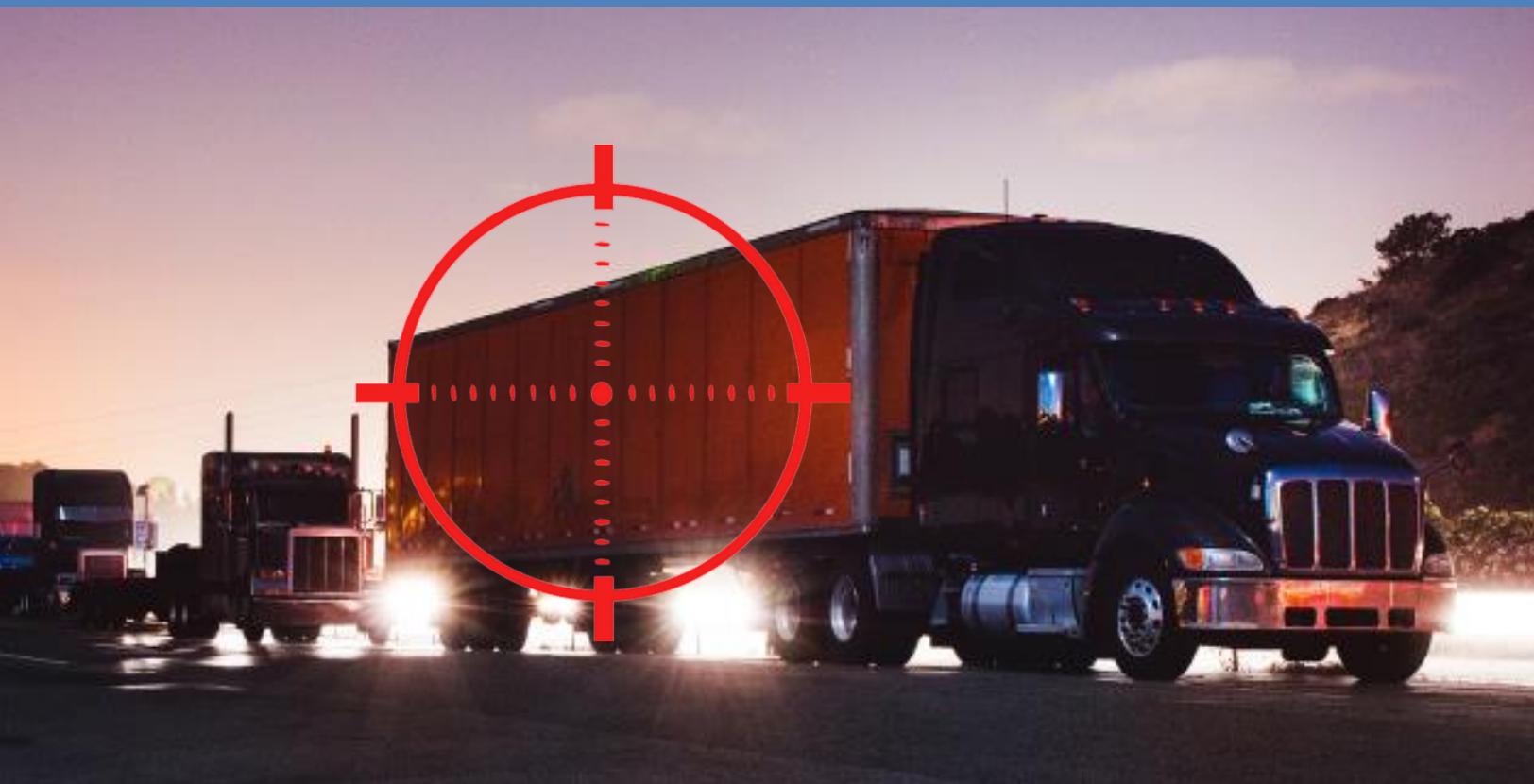




2016
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

IMPACT ON SUPPLY CHAIN SECURITY OF TCO INVOLVEMENT IN NON-DRUG CRIME



Group Members:

