Cyber Threats to Supply Chain on the Rise

www.globaltrademag.com/global-trade-daily/commentary/cyber-threats-to-supply-chain-on-the-rise

THE TECHNOLOGY THAT SUPPORTS A SUPPLY CHAIN OFTEN INVOLVES MULTIPLE NETWORKS WORKING TOGETHER: That makes monitoring a supply chain from start to finish difficult.

Cyber threats to supply chains have become increasingly prevalent due to extensive sharing of digital information between organizations and their suppliers. Still, some companies don't do enough to protect their assets, sensitive data and information by addressing the risks within their networks. Many breaches don't start at the top – attackers start somewhere in the supply chain and work their way up to the target through a trusted supplier.

No company or person is completely safe in the cyber arena, which means security must be part of everyone's job. The ancient proverb "it takes a village" is certainly applicable – not having a good understanding of cybersecurity, and what the risks are, can make you the weak link and an easy target. After all, you wouldn't rely on just one person to both pilot and serve drinks on a plane; how can you expect to rely on just one person in a 10- or 10,000-person company to ward off cyber threats and ensure the safety of the entire organization?

So what can you do?

Assess your risk profile.

Major security issues stem from companies not actively assessing their risk profile. Monitoring a supply chain from start to finish is difficult because very few companies use cyber-security products that are equipped to monitor their systems from end to end. Often, the technology that supports a supply chain involves multiple networks working together. By drafting and implementing a strong program, companies can address weaknesses and avoid becoming the victim of an attack. For example, companies should consider conducting ongoing vulnerability scans to protect against any new threats – a test only one-third of manufacturing companies surveyed in Sikich's 2016 report do on an annual basis.

Have a plan in place.

Well-planned decision making in the era of cyber risk is an important factor in protecting a company, and ultimately, a supply chain. Global supply chains are growing in complexity, so when it comes to cyber threats, you need a plan laid out for how you will respond *before* a breach happens – or remain vulnerable to the dangers that are damaging

to both people and businesses.

Provide risk training.

In addition to being aware of the potential threats that stem from cyber security failures, organizations should implement proper training and provide employees with information on how to mitigate the risk associated with supply chain cyber attacks and minimize the impact should an incident occur. As technology advances and improves, so do the criminals looking to target a supply chain. In order to maintain a high level of stability and employee understanding, companies must consistently update their processes and steps to mitigate risk.

Whether your business is small or large, don't make the mistake of thinking you're saving money now by not investing in cybersecurity measures. Cybercriminals are relentless and will stop at nothing to break into your system, which could end up costing more than the proactive measures that would protect against those threats. The harsh reality of cybersecurity threats in the twenty-first century could mean the life or death of your product or company.

Chloe Demrovsky,

CBCV, is the Executive Director at DRI International, leading nonprofit that helps organizations around the world prepare for and recover from disasters by providing education, accreditation, and thought leadership in business continuity and related fields.