



CENTER OF EXCELLENCE
HOMELAND SECURITY-EMERGENCY MANAGEMENT

Securing the Supply Chain Forum – 4/13/16

Securing the Supply Chain Forum

Background

The Centers of Excellence for Global Trade & Supply Chain Management and Homeland Security Emergency Management collaborated to conduct a Forum around the educational and business sector of the Supply Chain industry. The purpose of the event was to be a follow-up of the October 15, 2014 '*Protecting Washington State's Supply Chain: Security & Resilience Forum*' and provide an opportunity for industry representatives to address the needs and gaps with technology and security curriculum. It was important to ask representatives of the Supply Chain industry, "What are the best practices needed in order to help secure the supply chain and how does the new advancing technology play a role in that process?" The information gathered from the Forum would then be used to work with the community and technical college programs in Washington State to help modify or add new curriculum that live up to the training and education requirements/standards of the industry.

Overview

"Why do we want to lead off whether it is operational planning or educational when it comes to cargo theft?" Eric Kready, Intelligence Manager for FreightWatch International asked the attendees. Eric mentioned that it is intelligence that drives operations, while operations feeds intelligence and how it is important to know the threats and have the most intangible intelligence to lead with. Security rests on people, procedures, and technology. Violence is the key ingredient when it comes to cargo theft. The top three cargo thefts: (1.) food, (2.) clothing, and (3.) shelter/building supplies. All of these items are needed by everyone, they are unidentifiable, and are easily sold. Criminals focus on the supply and demand, especially in growing populations where certain supplies are needed. The targeting of pharmaceutical drugs are expected to increase.

Countries at most risk of cargo thefts:

- United States
- Russia
- Mexico
- Brazil
- South Africa

It is important to take into consideration that while some countries may appear safe to conduct business with/in that does not mean they have laws to prohibit theft. For example, Australia actually prohibits laws against cargo theft. Canada and some countries in Europe also do not

have laws that prohibit cargo theft. The most prolific crime across the globe is human trafficking with over 250,000 humans enslaved every year. Drug trafficking is also another prolific cargo crime, along with weapons trafficking. Criminals will utilize supply chains that are already in place.

Key Findings

Ways to help secure your supply chain:

1. Know the threats.
2. Consider insurance coverage and check backgrounds of all business clients.
3. Make your presence known in your supply chain. Constantly revisit pieces in your supply chain.
4. Identify the weak points on each type of steps in cargo transit.
5. Solve own problems with blue collar approach, and then get in coalitions to see large scale.
6. Set standards, train workers to deal with issues, and audit what supply chain partners are doing.
7. Consider the risks by creating a business continuity of operations plan (COOP).

What are the common versions of cargo theft?

- Ninety percent of theft is organized. Inside information is spotted such as insurance amount (whether items are high or low), routine delivery, and bill of lading, set up as team driver.
- Two-thirds theft occur on Fridays and/or Saturdays, because it prevents immediate detection.
- Fictional pick-up spots.
- Thieves will be patient and watch for opportunities. They also observe the routine of the drivers.

What steps can lower chances of cargo theft?

- Prevent by using: background investigations, security awareness training, in-transit security policies, GPS tracking in multiple places, and lock and seal loads with quality tools.
- Consider using the following technology: Global GPS, RFID, and e-seal, tracking and monitoring platforms.

There are at least three types of vulnerabilities: (1.) natural, (2.) intentional, and (3.) unintentional. Unintentional threats are not talked about very regularly, if at all. They tend to come out of complexities and lack of managing those complexities. Unintentional threats are outside of the system. The systemic comes from the lack of basic understanding of who is responsible. Vulnerabilities are increased as partnerships are increased.

Thefts can be a small part of daily/yearly total freight movement. There is no real value in chasing theft as it is best to have your business's insurance company handle it. Theft can bring down a whole supply chain, especially with an on demand system. Technology that can jam a

GPS are being used. Brand names can even become damaged resulted from the cargo hitting the black market.

While technology and gadgets may make life easier, such as refrigerators now being able to scan contents and order supplies, there are some risks. The danger is cyber hackers can get into our systems through back doors, and new gadgets we add on. One of the problems is the large number of new start-up companies producing the programs. They can forget cybersecurity or they can be purchased for the technology created.

What are some cyber dangers?

- Social media image.
- Breaches in large systems, and programs that copy and duplicate your digital persona.
- Extortion of program data or locking all the data is a criminal tactic.
- Manipulate data by inserting or changing information.
- Hacktivism. Reveal how to get into programs.
- Hacking new drone technology.

Educational Gaps and Analysis

- Students' knowledge management jobs are evolving to knowledge based job. Robotic control with humans overseeing capability.
- Ethics in school is almost too late; it needs to be a parenting issue.
- Consider IT as the world expands more emphasis needs to be on monetary protection.
- Use open source intelligence.
- Use students as research tools for businesses.
- Consider transportation standards course in security.
- Ethics. Schooling does not teach how to be a good person. Cultural changes. Ethics are part of curriculum but only so much time and schooling opportunity to teach ethics. Challenge industry with a new focus to ethics.
- Use of forecast modeling! Wrong interpretation is just as damaging as low level of knowledge.
- Consider class room topics are current not just following a text book.
- Create classes on international issues not just a US focus.
- Natural disasters like earthquake can hurt world economy.
- Sharing financial risk by driving world economy away from materialism.

Takeaways from Attendees

- Supply Chain is knowledge management.
- Intelligence drives operations; operations feeds intelligence.
- Sharing is caring. More collaborations.
- Establishing threat streams.
- Integration of technology.
- Confluence of risk management.
- Countries not permitting cargo laws.
- Private sector addressing risks/threats.
- Change out of truck drivers.

- Security practices in the U.S.
- Cargo interception – risks.
- Career and academic opportunities.
- Private sector has a lot on the ball; government sector can learn a lot.
- The process to the strategic national market.
- The gaps with the youth market.
- Risk concerns with the hiring process.
- How drugs are moved up north while electronics move south.
- Cargo threats can be seen as insider jobs.
- Cybersecurity and supply chain starting to intersect with each other.
- The increase need for collaboration between companies and academia.
- Knowing your overall supply chain.
- Audit discussion – expect what you expect.
- City/state level awareness.
- Ambiguous of supply chain industry.

Conclusion

For next year’s Supply Chain Forum it was recommended to have a broader discussions regarding individual supply chain functions. Sources for the supply chain functions comes from the Master of Industrial Distribution degree from Texas A&M. There will also be segments around the topic of securing our food supply since food and drink is often the most stolen item in the USA. There have also been concerns around farm to forks food adulteration that could happen along any part of the food chain. The intention and unintentional act that cause illness and death.

Business Process (Function or Supply Chain Specialty)	Description	Example Risk
Sourcing	Supplier Management	Sole source provider, Suppliers w/o ethics
Stocking	Inventory Management	ERP implementation
Storing	Warehouse Management/Fulfillment	Theft/shrink in the warehouse, Temporary/Seasonal employment practices
Selling	Sales management	Picking customers that don’t protect the brand
Shipping	Carrier management	Cargo theft
Supply chain planning	Supply chain optimization	Poor forecasting
Support Services	Information Technology	SaaS- data protection
Reverse Logistics*	Return of goods from customers or frustrated cargo	Normally a lower priority and lower visibility for optimization/security

*Not from Texas A&M