Eliasz Krawczuk – Crumpton Group, LLC
Emily Woodard – Fiat Chrysler Automobiles
Erin M. – DHS
Kevin P. – DHS
Mariko Kawaguchi – Element Case, Inc.
Robert Byrne – IBM Corporation
Ross Albert – HUB International

Public-Private Analytic
Exchange Program

January – August 2016

Table of Contents

Abstract	2
Introduction	2
Team Members	2
Non-Drug Crime Defined	3
Methodology	3
Findings	4
Government Overview of the Threat	4
Private Sector Overview of the Threat	6
Cross Collaboration	11
Conclusion	12

Abstract

The primary focus of this whitepaper is to identify and illuminate the greatest risks from transnational criminal organizations (TCOs) to the legitimate supply chain, specifically in the Mexico and United States markets. Our findings show that supply chain security is a primary concern of the various private sector entities we contacted, despite the fact that their experiences in Mexico varied. With concerns ranging from whether to arm and escort trucks en route through Mexico to awareness of stolen cargo, companies face a wide breadth of challenges in securing their supply chains. Threats to the supply chain are not limited to a specific government agency and remain a persistent challenge. Communication and exchanges of information between the government and private sector are improving; however, further efforts at collaboration should consider that the objectives of the government and private sector do not always naturally overlap. Increased transparency among trusted partners would contribute to a common working knowledge from which further best practices can be gleaned.

Introduction

The Public-Private Analytic Exchange Program is a six-month long collaborative project that brings together members from the intelligence community and private sector industry experts to explore key national security issues in greater depth. This year's topic areas ranged from applying private sector media strategies to fight terrorism, terrorist financing to new technologies in aviation security screening, to name a few. Our team was tasked with examining the impact on supply chain security of transnational criminal organizations' (TCO) involvement in non-drug crime.

Our team worked over a six month period to develop a joint analytical product of interest to both the private sector and the US government to better understand how to prepare for, prevent and respond to the threat of TCO's to the supply chain. Throughout the course of this project, our team's primary focus was to identify and illuminate the greatest risks from TCO's to the supply chain, specifically in the Mexico and United States markets.

Team Members

The Impact on Supply Chain Security of TCO Involvement in Non-Drug Crime team consists of seven public and private sector employees. Team members from the private sector hold security and supply chain risk-related positions at companies such as Fiat Chrysler Automobiles, HUB International, IBM, The Crumpton Group and Element Case. The public sector members come from the Department of Homeland Security and focus on border and trade security issues.

The following team members collaborated and contributed to creating this whitepaper:

- Eliaz Krawczuk – Crumpton Group, LLC
- Emily Woodard – Fiat Chrysler Automobiles
- Erin McKern – DHS
- Kevin Peters – DHS
- Mariko Kawaguchi – Element Case, Inc.
- Robert Byrne – IBM Corporation
- Ross Albert – HUB International

Non-Drug Crime Defined

For the purposes of this study, our team was focused on only those threats from transnational crime that are non-drug related.

While the sale of drugs and the associated violence that comes with it remain extremely profitable, TCO's have diversified their business operations considerably. Other profitable crimes such as piracy of stolen goods, extortion, oil theft and kidnapping tend to have a more direct effect on businesses and their supply chains.

Methodology

Our team's independent assessment of the impact on supply chain security of TCO involvement in non-drug crime was conducted from January through September 2016. Our work was guided by a number of key principles and utilized a set of carefully considered methodologies, which are described below:

From the outset, our team made clear that the goal was not to expose any proprietary or confidential information of private and public sector contributors. To that end, we provided every participating source with an assurance of confidentiality on two levels:

- (1) That the information provided by an individual source would not be attributed to that source in this paper nor in any other outside communication to the public.
- (2) That the names of government agencies, corporate entities and individuals contacted during this study would be anonymized in a manner sufficient to ensure any sensitive information is protected.

