How Emerging Technologies Impact Supply Chain Security

Strong supplier relationships and accurate data will make or break supply chains as federal agencies modernize their IT.

Kate Macri
Fri, 11/06/2020 - 15:41

Supply chain security can barely keep up with the breakneck pace of technological innovation and COVID-19 demands, federal IT leaders said at an ACT-IAC Emerging Technology Forum this week.
But supply chain security leaders like Cybersecurity and Infrastructure Security Agency and the General Services Administration are working hard to provide guidance and resources for federal agencies seeking to secure their IT supply chains in a mutable tech environment.

“For emerging technologies, we cannot take supply chain in a one-and-done strategy,” said GSA Deputy Commissioner for Acquisition in the Office of Technology Keith Nakasone. “I'll use the example of 5G. 5G will allow us to compute power down to the edge and edge devices. As we move things further out it really comes down to the data and how we manage risk. If we know from an acquisition perspective, we look at the prime contractor. Now we have to be concerned further down the chain and have to be concerned about vendor risk as well.”

Federal agencies can supercharge supply chain security by altering language in contracts to lock in security standards from the start as they modernize their networks for 5G.

“As we build out cases for emerging technologies, we're going to have requirements and language in the contracts to have some insight into the technology itself,” Nakasone said. “We're going to have these requirements that will be potentially unique to some of the emerging tech, but time is changing as well. We're in the infant stages of how we inject emerging tech, but we have to look at supply chain risk and cybersecurity moving forward.”

Noel Kyle, Supply Chain Risk Management Initiative lead for the National Risk Management Center at CISA, said public-private partnerships and information-sharing are vital.

“We have a program that consists of three pieces: partnerships, frameworks and analysis,” she said. “How do we put processes in place to share information across the federal government and the private industry, and where do we store that information, what kind of repositories do we build so people can get that access?”

Real-time visibility of the IT supply chain can slump because not every federal agency can see its vendors’ suppliers and those suppliers’ suppliers, all the way to a product’s various points of origin.
Throw emerging technologies into the mix, and IT supply chain complexities snowball.

“What 5G is doing for us, it's going to enable use cases that were never possible before,” said Nick Ward, CISO at the Department of Justice. “To get [internet of things] devices more and more, it's scary and exciting all at the same time. How do we protect that? What CISA is doing is critically important to make sure vendors understand supply chain risk is important. We need to make sure those vendors are paying more attention to that as they're bringing more things to market.”

At DOJ, zero trust and encryption are "crucial" tools, but strong vendor partnerships increasingly command attention.

“Partnerships with vendors are going to be crucial going into the future as the market gets more robust,” Ward said.

Supplier relationships boost security, but can also limit disruption. More than half of federal organizations reported a “catastrophic impact” to their supply chains due to COVID-19, according to a CISA survey. Big themes included a lack of supplier diversification and poor inventory management.

“[The survey] exposed how a reliance on lean inventory models, which in a normal environment provides efficiency and cost-effectiveness, when disrupted, could cause delayed deliveries,” Kyle said. “It also underscored the difficulties companies faced in understanding their junior tier suppliers.” CISA will release another report in November addressing these subjects, she added, “like mapping out the supply chain, broadening the supplier network, shifting amounts for inventory health.”

In the meantime, federal agencies can improve data collection to sketch a more accurate snapshot of their supply chains, and train the federal workforce to interpret that data.

“When we look at supply chain and the IT commodities, there is a heavy lift or demand on mobile devices as well as tablets, laptops,” Nakasone said. “One of the things we need to consider is the tools, how to access data in a distributed environment. The first thing is educate, train, develop and move forward.”