Supply Chain Strategies – A Call to ACTION

Cyber Security Summit International Webinar Series
April 27, 2021

Speaker: Joyce Corell, Assistant Director Supply Chain & Cyber Directorate, National Counterintelligence and Security Center (NCSC)

Moderator: Sean Costigan, Director & Co-Founder, ITL Security; Professor at George C. Marshall European Center for Security Studies

Report Author: Lindsey Konerza, Business Systems Analyst, University of Minnesota; Student University of Minnesota Technological Leadership Institute – Master of Science in Security Technologies (MSST).

Speaker Bio:
Joyce E. Corell is the Assistant Director of the Supply Chain and Cyber Directorate of the National Counterintelligence and Security Center (NCSC). Prior to this posting, she was the Assistant Director for the Strategic Capabilities Directorate in the Office of the National Counterintelligence Executive (ONCIX.) Corell served at the National Security Agency (NSA) for 23 years. Her last assignment was as the Chief of Technology Policy in the NSA Commercial Solutions Center. She spent a significant portion of her career focused on various aspects of defensive and offensive computer network operations, from capability development of national policy and legislation. Complementing these roles, Corell also led various activities surrounding partnerships with the private sector ranging from technology transfer, export control licensing, and the development of strategical alliances, both domestic and international. Corell graduated from William & Mary with a B.A. in Political Science. She received an M.S. in National Security Strategy from the National War College.

Introduction:
National Supply Chain Integrity Month has once again kicked off with the "Call to Action" awareness on supply chain risk management. The following Rapporteur report delves into the history of supply chain risk management at the federal level and the cross-collaborative controls that have been put into place to build and strengthen a more resilient supply chain.

History of Supply Chain Risk Management & Government
The public and private sectors often gave supply chain risk management a back-burner position to other forms of activities. No one cared, people and companies were busy, and no one gave this topic the proper attention it so deserved. The tipping point came when Kaspersky Labs, a Russian national cybersecurity and antivirus firm, made headlines with its ties to the Russian Federal Security Bureau (FSB). If entities located in the US were using Kaspersky Labs technology, the data likely would be transferred to Moscow with no way of protecting our nation state data. The risk was deemed too high if

this product were on a federal system, and pushing back against the authoritarian regime would become impossible. Understanding supply chain risk in this scenario led to recognizing how inflexible our policy tools were. The US needed to find ways to put the right policies and regulatory language into safeguarding supply chains. For the first time, real national-level attention was given to supply chain management.

Government Actions That Ensued – Power of the Purse

At the national level, the Executive Branch, regulators such as the Federal Communication Commission (FCC), and Congress acknowledged that risk was present, risk needed to be managed, and mechanisms needed to be put into place to manage supply chain risk. The FCC prohibited spending of federal funds on covered entities resulting in domestic carriers looking to operate their network could not use federal monies on high-risk suppliers like Huawei and ZTE. In late 2018, Congress made updates to the National Defense Authorization Act and the Foreign Investment Risk Review Modernization Act (FIRRMA), resulting in more robust controls over emerging and sensitive technologies. Choreography started to come together as the government recognized risk and acted with purpose and acknowledgment. These actions would set the tone for a whole nation approach to risk management domestically and internationally.

Biden Administration – Moving Full Steam Ahead

President Biden signed the Executive Order on America's Supply Chains. This executive order has both short- and long-term goals as it looks at specific supply chains, associated risk, and policies to help close the gap and reduce overall risk. In the short term, the four key supply chains addressed included semiconductor supply chain, advanced batteries, access to critical mineral and strategic materials (rare earth minerals), and pharmaceuticals, including advanced pharmaceutical ingredients. The executive order also contained long-term studies within the telecommunication industry and transportation industry and would highlight further how cybersecurity underpins these areas. The entire business operations environment, including digital assets, needs to be protected.

Awareness in Supply Chain – Call to Action

In the wake of Solarwinds, no longer can one review and assess risk in isolation, but the totality of the environment needs to be understood and managed. Thinking evolved to include security as a foundational aspect that needs to be part of the risk equation.

Lloyd's issued a Cyber risk report titled The Emerging Cyber Threat to Industrial Control Systems. The insurance industry would need to think differently in its approach to risk if someone took action through cyber means, and the same action would go on to cause a physical consequence. It becomes clear that security and safety merge and are two sides of the same coin. From a safety perspective, standards are out there and exist (ex. food safety or drug safety standards). The question finally becomes, how does one think about safety and security within the cyber realm?

Conclusion

As technology evolves, understanding the risks associated with the supply chain must be at the forefront of our discussions. To support and expand resilient supply chains, we need to maintain and develop healthy partnerships internationally. At home, we need reliable and trustworthy vendors and the ability to work together at the global level collaboratively. We must unite with a common goal to maintain a healthy and vibrant supply chain.