In order to formulate a better understanding and background knowledge of TCO threats to supply chains in Mexico, our group researched various open sources such as news articles, academic journals and government reports. In addition, we held meetings with government agencies including the DEA, DHS, Customs and Border Protection as well as local and state fusion centers for public sector experiences with these threats. We also met with private sector

companies across various industries including retail, manufacturing, information technology, food, beverage and logistics in order to ascertain their supply chain practices, vulnerabilities and ‘lessons learned’ while conducting cross-border and internal operations in Mexico.

Findings

We found that supply chain security is a main concern of the private sector entities we contacted, despite the fact that their experiences in Mexico varied depending on factors such as size and scale of operations, particular transit routes and proactive security measures in place. With concerns ranging from whether to arm and escort trucks en route through Mexico to awareness of stolen cargo, companies face a wide breadth of challenges in securing their supply chain. Threats to supply chain activity are generally highest in areas with inadequate local security services that are often susceptible to corruption. In general, companies with larger operations in Mexico were better equipped to handle TCO threats and to absorb the potential loss of products. Their improved capabilities were due to broader resources, although the manner in which companies addressed their specific vulnerabilities diverged based on their prioritization of resources.

Government Overview of the Threat

Main TCO threats to supply chain from the US Government’s (USG) perspective

Upon interviewing several public sector partners responsible for intelligence gathering, cross-border operations, and port and traveler security, we found that threats to the supply chain were not limited to a specific government agency. The USG agencies that participated in this project predominately focused their attention on TCO involvement in the drug trade through private sector supply chains. Their drug-focused approach was aimed at reducing the flow of drugs into the United States across the southern border and through air and sea ports. This, however, was not necessarily aligned with private sector efforts to reduce TCO activity against their supply chains outside of the United States.

For both Agency A and Agency B, the use of cargo containers to smuggle drugs and other illicit goods remains a significant concern.¹² Agency A monitors thousands of air and maritime cargo containers as they pass through screening each day. Technology screening tools can be effective in monitoring cargo, but a persistent challenge with cargo security remains the human element, according to government partners.³ Controlling who is in charge of cargo is key to prevent

¹ Agency A. "Supply Chain Risks at US Port." Personal interview. 24 May 2016.

² Agency B. "Supply Chain Risks from Drug Crime." Personal interview. 25 May 2016.

³ Agency A. "Supply Chain Risks at US Port." Personal interview. 24 May 2016.

exploitation by criminals. For example, most airlines hire their own personnel to handle baggage and cargo. A growing concern is the ability for TCO's to coerce supply chain personnel or embed their own members as an insider threat handling cargo at air and sea ports.

Additionally, Agency A indicated that export control is a growing challenge for the public sector working at ports and border crossings. Limited resources combined with the agency's focus on import control makes TCO appropriation of exports a significant vulnerability. Nevertheless, Agency A is pushing for preclearance operations to be conducted at the point of consolidation for export supply chains in the future, and discussions for a vetted exporter program are ongoing.⁴ US agencies also cited their inability to limit the movement of drug profits back to TCO's based in Mexico. Agencies are restricted financially, but also by infrastructure, as restricting the flow of traffic southwards would also slow US-Mexican trade. However, the relatively unrestricted movement of southbound US dollars enriches TCO's and ensures that TCO's are financially solvent. The continued flow of money southwards most likely also motivates TCO's to continue in their attempts to move drugs into the United States, as well as funding non-drug crime. Although criminal exploitation of the supply chain to move contraband such as narcotics remains a principal concern for the US Government; non-drug crime such as implementing insider threats, money laundering, extortion, bribery, kidnapping and infiltrating export and import operations are constant public sector concerns.

What measures has the USG taken to address these threats and risks?

