SUPPLY CHAIN connect™

By SUPPLY CHAIN CONNECT STAFF

All-Star Webinar Cast Addresses the Nation's Cybersecurity Issues

As the list of cybersecurity threats and vulnerabilities that public and private organizations have to worry about grows, Politico scrambled a group of experts to discuss the problems and brainstorm solutions.

On June 26th there was a meeting of the minds in Washington, D.C., where a group of government officials and supply chain experts converged to discuss how to go about securing the nation's supply chain against the growing number of security vulnerabilities. The presentation was both timely and relevant in an era where post-pandemic supply chain fraud is increasing by 13% every year.

"Given the rapidly evolving and highly sophisticated nature of modern cyberattacks, logistics firms and, by extension, their vendors and suppliers should be well aware of the cyber threat landscape," Institute of Supply Management (ISM) states, pointing to the 2021 ransomware attack on Colonial Pipeline as one of the most notable examples of this, but certainly not the only one. That particular group of nefarious cybercriminals disrupted fuel and gas supplies to regions in the Southern U.S., resulting in a $4.4 million ransom payment and devastating socioeconomic fallout.

To help sort through the long list of vulnerabilities, find solutions and also talk about how Uncle Sam is shielding the country against current and future threats, Politico hosted *On the Watch: Securing America's Supply Chain for Critical Infrastructure* at the end of June. Some of the notable participants were Doug Bush, assistant secretary of the Army; Jeannette McMillian, office of the director National Intelligence; and U.S. representatives Jake Elizey (Tex.) and Mikie Sherrill (N.J.).

The presentation was sponsored by Exiger, an artificial intelligence (AI) supply chain company that also had several panelists on call. Together, these public and private sector representatives discussed the latest challenges and solutions for protecting the supply lines into America's critical infrastructure.

Political & Policy Implications

Politico's Kevin Barron kicked off the 90-min. event by discussing the importance of both China and cybersecurity in the modern supply chain. After the COVID-19 pandemic, he says, more people started paying attention to the supply chain and the reliance on other countries for certain goods. Barron emphasized the need for increased coverage and understanding of critical minerals and metals, as well as cybersecurity and insider threats.

Barron also mentioned the political and policy implications of the supply chain issue, especially in a presidential campaign year. "We all remember when a lot more people in the world started to pay attention to the supply chain and realizing maybe we shouldn't be relying on others for certain things," Barron said. "That's become an enormous news topic and one that we'll be hearing about for a long, long time."

Exiger's Brandon Daniels and With Honor's Rye Barcott continued the COVID discussion, noting that counterfeit metals are getting into syringes that deliver lifesaving drugs while "Russian software is lurking inside of our federal govern-

ment infrastructure." Other problems include companies "masquerading as U.S. entities" when they are actually owned by adversaries.

McMillian took us on a reflective trip about eight years in the past, at which point "finding the smoking gun" was the government's primary response mechanism for cybersecurity issues. She says the focus has since changed and now involves more public-private partnerships centered on early detection and threat minimization. "It takes that [kind of] partnership to make sure we can continue to collaborate and have that transparency across the supply chain landscape," McMillian said.

Asked by Barron whether the government is partnering with private industry to a great extent in 2024, Daniels said that bridge exists and is focused on "building and maturing operational collaboration so we can secure our critical infrastructure against all threats and hazards." The partnership has evolved, he added, as has the widespread understanding that our critical infrastructure is on the front lines (namely in cyberspace).

There's still more work to be done. "No one has enough of the right people to do this; everyone wants more," said Daniels, who added that the Department of Homeland Security (DHS) has a council that's focused on using AI throughout the department's various missions, cybersecurity included.

Getting to the Bottom of the Problem

On a different panel, retired Air Force Major General Cameron Holt, who is now president of Exiger Government Solutions, talked about the government's attempt to reshore manufacturing that was taking place in China. "The Chinese Communist Party has really been focused on what America does not see as war, which is economic and information coercion and manipulation in a predatory fashion," Holt explained. "And over the decades they've been engaged in that in a very methodical process."

Exiger's Katie Arrington discussed how companies are "masquerading" as U.S.-based organizations and moving from country to country in an attempt to continue doing business with domestic private and public organizations. "Cameron and I were in the Pentagon together, and one of the biggest things that we struggled through was how do we share risk without getting sued?" Arrington explained, noting that most organizations lack clear visibility over suppliers, and particularly past Tier One.

The answer may lie in heightened awareness of the potential threats and vulnerabilities that organizations may be exposed to. "Industries need to understand that our adversaries are out to play to win," Arrington said. "Industry is building is our national defense, and if we're not working with them side-by-side—the Department of Defense (DoD), regulators, legislators and the White House—to create requirements to fund and resource it, we're never going to get to the bottom of this."