting efforts including processes, resource allocations, and even the manufacturer's ecosystem of suppliers.

Foreign ownership/citizenship influence.

Due to the global nature of large manufacturers, it is often difficult to verify that a supplier has provided adequate protections from foreign influences within their manufacturing process and ecosystem. A risk assessment should include hiring and background check practices, including screens for financial/foreign connection influences.

In addition, corporate executives should also be evaluated and scored. A small recommendation by a Board member changing the location of device manufacturing or 3rd party supplier could directly impact the security of the product.

Validate supplier's product security testing.

Product testing is an essential part of any vendor selection process and a major component of a cyber risk score. Testing methodology, geographical location of the test, and citizenship of those performing the testing should all be considered in scoring and a risk mitigation strategy. There are many test stages within any manufacturing process where adversaries could affect the security of the product; including printed circuit board (firmware), software installation, and final system tests. Do your homework, ask the questions, and make sure that your supplier agrees to periodic reviews and notifications when manufacturing locations change.

Additionally you may consider adding a controlled agency specific "post-manufacturing" test within the suppliers quality assurance process and/or at incoming inspection which will help verify suppliers aren't creating a "back-door" into your network.

Secured product validation.

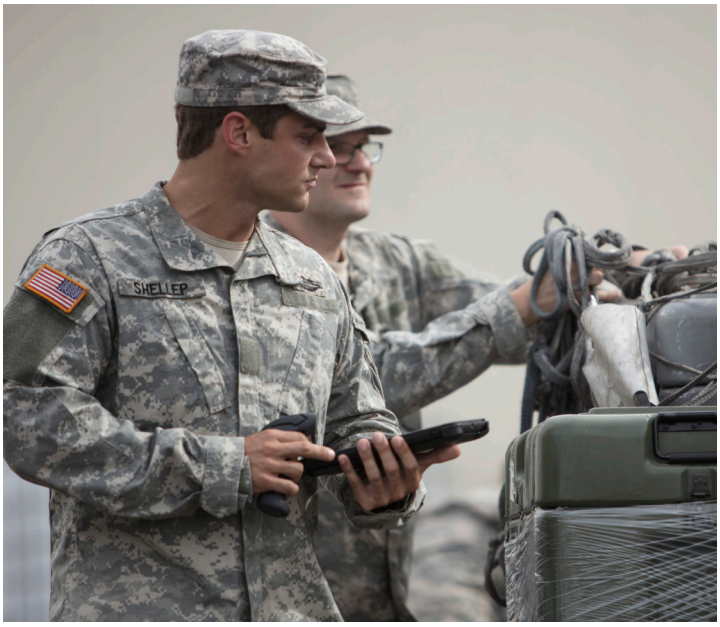
Risk scores can be greatly improved with the implementation of internal device certification technologies. There are a wide variety of technology resources available to help the government test the devices received from manufactures. For example, some manufacturers use pre-boot loaders that are digitally signed; this offers verification to the integrity of the device components. Some manufactures even have electronic "signatures" tied to each individual device, which can verify if the core hardware baseline has been modified between manufacturing and receiving.

Shipping & receiving.

It's not about an entire shipment; a cyber adversary may only need to target one piece of equipment to create the intended "back door" to attack the network or possibly national security. The ability to receive a shipment with confidence requires a full security review from point of manufacturing, warehouse and staging, transport, to the receiving agency. Some of the same risk analyses discussed needs to be applied, such as background checks, but the overall focus becomes confirming the physical product has not been opened and manipulated.

Staging and transport.

Part of maintaining security during staging or transit within a supplier's network is to simply "hide in plain sight". Many supplier agreements require that the equipment being procured and the location of its shipping are tracked using obfuscation methods, which make it difficult to know "to whom" equipment is being shipped. The most common obfuscation method use automated barcoding labels on shipping containers concealing customer identity and destinations from warehouse employees.



Operation Safe Commerce.