When discussing supply chain risks for several public sector agencies, it became apparent that threat mitigation depended largely on cooperation with other public sector partners and foreign entities. At a major US port of entry, Agency A indicated that their vetting of cargo and travelers begins abroad; consisting of pre-clearance locations, diplomatic attachés, and customs-trade partnership programs such as Customs-Trade Partnership against Terrorism (C-TPAT).

“Agency A indicated that their vetting of cargo and travelers begins abroad; consisting of pre-clearance locations, diplomatic attachés, and customs-trade partnership programs...”

For Agency A, cargo inspections are a multi-layered process, beginning with mandated advanced information on freight. Before freight arrives at the port, this agency is aware of the type and quantity of products coming in. Furthermore, federal employees of Agency A are tasked with inspecting cargo before it is loaded for shipment. Agency A also conducts central and local targeting and risk assessment prior to and after arrival of cargo to the port of entry.⁵ This multi-tiered screening procedure often makes time-consuming, physical inspections of cargo unnecessary unless red flags are detected.

⁴ Ibid.

⁵ Ibid.

Agency B emphasized that commercial trucking across the US-Mexico border and within the US is itself a huge network. From a major transit hub, for example, commerce via truck can reach 80% of the US population in within 48 hours. Because of the sheer amount of commercial cargo moving across the border each day, Agency B recommends addressing the vulnerability through close cooperation with local partners. State- and municipal-level entities can respond more rapidly to on-the-ground challenges through law enforcement, legislative regulation, and leveraging local business associations. Agency B typically advises their local partners with ongoing investigations but generally pushes for local-level security.

State-run Agency C works within a national network to engage with the private sector on security issues, including the vulnerability of industry supply chains. These working groups are continuously expanding to include new industry leaders, those most seriously impacted by TCO-targeting in Mexico and in the border region, and cooperative businesses eager to lend a hand to the public sector to address a major threat. Despite some reluctance from the private sector to share information with Agency C, complexities of both private and public sector operations indicate that continued discussions are both beneficial and necessary for both sides to understand one another.

Supply chain security depends on a continuous vigilance from beginning to end, so outside direct customs inspections, law enforcement operations, and vetting and screening programs generally localized in the border region, USG involvement largely consists of partnering with the private sector. Building trust and increasing transparency for both the USG and the private sector will be crucial to achieving meaningful measures to reduce the risk TCOs and others pose to supply chain security.

Private Sector Overview of the Threat

Main TCO threats to supply chain from the private sector's perspective and mitigation techniques

Supply chain risk remains one of the biggest security and business concerns of private sector companies operating in Mexico. A recent study by FM Global ranked countries in terms of their supply chain risk and resilience factors. According to FM Global's "resilience index," Mexico still presents a high level of risk in terms of supply chain security, but not quite as severe as other countries in the region such as Venezuela and Nicaragua.⁶ TCO's have a history of targeting the least protected supply chains and the companies whose products could earn the highest profit. The risks to companies are highest when products are in transit or at company sites in Mexico where a supply chain begins or transits through. When in transit, companies may face attempts

⁶ 2016 FM Global Resilience Index. *HOW DOES YOUR SUPPLY CHAIN RANK?* *Fmglobal.com*, Web. 2016.

by TCO's to directly steal goods. At company sites, TCO's may attempt to gain access to products or cargo.⁷ In some cases, criminals have attempted to move contraband by concealing illicit materials in cargo carriers during the loading stage of supply chain operations.⁸

TCO's also seek to have individuals employed at sites as "insiders" in order to introduce contraband into legitimate shipments, facilitate attempts to steal products at sites or provide TCO's with cargo transport information to ease attempts at theft during transit. Much like the public sector, multiple private sector partners have expressed their principle difficulty of preventing insider threats within their supply chain. In a 2015 study conducted by Vormetric Data Security, 87% of respondents from Mexico-based organizations indicated that their company is somewhat or more vulnerable to insider threats. Furthermore, 49% of those polled stated that their organizations were protecting their data more vigorously due to a previous data breach or due to lessons learned from their competitors.⁹

"Targeting employees with intimate knowledge of an organization's supply chain or planting TCO members into a company are attractive options for carrying out illicit operations."

