Vast Exposure of Supply Chain Risk

Managing the supply chain means managing risk. Enterprises can’t do one without experiencing the other in today’s global world.

BY LARA L. SOWINSKI, JOHN R. YUVAAMY WUNDERLIN — MARCH 27, 2019

GETTY IMAGES

Remember the days when counterfeit goods and single-source suppliers were top of mind? While still part of the overall risk portfolio, it's now about data integrity, political/government agendas, trade agreements, natural disasters and more. What all these risks have in common is their global positioning and impact on external forces beyond a company's control.

In this article, the *Supply & Demand Chain Executive* editorial team examines three areas of supply chain risk, their potential impact and mitigation strategies.

- International trade compliance
- Geopolitical disruptions
- Cybersecurity exposure

Cost of Non-Compliance in International Trade

In Latin, it's Ignorantia juris non excusat, or simply put, there's no excuse for ignorance of the law. One U.S. importer, ELF Cosmetics, was hit with a $996,080 penalty earlier this year for violating sanctions on North Korea by importing false eyelashes from two Chinese suppliers whose products contained materials sourced from North Korea.

This move by the Treasury Department's Office of Foreign Assets Control (OFAC) illustrates the aggressive response and costly penalties that await importers who fail to comply with regulations designed to keep U.S. companies from trading goods and transacting for services with bad actors overseas.

In a document, OFAC stated that, “This action highlights the risks for companies that do not conduct full-spectrum supply chain due diligence when sourcing products from overseas, particularly in a region in which [North Korea], as well as other comprehensively sanctioned countries or regions, is known to export goods.” Therefore, “OFAC encourages companies to develop, implement and maintain a risk-based approach to sanctions compliance and to implement processes and procedures to identify and mitigate areas of risks.”

Sergio Retamal, CEO of Global4PL and DPLGuru, points out that the cost of non-compliance when it comes to vetting overseas suppliers and others with whom a company transacts business goes far beyond monetary fines and penalties.

For example, it’s not uncommon for a company that has been fined to experience additional scrutiny of their operations and shipments. Their legal costs are typically increased too, because they then have to devote more staff and/or resources to making sure the company remains compliant.

The government also evaluates whether a company is acting in good faith and had processes and procedures in place, or on the contrary, if the company was not even doing the minimal requirements with regards to knowing who the end user is (in the case of outbound shipments that originate in the U.S.) or who the seller, provider or vendor is in the case of imported goods/services.

In the case of ELF Cosmetics, “Among the aggravating factors cited by OFAC is that the company’s OFAC compliance program was either non-existent or inadequate,” noted trade law firm Sandler, Travis & Rosenberg. “Instead, the company’s production review efforts focused on quality assurance issues pertaining to the production process, raw materials, and end products of the goods it purchased and/or imported. In addition, the company appears to not have exercised sufficient supply chain due diligence, as its compliance program and supplier audits failed to discover that about 80 percent of the goods supplied by two of its China-based suppliers contained materials from North Korea.”

Nonetheless, “OFAC said the company’s cooperation and remedial measures were mitigating factors,” added the trade law firm. “In addition to immediately disclosing the apparent violation and terminating the conduct at issue, the company took a number of steps to prevent future violations. These include implementing supply chain audits that verify the country of origin of goods and services used in its products, newly requiring suppliers to certify that they will comply with all U.S. export controls and trade sanctions, and conducting enhanced supplier audit that included verification of payment information related to production materials and review of supplier bank statements. The company also expanded its efforts to train employees on U.S. sanctions regulations and other relevant U.S. laws and regulations.”

Geopolitics Gets Messy

Discussion around geopolitical risk has traditionally been low for many U.S. organizations. A series of tariffs imposed in January 2018 by President Donald Trump caught many companies off guard, thus sparking a new dialog around politically-motivated disruptions.

“Prior to our current president, I didn’t hear a lot about [concerns around geopolitical risk]. That was more of the fifth, sixth topic down the conversation,” says Mike Varney, a partner in the Crowe LLP risk consulting group He is responsible for leading the firm’s delivery of global risk services.

“That’s changed, specifically after last year and the impact the tariffs have had on organizations. Because it hit them directly in their pockets books, now you’re starting to hear it discussed more,” he adds.

Varney now ranks geopolitical risk in the Top 3 most pressing supply chain risks, along with regulatory and cybersecurity, and believes the trend will only continue to grow. He points specifically to a trend toward nationalism globally and China’s ambitions to become a world superpower.

“As you start to see this nationalism take stronger hold, it may create barriers in how you can move goods and source goods across borders,” he explains.

Take Brexit for example. A fear of immigration persuaded many British citizens to vote in favor of a break from the European Union in an effort to create more secure borders —a decision which the impacts on global trade are still unknown. The controversial vote was somewhat unexpected, and many companies are now working to prepare for the possibility of a No-deal Brexit ruling.

