U.S. Resilience Project

CASE STUDY

Hewlett-Packard
Based on interviews with
Robert Moore, Vice President, Global Security Services; and
Fred Smith, Director, Supply Chain Global Security Group Programs & Supply Chain

HP: Mature Business Processes for End-to-End Supply Chain Security

Supply Chain by the Numbers

HP has one of the industry's most extensive supply chains: more than 1000 production suppliers (responsible for product materials, components, manufacturing and distribution services) in more than 1200 locations; 450 supply chain nodes, and a billion customers worldwide. HP ships more than 60 million computers, printers and servers every year — approximately 3.5 products every second.

HP views supply chain as a competitive differentiator. The company takes an end-to-end view of supply chain management from manufacturing to distribution — and everyone in the company is expected to be actively engaged in managing supply chain risk in some capacity.

Continuous Crisis Management, Continuity and Contingency Planning

Given its global footprint, HP maintains significant risk and crisis management capabilities. In 2011 alone, the company faced drought, floods, tornados, earthquakes, hurricanes, protest demonstrations, — and that was just in the United States. On the international front, a quick survey of the headlines included crises ranging from civil unrest in the Middle East, a devastating

earthquake in New Zealand, a series of disasters in Japan, a state of emergency in Bahrain, financial crisis in Greece, attacks in India and Norway, followed by typhoons in the Philippines and flooding in Thailand. According to the chief security officer: "No global company can take 'time off' when it comes to crisis management and business continuity planning."[1]

HP takes an enterprise-wide, all hazards approach to risk management because it is impossible to anticipate every crisis — and that is particularly true for supply chain disruptions. In an era of volatility, HP sees no substitute for effective planning. When the 9.0 magnitude earthquake struck the northeast coast of Japan on March 11, 2011, HP's team was activated within an hour. A war room was set up from which every supplier in Japan, including sub-suppliers, was contacted; alterative sources for constrained parts were identified; and daily updates and triage were managed. This kind of competency comes from preparation and communications.

Additional impetus for supply chain management came from the 2011 floods in Thailand, which created a worldwide shortage of hard drive disks and continued to affect HP's computer and server sales in the first quarter of 2012.

Supply Chain Risk Management

Far from minimizing investment in supply chain risk management, HP spends roughly $60 billion annually, or nearly half of its total sales, in support of its supply chain. Every year, the company conducts an annual supply chain mapping process to identify the most critical first- and third-party exposures. It regularly exercises supply chain continuity plans and emergency response capabilities in table-top drills. It also convenes an annual Suppliers Summit, bringing together more than 500 representatives from 150 suppliers, to share vision and priorities.

HP encourages its supplier base to adopt supply chain practices as well as technology solutions — and early resistance has turned into a standard part of doing business for most suppliers. Security programs tend to differ based on product, country and regional risks; HP suppliers have adopted much more stringent security measures in higher risk areas.

HP conducts about 100 audits of its supply chain partners every year — with follow-up action to ensure that corrective measures are implemented. Sites are selected for audit based on product value, volume and risk.

Mature Business Processes Support Supply Chain Risk Management

Supply chain security begins with a set of rigorous business processes and controls. More rigorous controls evolved in lock step with globalization. Twenty years ago, supply chain executives had more hands-on control when manufacturing and warehousing was done in-house. The globalization of manufacturing and distribution networks necessitated more organized business processes to combat corruption, quality issues and theft. There are many processes in place to create confidence in the materials being sourced, the quality of the manufacturing process, security of the products in shipment, and end-of-life disposal.

1 *Priorities for America's Preparedness: Best Practices from the Private Sector*. U.S. Resilience Project. http://www.usresilienceproject.org/reports.html.

In recent years, some new issues have emerged that have increased the scrutiny of supply chain controls, including cybersecurity, hi-tech counterfeiting, and social and environmental responsibility in the supply chain.