According to the Vormetric poll, Mexico-based organizations have reported that the most dangerous insider threats usually are 'privileged users,' or those employees who have increased permissions and oversight over daily operations and are often responsible for managing data and services.¹⁰ In terms of supply chain, privileged users are likely to know loading and shipping timetables, intended routes and trade compliance and procedures.

Therefore, to a TCO with constantly evolving tactics and interests, targeting employees with intimate knowledge of an organization's supply chain or planting TCO members into a company are attractive options for carrying out illicit operations.

In two private sector partners' experiences, corporate restructuring was attributed for an increase in insider threat cases, as employees who were leaving the companies were more liable to betray the company.^{11,12} In another example, a private sector partner indicated that outsourcing of their supply chain contributed to their difficulties in combating insider threats. In this instance, limitations in dealing with third party affiliates for supply chain resulted in less control and restricted hiring practices over supply chain employees (Company A).¹³ In order to mitigate these

⁷ FreightWatch International, comp. *FreightWatch International Intelligence Report Cargo Theft-Mexico*. Issue brief no. Q1-2015. FreightWatch International, 2015. Web. 2016.

⁸ Company A. "Supply Chain Risks for Technology Industry." Personal interview. 23 May 2016.

⁹ 2015 Vormetric Insider Threat Report /Mexico And Brazil Edition. *TRENDS AND FUTURE DIRECTIONS IN DATA SECURITY*. Vormetric.com. Vormetric Data Security, 2015. Web. 2016.

¹⁰ Ibid.

¹¹ Company B. "Supply Chain Risks for Beverage Industry." Telephone interview. 25 May 2016.

¹² Company F. "Supply Chain Risks for Logistics Industry." Telephone interview. 16 June 2016.

¹³ Company A. "Supply Chain Risks for Technology Industry." Personal interview. 23 May 2016.

risks, one private sector company decided to conduct periodic 'lifestyle checks' to assess whether privileged users were susceptible to bribery by TCO's, or who seemed to be living above their means.¹⁴

Another major TCO threat to private sector supply chains are the physical security risks along overland shipping routes. Annual reports by Freight Watch International (FWI) indicate that there remains a severe risk of TCO's targeting cargo vehicles along Mexico's highways. In the first quarter of 2015, FWI reported that 58% of cargo thefts occurred during the loading stage of freight transport, while the majority of other incidents occurred in-transit.^{15,16} Furthermore, in 2015 hijacking was the most common cargo theft tactic, followed by theft from trailers and then warehouse burglaries.¹⁷

For two private sector companies, drivers of shipping vehicles were the most at risk; suffering hijackings and armed robberies on several occasions.^{18,19} To combat this trend, Company F implemented anti-intrusion technology in cargo vehicles which has proven effective for maintaining physical security. These anti-intrusion measures consisted of video surveillance of the inside of the vehicle, and live monitoring of the vehicle from an outside company along with remote shut-off capabilities. These security enhancements are also advertised on the vehicle itself to deter criminals.²⁰ Meanwhile, Company E sought assistance from the Mexican government and local authorities in order to request increased security measures in high risk areas.²¹ Another private sector partner, Company B, also discussed their mitigation techniques for physical security risks along Mexico's highways, discovering that both overt and low-profile security postures have yielded success in decreasing security incidents on the road.²² Company H required an armed motorcade consisting of at least two drivers in the primary vehicle as well as a chase security vehicle with armed officers. This allowed them to have at least one driver in the primary vehicle at all times. Furthermore, Company H was only allowed to make stops at authorized locations, while keeping in contact with the command center at all times.²³ Instead of

¹⁴ Ibid.

