Eliminate Hidden Risks in the IT Supply Chain

MARKET TRENDS REPORT

Executive Summary

Early in 2019, IT experts from government and industry convened the Homeland Security Department's newly formed Information and Communications Technology Supply Chain Risk Management Task Force. The public-private partnership began its work by enumerating and categorizing threats to IT supply chains, including the subcategory of threats classified as "natural events" or "acts of God." Having listed hurricanes, tornadoes, tsunamis, wildfires and other potentially disruptive natural events, the group was ready to move on when someone from the back of the room piped up: "What about a pandemic?"

The room fell silent. "Nobody had any idea that a pandemic could really impact the supply chain," recalled Tommy Gardner, Chief Technology Officer for HP Federal and a co-chair of the task force's Threat Working Group. "They were thinking about Ebola, something that is localized and quickly fades," but after a little more thought, everyone agreed and I said, 'Yeah, that's a possibility. Let's throw it in there.'"

A year later, the coronavirus pandemic is 2020's biggest disrupter of IT supply chains.

The anecdote illustrates the challenge, even among security and logistics professionals, of identifying and mitigating threats to critical IT supply chains, sprawling networks that crisscross the globe to generate greater efficiencies, streamlined production, cost savings, innovation and faster delivery of products. Yet they are vulnerable to constantly evolving threat vectors, from hurricanes and pandemics to security breaches perpetrated by nation-states and criminal enterprises.

IT supply chains produce value and they are inherently difficult to secure, making every IT procurement by a federal agency a de facto security decision.

To learn more about how agencies can reduce risk associated with inadequate supply chain security, GovLoop teamed with HP, a global supplier of IT devices and a leader in IT security. This report will discuss how agencies can mitigate threats to supply chain security.

IT Supply Chain Security, By the Numbers

80%

The percentage of all security breaches that originate in the supply chain.

350,000

The number of new malicious programs registered daily.

Two-thirds

The estimated portion of enterprise organizations compromised in the past 12 months in an attack originating with an endpoint device.

$7.12 million

The average financial loss of companies (see above) compromised in endpoint device attacks.

80%

The proportion of 1,300 IT security professionals who said software supply chain attacks have the potential to become one of the biggest cyber threats.

78%

The percentage increase in supply chain attacks, via loopholes in third-party services, between 2017 and 2018.

2019

The year President Donald Trump, recognizing the potential "catastrophic" impact from supply chain threats, signed an executive order for securing the IT supply chain.

"U.S. critical infrastructure and governments at all levels rely heavily on Information and Communications Technology (ICT). Ensuring resilience and trust in our ICT supply chain is more than just a cybersecurity issue – it touches national security, economic security, and public health and safety."

Finding Hidden Risks in the Supply Chain

CHALLENGE: GLOBAL-SCALE RISK

Global supply chains span continents and time zones, vastly enlarging potential attack surfaces. When government agencies procure IT products from sources that can't be verified as secure, they introduce into their enterprise global-scale risk.

Glen Urban, former dean of the MIT Sloan School of Management and originator of trust-based marketing, posited that all successful business is based on trust. Federal agencies must have confidence in a procurement process comprising tens of thousands of suppliers and sub-suppliers.

"If you can't trust your partners or your supply chain, you are not going to be successful over the long term," Gardner said.

Like disruptive natural events, bad actors introduce chaos into the supply chain. The biggest source of disruption: State-funded advanced persistent threats (APT) seek to control or sabotage government IT systems and agencies. Similarly, criminal organizations try to embed ransomware in order to extort funds from victims. They also steal private data, such as credit card information, usernames and Social Security numbers to fuel the lucrative and illegal practice of identity theft.

"Civilian hackers, a lesser threat, are dangerous because they are unpredictable," Gardner said. "Sometimes they screw up networks and shut a whole company down."

Saboteurs have installed counterfeit components on the boards of products, such as the "ET Phone Home" hack that siphoned off targeted data streams on compromised products. A sample audit of products shipped by a large IT vendor a few years ago found that 30% of parts sold by the company weren't legitimate components. "Underhanded suppliers … had taken out the boards and put in a lesser board that didn't run as fast or have as much memory," Gardner said.

In another potential ruse, a ship departs a location like Taiwan with IT products bound for California. Its tracking system goes down in transit. The vessel arrives two weeks late. Did the ship change course to avoid a typhoon, or some other reason stated by the vessel's captain, or was there a rendezvous at sea or deviation from the route that compromised the products' integrity?

SOLUTION: PRACTICING PROCUREMENT HYGIENE

Securing the IT supply chain is a process of working with trusted partners to analyze risk and make sound decisions. Established IT companies have relationships with suppliers, developed over decades, that they leverage to reduce that risk.

