SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Program Best Practices > Supply Chain >

Security's Opportunity in Supply Chain Security

At the February 2024 SEC Security State of the Industry (SSoI) briefing, SEC Subject Matter Expert of Global Supply Chain Security Mark Kelly and SEC Tier 1 Security Leaders emphasized the increasing criticality of supply chain security for companies across industries, as well as security leaders' unique potential to bridge functions and bring value in addressing it.

As the former Global Head of Field Security & Supply Chain operations for Dell, where he stood up end-to-end supply chain security, Kelly most recently came from an organization that clearly valued and prioritized the security of the supply chain. And Dell wasn't alone; world events of the past 25 years, from 9/11 and CTPAT to Brexit and Covid-19, have pushed businesses to an increased understanding of the many global interdependencies upon which their success relies.

Supply chain security extends across the business lifecycle, said Kelly. "It is a holistic end-to-end protection of your company's products or services, from procurement - whether it's your parts, your vendors, your components – to design and proprietary information, to the manufacture, production, and delivery of those products and services."

However, he noted, many organizations still view supply chain security as simple logistics -- nothing more than a means to an end. Such organizations are missing an opportunity to improve their assurance, resilience, integrity, and brand protection.

Here are two of the major takeaways from the full SSoI briefing.

The supply chain threat landscape is complex and changing.

Direct and immediate physical threats to product, such as cargo theft, are no longer the primary players in the supply chain threat landscape. Kelly pointed out that reports on supply chain risk from Overhaul, the World Economic Forum, CargoNet, WTW and others all identified the following four themes as critical to supply chain security:

- Climate (How will Category 6 hurricanes – a new designation created because of increased storm severity - impact shipping lanes?)

- Cyber (Can a cyberattack like the one suffered by Clorox in 2023 disrupt your ordering and delivery or cause manufacturing shutdowns?)
- Geopolitical (How will war, elections, tariff fluctuations, and regulation impact supply chain availability?)
- Third party risk management (Is every organization in your chain as secure as you? Do you rely on something more than self-attestations to prove it?)

In addition to these, litigation, financial crime, product damage, counterfeiting, theft of intellectual property, labor disruption, limited or single-source supplier availability, and brand damage can all play a major role in supply chain security.

Issues like these have to be dealt with through intelligence and risk ranking, said experts on the call, based on the data and profile of your own organization. However, said Kelly, "I've had number of clients tell me that they don't have to worry about things like cyber risk or geopolitical concerns, and to me, that feels a bit narrow. Unless you have 100% control of all of your materials, all of your manufacturing, all of your distribution – these issues do pertain to you."

Supply chain security can bring opportunities and value.

There are a number of areas related to both the stakeholder experience and operational efficiency where supply chain security can add value, according to SSoI speakers. Security leaders need to identify business priorities and apply a security lens to find opportunities in those realms.

If you track high value shipments or products, can you use that capability to improve your customer experience through estimated delivery times? Or increase efficiency by reducing overtime?

Can you educate, train and force multiply your physical security people to help evaluate issues in the field?

Can your staff facilitate regional discussions around cross functional training and awareness?

"In an effort to gain market share, companies are starting to use security as a differentiator, whether that entails enabling better operational visibility, realizing efficiency spend, or in some cases, even charging clients for heightened security," said Kelly.

Think about where you can embed security in the business cycle and how you can exert influence in non-security spaces. One speaker emphasized the need for security to create partnerships across the business and integrate actionable intelligence from across all functions.

Next Steps

Speakers advised SSoI participants to begin to educate themselves about supply chain security and its opportunities in their organization, even if they don't feel the need to pursue an increased scope for supply chain security at this time. More companies are asking for end-to-end supply chain security, and security leaders need to be prepared to respond.

SSoI briefings are regular events at which SEC faculty and Tier 1 security leaders share insights on specific areas of concern to security leaders. Information on the Tier 1 Security Leader program is available here.

For a discussion on what the best companies are doing around supply chain assurance, contact us.

Visit the Security Executive Council web site to view more resources in the **Program Best Practice : Supply Chain** series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com
Website: https://www.securityexecutivecouncil.com/