¹⁵ FreightWatch International, comp. *Supply Chain Intelligence Center: Mexico Cargo Theft Q1-2014* (January-March). Issue brief no. Q1-2014. FreightWatch International, 2014. Web. 2016.

¹⁶ FreightWatch International, comp. *FreightWatch International Intelligence Report Cargo Theft-Mexico*. Issue brief no. Q1-2015. FreightWatch International, 2015. Web. 2016.

¹⁷ Ibid.

¹⁸ Company E. "Supply Chain Risks for Automotive Industry." Personal interview. 19 July 2016.

¹⁹ Company F. "Supply Chain Risks for Logistics Industry." Telephone interview. 16 June 2016.

²⁰ Ibid.

²¹ Company E. "Supply Chain Risks for Automotive Industry." Personal interview. 19 July 2016.

²² Company B. "Supply Chain Risks for Beverage Industry." Telephone interview. 25 May 2016.

²³ Company H. "Supply Chain Risks for Technology and Entertainment Industry." Interview. 22 June 2016.

completely mitigating the risk though, these extraordinary measures may have driven TCO's to target other cities and carriers.²⁴

Figure 1

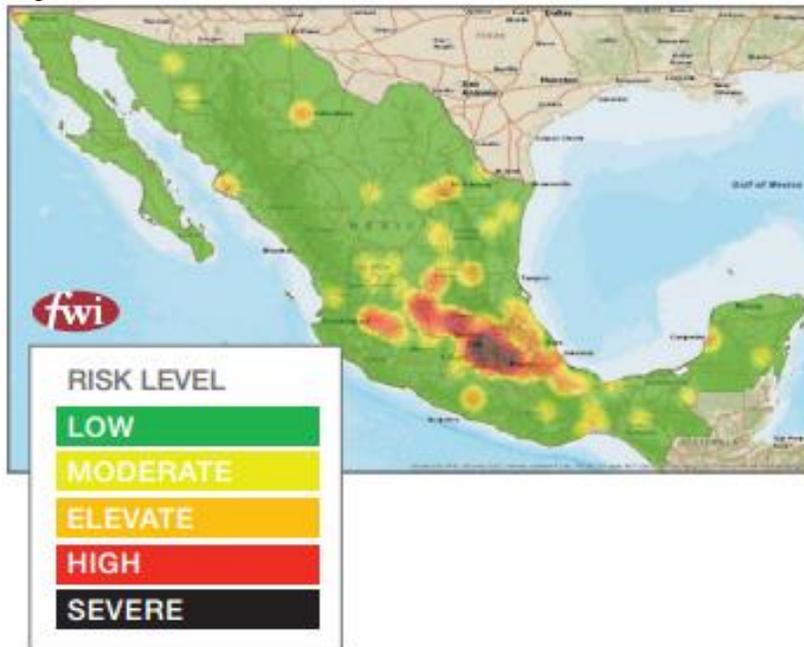


Figure 1 illustrates the risk levels from Low to Severe in Mexico's different highway zones

Another vulnerability identified among several companies was the outsourcing of supply chains. While outsourcing portions of supply chains is important for the competitiveness and efficiency of many companies, it does present the prospect of increased risk and exposure to their operations.²⁵²⁶²⁷²⁸ Outsourced portions of a supply chain afford a company less control and accountability for the implementation of security requirements. Some companies that were interviewed have implemented periodic review processes (including physical audits) of their supply chain vendors to validate implementation and consistent execution of security requirements. In addition, certification in industry and government-sponsored supply chain and trade programs has helped fortify the rigor and discipline necessary to assure that strong security measures are implemented throughout a supply chain.

²⁴ (Figure 1) FreightWatch International, comp. *FreightWatch International Intelligence Report Cargo Theft-Mexico*. Issue brief no. Q1-2015. FreightWatch International, 2015. Web. 2016.

²⁵ Company A. "Supply Chain Risks for Technology Industry." Personal interview. 23 May 2016.

