The Importance of Communication in Smart Supply Chain Security

Mandy Stanton
mstanton@mwlaw.com
(501) 688.8844

10/22/2020

According the National Institute of Standards and Technology's (NIST) Best Practices in Cyber Supply Chain Risk Management report, smart supply chain operations are ushering in a fourth industrial revolution through digitization and network connectivity of all industrial processes. Smart supply chains leverage automation, robotics and data management to provide greater efficiency at lower costs. Its capabilities enable end-to-end, real-time information sharing and communication internally and externally along the supply chain to improve performance.

Despite the dynamic nature of the future of supply chains, security is an important aspect of interoperating with others in networked and cloud-based environments. In 2019, supply chain attacks were up significantly. Of the respondents interviewed as part of BlueVoyant's Global Insights: Supply Chain Cyber Risk report, 92% had experienced a breach that originated from weakness in their supply chain in the last twelve months. No cloud-based operational service will ever be completely free from cyber risks. There is often a misconception that a business's vendor is secure or the vendor presents their products as secure. However, upon integration of systems, vulnerabilities can float to the surface. So how can we manage the endpoint risk?

Communication between manufacturers, integrators and end users is more important than ever to ensure all parties have a sufficient understanding of the products and intended services. From an internal perspective, it is important for supply chain managers to have a "big picture" approach to security with other areas of management to protect the organization's digital assets and create an integrated approach to security. Cyber criminals seek to exploit the flow of data assets – whether physical or virtual.

Business should identify these integration points by mapping the supply chain data flow. Cyber risks arise from not comprehending what information is being collected, where and how it is used and by whom, and where it is stored both internally and externally. Mitigation starts with this map and setting expectations for these operational touchpoints.

While vendors should have a vested interest in ensuring their device have strong and effective security solutions and those solutions should be built in to the design of the product, it does not prevent an integrator from unknowingly creating an opening into the system. If an integrator or user does not comply with network controls, it can endanger the security framework. A proficient grasp of the product security at all levels may reduce human error to which many businesses fall prey.

As smart supply chains rise, security will only become more important to combat the loopholes the process creates for attackers. Laying the groundwork for a comprehensive foundation to supply chain security requires effort from everyone to reduce these threats as much as the landscape allows.