U.S. Resilience Project

CASE STUDY

Verizon
Based on interviews with Henry Shiembob, Executive Director, Cyber Security and Fraud Operations

James McConnell, Director of Security

Marcus Sachs, Vice President, National Security Policy

September, January 2012

Verizon: Building Security into the Network

Verizon is more than just a phone company. Operating in more than 150 countries, it is a network owner and operator, systems integrator, and global purchaser. Its supply chain runs the gamut from wireless testing equipment to mobile devices to the purchase of millions of miles of fiber-optic cable. One of Verizon's many supply chain security priorities is to assure the security of the network and the devices connected to it, while also maintaining the integrity of the services required to maintain the network and the revenue-generating services riding on it.

The Business Case for Supply Chain Security and Resilience

Supply chain resilience is one of Verizon's many business objectives. Cutting back on supplier assessments or failing to perform independent verification and validation would certainly cut costs; however, Verizon understands that cutting corners also cuts reliability, which is the cornerstone of its competitiveness. Verizon maintains a private and public infrastructure, and customers have choices about which communications infrastructure to use. Verizon's network must be resilient in order to retain the company's customer base — failure of the network is not an option.

Verizon prioritizes network resilience, rather than price alone, in managing its supply chain. For example, given a choice between paying $1,000 or $10,000 for a piece of network equipment, Verizon will not always choose the cheaper option. The $1,000 piece of equipment might use stolen intellectual property — essentially a copy of a $10,000 piece of equipment patented in the United States — or its reliability may be low.

Supply chain resilience and security are linked. On 9/11, for example, Verizon's communications infrastructure kept operating under extreme conditions. When one of the hijacked aircraft crashed into the Pentagon, it landed on top of one of the two communications points of presence (PoPs). The switches, which were located only a few floors below the point of impact, kept operating despite the fires, leaking jet fuel, and water. This kind of resilience cannot be obtained without focused attention to the quality, integrity, and security of the components in the supply chain.

Communications networks are designed to withstand or recover from a spectrum of disasters — a mindset that goes back to the Cold War. With a demand for high uptime, the communications network keeps working during most types of emergencies — including floods, fires, earthquakes, and hurricanes. It works because of Verizon's workforce and the company's ongoing focus on its supply chains. Verizon's view of supply chain goes beyond procurement, maintenance, and disposal — it views supply chain as an important part of the reliability and performance of the network and supported services.

Supply Chain Security Good Practices

For Verizon, cybersecurity is not just a technology problem. Many non-cyber business practices need to be implemented to assure cybersecurity, including knowing who the company is doing business with, knowing the ownership and location of contractors and subcontractors, and ensuring validation and compliance with contract terms and conditions. These supply chain processes are just as important as testing the quality and security of devices when they arrive from manufacturers.

Verizon implements numerous security processes that help manage cyber risks in the supply chain, including the following:

Vendor Controls: Security processes are embedded into supply chain processes, from the selection of appropriate vendors and locations, to the completion and delivery of products or services, to the turndown of the relationship. Prior to any contractual agreement, prospective Verizon suppliers are scrutinized on criteria such as ownership and location; links to foreign countries; and red flag violations, including export controls. Verizon uses its own intelligence and public information to review suppliers.

Internal Clearance Processes: Verizon conducts an additional internal clearance process on prospective vendors to make sure that the business relationship is in compliance with all legal and regulatory imperatives, as well as all security priorities. This process includes background checks, export control statements, requirements for off-shoring or outsourcing notification and approval, disclosure of baseline security for handling data, and other clearance requirements, including assessments of physical and cyber controls.

Risk Prioritization: Verizon prioritizes these assessments both by ranking the criticality of components and the assurance levels desired for suppliers that have access to Verizon data, products, or systems. Many of the major components are purchased from key vendors that are within a trusted category and face restrictions on where products can be developed and manufactured, as well as where services may be performed. For certain relationships, Verizon contractors are required to list their subcontractors.

Assessments of High-Priority Vendors: Verizon also performs on-site reviews of high-priority vendors to ensure that they are complying with requirements and meeting appropriate security practices. Verizon employs on-site inspections and audits for these reviews, because there is concern that questionnaires may create a false sense of security. Vendors often give the answer that they think their customers want to hear or describe what the vendor believes is in place. Experience has shown that questionnaire answers rarely match up to the findings of on-site inspections.

Anti-Counterfeiting Efforts: There is a growing problem with counterfeit goods, which introduce potential risks when they connect to the Verizon network. Federal agencies estimate that 10 percent to 11 percent of the global electronics supply chain is counterfeit — everything from iPads and iPods to routers, switches, and heavy machinery. A circuit card that would normally cost $1,000 might be discounted by a licensed re-seller to $700-800 wholesale. But, when that product is offered as brand new for $99 on an auction site, there is no way it is genuine.

There is no way to stop a customer from going online and buying a fake or modified phone. However, Verizon's own procurement processes — strong relationships with suppliers and other technical controls — lower the risk of counterfeit products being used in its environment or entering its supply chain. To further understand the vulnerabilities in its supply chain, Verizon maintains a rigorous independent verification and validation program.

Security Controls: Verizon also employs other detective controls, including supply chain fraud analytics, supply chain link analysis, supply chain mapping, and supply chain security awareness.