²⁶ Company B. "Supply Chain Risks for Beverage Industry." Telephone interview. 25 May 2016.

²⁷ Company D. "Supply Chain Risks for Food Industry." Telephone interview. 26 May 2016.

²⁸ Company E. "Supply Chain Risks for Automotive Industry." Personal interview. 19 July 2016.

How Type of Industry and Products Determines Companies' Mitigation Techniques

The impact of TCO's on the private sector is not uniform across all industries, or even companies in an industry with similar products. In addition to proactive and reactive security measures by companies, the size, products, and value of a company's products help determine the likelihood a company is targeted. A number of strategies have worked well based on discussions with companies operating in Mexico:

- Companies that supply high volume, low cost products from Mexico to the US have been able to mitigate TCO risk by increasing the speed of their supply chain and consolidating products in US based distribution centers before determining their final destinations in the US.
- Companies that move high value goods through Mexico should look into investing in security escorts, as well as cargo proofing. Internet-connected devices offer the possibility to monitor access and block stolen products.
- Companies that supply short term consumables or non-uniquely identifiable products should attempt to reduce the ability of TCO's to steal products in transit. Goods, such as produce, are easily resold for near their full value. Decreasing and tracking the number and time of stops while goods are in transit can help reduce theft and ascertain higher risk zones.

Private Sector 'Lessons Learned'

In addition to mitigation techniques which are dependent on scope of industry operations and products, we found that the following general practices helped private sector companies combat TCO threats originating in Mexico:

- More self-regulation within the corporate sector proved as an effective measure against criminal elements. This includes maintaining authorized economic operator (AEO) certification compliance, particularly for companies operating at the global level.
 - Additionally, enforcement of good trade security practices through government-led monitoring of AEO programs and controls.
- Increased regulation requirements at the local level.
- Implementing proactive measures to prevent a problem rather than doing damage control after the fact.
- Scrutinizing the entire supply chain, including where raw materials are extracted.

- Choosing to work with a distributor that has a reach in every major market in Latin America but with a US-based headquarters for better accountability.²⁹
- Choosing to sell products online only in certain high risk areas instead of traditional outlets like kiosks and shopping malls.³⁰
- Leveraging the existing supply chain by using track and trace authentication labels on products and allowing the distributors and customer to authenticate products and actively report instances of counterfeits.³¹
- Closing down or re-locating higher risk factories and requiring strict travel protocols for employees and senior executives.³²

Cross Collaboration

Cross collaboration between private and public sector entities is pivotal for addressing the vulnerabilities and criminal risks threatening supply chains. Several of the companies and government agencies contributing to this project cited collaboration with the government, other industries or competitors as crucial methods for securing supply chain operations. For example, one effective partnership program that includes alliances with governments (especially Customs authorities) is the Business Alliance for Secure Commerce (BASC). The BASC's focus is on ensuring the integrity of shipments and preventing the introduction of contraband including narcotics, weapons, and migrants.³³

Additionally, authorized economic operator (AEO) programs such as Customs-Trade Partnership against Terrorism (C-TPAT) in the United States and Nuevo Esquema de Empresas Certificadas (NEEC) in Mexico provide companies the opportunity to get their supply chain operations certified by implementing increased security measures. In return, they receive benefits including fast lane treatment for imports and exports, reduced customs and border inspections, and an assigned account manager or security specialist.³⁴

Although collaboration with US government programs was common across our private sector interviews, most companies indicated that their dialogue with the Mexican government is limited. Hesitation in working with Mexican security forces and officials were based on concerns about corruption and Mexico's capabilities to actually provide assistance. For example, companies A, F and I work with the Mexican government as much as their legal departments will allow.³⁵ Company D has not engaged with the Mexican government due to concerns that a

²⁹ Company I. "Supply Chain Risks for Manufacturing Industry." Interview. 22 June 2016.

³⁰ Ibid.