“They still don’t really know what’s going to happen once this settles, but trade deals are going to need to be renegotiated, which is likely to impact pricing and availability. Companies are already moving out of the UK, so there’s disruptions in the flow of goods…and there’s just that uneasiness that’s going around,” says Varney.

While countries such as the United States and the U.K. begin to take a closer look inward, the opposite is true for many companies’ supply chains. The globalization of suppliers and operations means a company is much more likely to be affected by a politically-motivated event around the world.

“If you look at what [manufacturers] have been doing for the last 15 or 20 years, they have been elongating their supply chains, moving to different regions of the world where traditionally they weren’t connected,” explains Bill DeMartino, general manager of RiskMethods North America. “Supply chains, in combination with the fact that

they're also trying to be lean and agile, have grown brittle. Thus, any force that would have historically impacted the organization is much more likely to affect the company and impact the brand or bottom line."

Approaching Geopolitical Risk

The tricky thing about geopolitical risk, however, is that it "tends to be farther reaching…and permeates to the supply chain on a quicker basis," says Varney. It's easy to think, for example, that a war in the Middle East will only affect the Middle East, but "as we've seen, it spreads across the globe," he adds.

It also can be difficult to predict. "There's many different ways that it will show itself," notes DeMartino, which he says means companies must really think about how those threats are going to manifest in their individual supply chain.

The first step is acknowledging that there is the possibility of a geopolitical event disrupting your supply chain. Once you acknowledge it, Varney says companies need to assess the environments in which they operate and then utilize a variety of tools to gauge the likelihood of said events.

"Risk is the what could go wrong; it's the unknown in the market. But using some of the tools available in the marketplace, following the press and being aware of issues that could occur can alleviate [potential risk]," he explains.

RiskMethods' supply chain risk management software is one such tool that can do that heavy lifting for companies. The company helps organizations create risk profiles for each supplier or partner in their supply chain based on a range of sources and continuously monitors that relationship.

"It is not the enterprise's job to figure out what the latest and greatest source of information is that it can leverage about its supply chain. That's really what our job is for them—to continuously look for and identify new sources of reliable information that we can leverage to bring continuous insights to our customers," says DeMartino.

Once you've acknowledged the possibility of a geopolitical disruption and evaluated the regulatory environments of your operations, the final step is asking the "what if" questions. Question such as: What if a regulatory or a regime changes materially? How will it impact our ability to move product to our facilities? What would be the cost if we were to continue the same movement of it? What if a sub-tier supplier is impacted? What if there is political unrest that occurs in a region that we're operating in? What if there's a change in the way things can be sourced, and how will that impact my supply chain?

Speaking specifically about the recent impact of the Trump Administration's tariffs, Varney says many of his clients were unprepared because they simply hadn't yet asked themselves, "If the tariff regime were to change materially, what would we do?"

Establish Your Mitigation Plan

Unfortunately, most companies are still not as prepared as they should be for a supply chain disruption, says DeMartino.

"Most organizations have business continuity plans in place, but those tend to focus on disaster situations—worst case scenarios," he adds. In the case of geopolitical risks, however, DeMartino says most are not long-term disasters. And those disaster recovery plans often lack the level of capabilities needed to react to more nuanced threats that are going to impact the supply chain.

For those companies that have not prepared for the impact of a sudden geopolitical event, Varney recommends a four-step mitigation plan: assess, strategize, implement and review.

"The first step is asking, "Do you understand the impact? Have you assessed what the impact is if you do nothing," he explains. Doing nothing is typically not the answer to the problem, he's quick to add, but it is important to understand the impact on a broad basis. Once you've done that, you can create an initial strategy with options to help mitigate the problem in the short term.

When handling the recent tariffs, for instance, Varney says his customers looked at such strategies as whether they could shift production out of China to another country they had operations, or whether they should keep production in China and raise prices for customers. One client that has operations in China and India was able to stop production in China and ramp up production in India with almost no impact to its operations.

The third phase is implementing that strategy.

Varney notes this is often a short-term solution that will be revised in the final stage of migration.

"The fourth phase is developing a continuous loop—come back, monitor, review and develop a more long-term play or make adjustments to address issues in the short-term solution."

An increasingly digital supply chain, however, means such decisions can now occur in real time. Varney says companies should be implementing processes and approaches long before a geopolitical event strikes to gain the supply chain visibility that can

prevent disruption.

Greater Exposure to Cybersecurity Risk

Every day companies exchange copious amounts of data with supply chain partners as a normal means of conducting business in a global marketplace. Simultaneously, cyber thieves are targeting company servers and IT systems to infiltrate, disrupt and paralyze their operations. What makes this scenario more disturbing is that companies lack supply chain transparency below the first tier. Often, lower-tier suppliers are third parties a company has never vetted nor has visibility into their operations. This poses a significant threat in thwarting cybersecurity incidents.

In its survey, Corporate IT Security Risks, Kaspersky Lab reports breaches of IT infrastructure hosted by a third party cost enterprises globally an average of $1.64 million per incident. If that doesn't raise a level of concern, it should.

