Putting Trust in the Supply Chain

3 November 2019

Global supply chains play a crucial role in giving customers in any industry what they want: more selection at better quality for less money. By connecting specialized component makers around the world, global supply chains provide focused expertise that improves quality at a scale that delivers lower costs.

Information technology manufacturers, more than most industries, have built global supply chains, and customers have reaped the benefit of more powerful technology at lower prices. Yet to run a truly world class supply network, technology companies must also ensure the security of each link in that chain.



To assure customers can depend on every part of Lenovo's supply chain, Lenovo created the Trusted Supplier Program. The program's goal is simple: to ensure that every supplier meets high security standards set by Lenovo's customers.

The Trusted Supplier Program has been recognized as an industry leader by experts in supply chain security. Gartner recognized Lenovo as a Top 35 Supply Chain in the world since 2013, and International Data Corporation (IDC) also praised Lenovo's auditable supply chain as "best practices" in the industry. And Chain Security, LLC, a leading supply chain security firms in the United States, spent almost three years examining Lenovo's security processes, corporate governance and supplier programs and determined that Lenovo is "ahead of the industry" in its commitment to these areas. (You can read more about Chain Security's report here.)

So how does Lenovo's Trusted Supplier Program work? The program provides customers security assurance by:

- Identifying and addressing security risks for Intelligent Components
- Ensuring that suppliers have a security program designed to prevent security issues, incident response capability, will allow security assessments of their products, and will offer security fixes subject to a service level agreement
- Providing auditable security assurance to customers

To accomplish this, the Trusted Supplier Program starts with a detailed security questionnaire. With more than 200 questions, this step asks suppliers about nearly every aspect of their business from access control to human resources to security policies and practices for their own IT systems, software testing, and shipping practices, to name a few. In addition, each supplier must show they have a formal process and established team to address new security incidents that arise.

Lenovo also evaluates each supplier's development and manufacturing process to help them identify and mitigate security risks. Through the Trusted Supplier Program, suppliers contractually own the security of what they supply to Lenovo. Once qualified, suppliers are subject to re-evaluation on a regular basis, requiring an ongoing effort to keep up to date with industry best practices and processes around security.



Lenovo also evaluates each supplier's development and manufacturing process to help them identify and mitigate security risks.

The program covers "intelligent components," which are broadly defined as any:

- Software or firmware executable on any microprocessor
- Semiconductor devices that has data processing ability
- Component or device that has internal memory
- Component or device that performs an input/output function

What types of components meet these definitions? Some include: CPUs, disk drives, fingerprint sensors, BIOS and firmware, memory, keyboards, network cards and switches, integrated circuits, solid state disks, optical disk drives, and software.

To date, Lenovo has approved hundreds of suppliers and is working with potential new suppliers to ensure they meet the program's standards.