³¹ Ibid.

³² Company H. "Supply Chain Risks for Technology and Entertainment Industry." Interview. 22 June 2016.

³³ "BASC News." BASC. World BASC Organization, 2005. Web. 2016. <<http://www.wbasco.org/index-eng.htm>>.

³⁴ Agency A. "Supply Chain Risks at US Port." Personal interview. 24 May 2016.

³⁵ Company A. "Supply Chain Risks for Technology Industry." Personal interview. 23 May 2016.

problem could become “out of their control”.³⁸ Meanwhile, Company E has reported issues to Mexican security forces, although their support varies based upon their deployment to other high-risk areas. Furthermore, this company indicated cooperation with Mexican government officials at the state and national levels as a joint security effort with representatives in their industry.³⁹

Private sector companies also indicated that success in benchmarking has included banding together with competitors. When faced with criminal threats that impact multiple industries, companies report that it is important and mutually beneficial to cooperate and share best practices. In the area of enhanced security measures, there is value in learning from the experience of others rather than trying to develop and implement unique solutions. This has provided benefits, particularly in addressing the counterfeit product market for Company I, as perpetrators are likely to counterfeit products of multiple brands. Sharing information regarding counterfeit manufacturers, distributors and sellers with other companies in the same industry and even pursuing legal actions has resulted in eliminating or reducing repeat offenders. Similarly, Agency C indicated that fusion centers in the US have sought collaboration with private sector industry liaisons. These liaisons are usually mid-level managers who represent their regional industry, including their competitors, in the interest of security.⁴⁰

Conclusion

Best Practices & Recommendations

It is impossible to ascertain to what extent TCO non-drug crime supports the drug trade and TCO efforts to move drugs into the United States. However, it is likely that as the public and private sector reduces the ability of TCO’s to move drugs through supply chains; non-drug crime will further grow as a percentage of TCO earnings, and thereby become more important to the continued existence and functioning of these criminal groups. TCO’s operate throughout Mexico, and are the primary threat to business activity and multinational supply chains in the country. TCO operations have led to heightened insecurity across a majority of Mexican states, and many groups are rapidly diversifying their activities, extending into illegal mining, illegal logging, reselling pirated goods, and extortion.

Further meetings between private and public sector counterparts should focus on the identification of risks, weak points in supply chains, and how changes in policies or private sector efforts change the operating environment. In addition, closer US-Mexican collaboration on

³⁶ Company F. "Supply Chain Risks for Logistics Industry." Telephone interview. 16 June 2016.

³⁷ Company I. "Supply Chain Risks for Manufacturing Industry." Interview. 22 June 2016.

³⁸ Company D. "Supply Chain Risks for Food Industry." Telephone interview. 26 May 2016.

³⁹ Company E. "Supply Chain Risks for Automotive Industry." Personal interview. 19 July 2016.

⁴⁰ Agency C. "Supply Chain Risks at US Fusion Center." Personal interview. 25 May 2016.

TCO involvement in non-drug crime could offset the risks to US companies that rely on supply chains in Mexico or across the US-Mexican border.

Communication and collaboration between the government and private sector are improving; however, further efforts at information sharing are necessary to combat evolving TCO tactics, techniques and procedures. Nevertheless, private and public sector partners should consider that the objectives of these two sectors do not always naturally overlap. An ongoing challenge is the potential for misunderstanding by both sides. Successful intelligence sharing is only possible if both sectors have a clear understanding of their counterpart's key operations and activities. Although protection of proprietary, sensitive, or classified information by both the private and government sectors remains a priority, increased transparency among trusted partners would contribute to a common working knowledge from which further best practices can be gleaned. Finally, further awareness and participation in government-private sector 'partnership' programs, as demonstrated by this DHS Analytical Exchange project, will benefit all stakeholders engaged in operating secure supply chains.

All judgments and assessments are solely based on unclassified sources and are the product of joint public and USG efforts.