The Department of Homeland Security publishes and maintains best practices for the shipping function of supply chain security known as "Operation Safe Commerce". In their recommendations they advise that when taking possession of equipment from overseas vendors that agencies review the origination of cargo, packaging, and container and verify that the documentation of cargo, packaging, and sealing verification is in order by port authorities. Also, in their recommendation is to review the Port of origin, movement from container to deconsolidation point, and even storage location before transport occurs.

"10+2".

The Security Filing, commonly known as the "10+2" initiative, is a Customs and Border Protection (CBP) rule that requires importers and vessel operating carriers to provide additional advance trade data to CBP pursuant to Section 203 of the SAFE Port Act of 2006 and section 343(a) of the Trade Act of 2002, as amended by the Maritime Transportation Security Act of 2002, for non-bulk cargo shipments arriving into the United States by vessel.*

* Sourced from US CBP–Importer Security Filing and Additional Carrier Requirements, March 20, 2010.

Lab & testing.

Depending on the potential impact of a data breach, it is recommended that a supply chain "lab" be established (or outsourced) to receive and test equipment that will eventually touch your network. This lab should be equipped with the tools and personnel necessary to adequately verify that the equipment being received meets the original manufacturing digital and electronic signatures that have been recorded by the manufacturer. The personnel should be well trained on the types of equipment being purchased and be certified through the manufacturer on the best practices to perform appropriate supply chain vetting and verification.

If it is impossible to test all equipment being shipped, it is recommended that a random sample from vendors (using the supply chain obfuscation previously mentioned) be used. Much like airport screening, this can serve both as a deterrent and a detection mechanism.

In the most severe conditions, it is recommended that agencies place a digitally-encrypted and signed implant in their devices, which can monitor changes to the equipment's shipping baseline during the installation process and before it reaches full operational status.

Installation.

Installation is often a very intimate part of bringing equipment online. Whether you have employees or contractors perform the work, the possibility of human error or malicious intent is always possible. In addition to fully vetting your installation personnel, including a financial background check to gauge vulnerabilities to foreign influence, it is recommended that your security operations center have full access to test and verify your implant code and to look for changes in the operational status of the installed equipment.

Data evaluation and network segmentation.

With the modernization of network technologies most networking manufacturers are offering some form of Software-Defined Networking (SDN) capabilities. Defining network segments within your network and using properly designed SDN best-practices not only helps contain lateral movement of cyber villains, but it also helps to detect supply chain malicious intent. As an example equipment that is "chatting" outside of its security boundary is a clear red-flag that something is amiss and should immediately be investigated.

Network monitoring & penetration testing.

Once equipment has been verified by the manufacturer, tested by receiving, shipped and installed onsite, penetration tested, and has reached full operational status, it is time to pass the baton to the Security Operations Center (SOC) for integration into their regular monitoring behavior. Within 90 days, a post-installation penetration testing and traffic analysis should be done by a forensic team. If all lights are green, this new equipment can be passed to the regular penetration testing and SOC monitoring team to put into its random testing schedule.

Verizon solutions.

Leveraging industry experience and expertise is echoed throughout government agencies for technology solutions but shouldn't that also apply to the processes which provided physical products supporting those implementation efforts. We at Verizon have solutions to help you cyber fortify your supply chain.

Verizon offers testing of equipment through our ICSA Labs organization. ICSA Labs began as National Computer Security Association (NCSA). Its mission was to increase awareness of the need for computer security and to provide education about various security products and technologies.

In its early days, NCSA focused almost solely on the certification of anti-virus software. Using the Consortia model, NCSA worked together with anti-virus software vendors to develop one of the first anti-virus software certification schemes. Over the past decade, the organization added certification programs for other security-related products, and changed its name to ICSA.

ICSA Labs have been providing credible, independent, third-party product assurance for end-users and enterprises since 1989. ICSA Labs is currently an independent division of Verizon providing resources for research, intelligence, certification and testing of products, including anti-virus, firewall, IPsec VPN, cryptography, SSL VPN, network IPS, anti-spyware and PC firewall products.

Consider a global telecommunications partner whose reputation and business is built on generations of experience; consider Verizon as the partner to help you build a supply chain security program to meet your individual needs.