Modernization Means Higher Risk

The modern supply chain functions on the accumulation and exchange of data processed by automation, artificial intelligence and Internet of Things (IoT)—all data-intensive processes capable of infiltration. What's more is that the data resides in a cloud-based repository.

Despite this vulnerability, phishing scams remain a primary means of breaching company and supply chain firewalls. Unsuspecting employees open a familiar but malicious email, unknowingly sharing personal and company information. Cybersecurity Ventures reports that since 2013, there are 3,809,448 records stolen from breaches every day. Do I have your attention now?

Cyber threats and their impact on companies and extended supply network are well documented—Marriott, Yahoo, Target Corporation. Nearly every industry segment, including retail, aerospace, banking and the like are victims of cyber events. The question is why are companies not better prepared?

According to a December 2018 report, Measuring and Managing the Cyber Risks to Business Operations, sponsored by Tenable and conducted by the Ponemon Institute, the following are reasons organizations are vulnerable to cyberattacks:

- Understaffed IT security function
- Lack of resources to manage vulnerabilities
- Proliferation of IoT devices in the workplace
- Complexity of the IT security infrastructure
- Lack of controls over third-party access to sensitive and confidential data
- Dependency on manual processes to respond to vulnerabilities

- Insufficient visibility into their organization's attack surface.

As companies globalize and extend their supply chain network, the number of data touchpoints increases as well—often without a company's knowledge. Sensitive data may reside on multiple servers around the world with entities a company is not aware of. A second-tier supplier, for example, may outsource services to an unknown third party with negligent cybersecurity protection and protocols.

Stewart Curley, chief financial officer for LookingGlass Cyber Solutions, says more than ever, there are multiple points of entry a cyber thief can exploit. Automation and collaborative tools are changing how companies function, but with the added risk of exposure.

"Companies are collaborating more and relying on best-of-breed third-party applications for everything from enterprise resource planning to human resource management to accounting systems. Collaborative applications such as Slack and SharePoint are now common in the workplace as well," says Curley. "Anytime you broaden your partner collaboration and number of people contributing to a project, there's the potential for risk gaps. With greater efficiency comes greater risk."

Does increased risk lead to assertive risk management enforcement? Not often. Curley says companies rely too heavily on contract language as a means of ensuring compliance to cyber security concerns. If it's in the contract, the responsibility lies with the supplier.

"You're only as strong as your weakest link. Taking the word of your partners that appropriate safeguards are in place is not nearly enough nor is relying on an insurance policy," says Curley. "There's a great deal of trust but no verification process. Cybersecurity must be addressed head-on. Compliance must go beyond checking the boxes and extend into verifying that policies are practiced."

Risk Mitigation Strategies

Most cyber attacks are not on the technological defenses of the company but against the employees themselves. G. Mark Hardy, CISSP, president of National Security Corporation, says technology is reliable. In a matchup, computer versus computer, it ends in a stalemate because neither can penetrate the other's defenses. The intrusion and safety systems would block them from a breach.

"Attacks succeed because people on the inside inadvertently are co-opted into the attack scenario through behavior. Thus, the best defense is security awareness training and follow-up testing to ensure compliance," says Hardy.

First and foremost, Hardy says companies must be proactive in their approach to risk mitigation. In the case of cybersecurity, it's imperative to ask for a supplier's risk framework, or even better, request a copy of the auditor's SOC 2 audit report to verify safeguards.

"Before we can establish trust, show me how you make informed, risk-based decisions. If I see that you take reasonable precautions, minimize unnecessary risk and prioritize security over functionality, there's a good chance you're going to be a safe provider," he says. "It's also never a bad idea to ask the supplier for the ability to conduct a team spot check or other form of visibility into its operations to maintain a level of assurance. A passing inspection today doesn't mean things could not decay over time."

A more formal process to ensure compliance is following a risk framework with known controls based on proven practices. Hardy says in Europe, for example, many companies rely on the International Standards Organization (ISO 27001) framework. In the U.S., the National Institute of Standards and Technology and its special publication (NIST SP) 800-53 outlines all the possible controls to reduce enterprise cyber risk.

"NIST provides numerous controls that serve as the framework, a shopping list, of the policies and practices to best protect enterprises against cyber threats," says Hardy. "While U.S companies rely much less on the ISO 27001 certification, it would serve them well to have this certification if they're doing business in Europe or Asia. It's an objective external standard that's been validated by auditors demonstrating a reduction of risk to a known set of control levels. Think of it as a Good Housekeeping Seal of Approval."

DPLGuru Helps Companies With Compliance

If you think U.S. companies involved in international trade generally have a good compliance record, the report from those in the field suggests otherwise.

Sergio Retamal, CEO of Global4PL and DPLGuru, remarks that there is plenty of room for improvement when it comes to compliance.

"Ninety percent of the companies that we work with don't have a record retention program that would pass an audit initiated by any of the federal agencies that are involved in overseeing international trade," he says. Moreover, 97 percent of those companies "don't understand that Denied Persons List (DPL) screening is the most basic step with regards to export compliance."