Historically, the drivers of government acquisitions were cost, performance and scheduling (CPS). Agencies acquired IT products with specific performance capabilities and metrics, on a schedule, at the best value or lowest price technically acceptable. That's no longer good enough, say a growing number of leaders in the field.

"We've got to look at who has the best cybersecurity and who has the most secure supply chain, and only then look at cost, performance and schedule," Gardner said.

Procuring technology from the low-cost bidder is a high-stakes gamble. Cities victimized by ransomware attacks in recent years were vulnerable, in part, because they had procured IT products with security flaws. "If you don't make product decisions with security as the No. 1 factor in the selection process, you are putting your mission and your agency at risk," Gardner said.

Moreover, agencies can anticipate and plan for supply chain disruptions. When a tsunami hits Japan or Taiwan and wipes out a factory, or a tornado levels a large IT storage center in Tennessee, disruptions to supply chains can compromise the functional capacity of agencies that don't have backup. Agencies can lessen the impact of unavoidable disruptions by planning for redundancy – diversifying procurement channels and partnering with vendors that have strong security records.

"You're not going to cover every possible threat or risk, so you try to design your system and your processes to identify and focus on major risks, the ones that could cause the most damage," Gardner said.

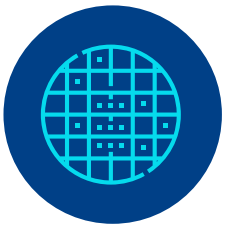
Best Practices in IT Supply Chain Security

Although threats to the security of IT supply chains can never be eliminated, agencies should adopt practices and policies for minimizing their exposure to potential breaches. Frequently, best practices available to agencies and vendors mirror initiatives pursued by high-level security agencies, such as the National Counterintelligence and Security Center. NCSC recently issued a report on supply chain risk management.

Stop thinking of supply chains as innocuous pipelines of IT products. Every supply chain potentially has a Trojan Horse linked to it. Pay attention. NCSC is putting into place new processes "to identify suspect or high-risk vendors, products, software and services that pose a risk to our economic and national security."

Take action now to strengthen IT security protections that will be required of emerging 5G wireless technology. Adopt a risk-based approach to supply-chain security. "Threat detection, response, and mitigation tools should be leveraged across all aspects of the lifecycle," NCSC advised. "These tools and capabilities should be optimized for specific supply chains."

Buy from IT vendors that have invested resources to develop the most secure IT supply chains. To improve vendor integrity, NCSC "will create a supply chain risk assessment shared repository, address deficiencies in the federal acquisition process, and seek more streamlined authorities to exclude high-risk vendors," the report states.



Use AI-based malware defense solutions to expose threats that otherwise could go undetected for months or years. Advancing detection capabilities on a parallel path, NCSC reported initiatives to "enhance capabilities to detect and respond to supply chain threats ... and to develop access to new sources of information and increase the analytic capacity to understand and assess foreign intent and capability to exploit U.S. supply chains."

Pop the hood on the technology, the manufacturer and the vendor. Look inside. Does the manufacturer have a trusted computer network? Do they use zero trust principles? Is cybersecurity built into the product or bolted on after the design? Demand original equipment manufacturer (OEM) parts and components and seek out vendors who are committed to using them. "To advance supply chain integrity across the federal government, supply chain security must be elevated to a top priority and be present throughout the acquisition process," NCSC said.

HOW HP HELPS

HP is an industry leader in cybersecurity and IT supply chain security. HP invests billions of dollars annually to fortify the cybersecurity of its products and to protect the company's networks.

HP's trusted relationships with suppliers (and their suppliers' suppliers), developed over many years, provide a robust, front-line defense against cybersecurity threats. HP has also invested in secure networks that protect supply chain data.

"You can't afford to be second place in this business," Gardner said. "It's not like car rentals. 'We Try Harder,' just doesn't cut it in IT security."

Learn more: www.hp.com

Conclusion

Proliferation of complex IT supply chains has created a critical security threat. Developed to meet growing demand for cost-effective technology products, global IT supply chains have become a conduit for nefarious forces seeking to infiltrate the IT systems of legitimate organizations, including government agencies. The scope and complexity of IT manufacturing and distribution networks contribute to the challenge of maintaining supply chain security – and the technology products they deliver.

There is no easy solution for thwarting threats to supply chain security, no software for reliably repelling bad actors. The cost of vigilance is high, yet the cost of cutting corners can be higher.

To minimize supply-chain risk, agencies can align themselves with vendors known to promote robust cybersecurity programs, including supply chain security – that is, established vendors with a record of cybersecurity rigor.

ABOUT HP

HP creates new possibilities for technology to have a meaningful impact on people, businesses, governments and society. With the broadest technology portfolio spanning printing, personal systems, software, services and IT infrastructure, HP delivers solutions for customers' most complex challenges in every region of the world.

More information about HP (NYSE: HPQ) is available at www.hp.com.