Cybersecurity: The visibility of cybersecurity issues and the scale and scope of the response is increasing — and HP customers want to know that HP is managing the risk. There are two aspects to cybersecurity. On the supply chain side, the maturity of existing business processes and controls can go a long way toward securing the cyber supply chain. HP's initiatives to secure the manufacturing process against firmware or malware, regular testing, and its anti-cargo theft and anti-counterfeiting programs reduce the risk of malicious insertion of compromised or counterfeit components through its supply chain.

Although supply chain security and resilience processes are mature, the standards to secure cyberspace are still in development. HP is working with other industry members in co-developing a set of secure practices as part of the Open Group Trusted Technology Forum.

Cargo Security: HP shipping requirements include the seven step container inspection process for all shipments to the United States. All seal variances are reported and investigated. There is a global reporting process for compromised freight.

Overall, industry experts suggest that $40 billion a year is lost to cargo theft worldwide, and high tech electronics are one of the most popular targets. HP uses various GPS satellite-type technologies to track products in transit, particularly by truck or rail. Covert GPS units — monitored by third party security companies — send out "pings" on a regular basis that allow law enforcement officials to track and recover stolen goods.

For ocean containers, HP typically uses physical security methods, such as high-security or bar-lock seals. High value shipments that are vulnerable to theft are accompanied by a variety of security protective measures, from security escorts to covert tracking of the tractor, trailer and the product itself.

Counterfeiting: Counterfeiting is a significant concern for HP in an industry in which it is estimated that as many as 10 percent of products are counterfeit. The International Anticounterfeiting Coalition estimates that brand holders lose approximately $600 billion of revenue annually due to counterfeiting.[2]

HP is leveraging technology solutions, particularly in the printing and imaging areas, to reduce losses from counterfeiting, and achieve a loss ratio that is well below the industry average. HP links printing innovation with QR codes that users of mobile devices can use to scan the bar codes to check whether the product is genuine.

2 Richetto, David. "Advanced Security Prevents Counterfeit Products." Electronics Design, Strategy, News. November 3, 2011. http://www.edn.com/article/519756-Advanced_security_prevents_counterfeit_products.php.

A relatively simple approach is to have a particular set of numbers, bars or other kind of code printed in several places on the packages. A more technical approach is to duplicate the overt code in infrared or ultraviolet ink — which is invisible unless viewed under IR or UV lamps. Comparisons of the overt and covert codes determines whether the product is authentic.

With variable date printing, it is now possible to give each item, case and packet its own unique code. Variable printing makes it possible to compute a set of non-linear unique codes ahead of time, which makes it difficult for counterfeiters to identify a sequence of numbers.

For the future, a new technology will be smart packaging, in which the package itself is imprinted with electro-conducive ink. Such inks can be charged in different ways and contain unique information that can only be decoded when passed through a reader. This will help drive security at the digital front end.[3]

Supply Chain Transparency for Social and Environmental Responsibility

HP has an aggressive program to monitor the social and environmental conditions in its supply chain. It was the first electronics company to publish a list of its suppliers, representing more than 95 percent of HP's procurement expenditures for materials, manufacturing and assembly of HP products all over the world. The list includes contract manufacturers, electronic manufacturing service providers, and original design manufacturers, as well as commodity suppliers. HP has set key performance indicators for suppliers and evaluates their performance through self-assessments and on-the-ground audits. This level of transparency gives HP the capability to assess issues in its supply chain, such as excluding purchases of conflict minerals.

Integrating Supply Chain Risk Management

With complex supply chains, one group cannot manage all risks. At HP, efforts are underway to strengthen communications and cooperation to manage end-to-end supply chain risks. Currently, the supply chain security (including anti-counterfeiting), cybersecurity, and business continuity functions are all in the same organization and work closely together. These units, in turn, work closely with the logistics function and business units. Supply chain security and logistics functions meet at least weekly to review joint initiatives and operational concerns.

3 Firth, Simon. "Fighting Fakes." March 2006. http://www.hpl.hp.com/news/2006/jan-mar/fake.html.