Scrutinizing Content for Greater Supply Chain Security

Scott Sangster
Tue, 2015-10-20 00:02

The global trading environment is in constant motion and exerting its influence on supply chains. Supply chain security is rising in importance, and companies across various industries need the right people, processes, technology and content to support security policies and compliance. Whom you're doing business with, whether you're complying with customs regulations, and your data security policies are key pieces of content in the supply chain security puzzle.

Whom Are You Doing Business With?

Companies have a legal obligation to ensure they do not conduct business with prohibited or restricted entities, corporations, countries, or persons. It's incredibly challenging to collect, maintain and update denied, restricted and sanctioned data from multiple global lists—some of which change hourly. Researching individual lists, determining which ones are relevant to the business, reviewing each on a case-by-case basis and using manual techniques or limited tools like Excel to screen are all far from efficient. Businesses today require much more sophisticated methodologies and technology-based solutions to lower risk and ensure compliance.

While there is no legal requirement in the U.S. to screen, there are legal consequences for conducting business with the wrong parties: $1 million in criminal penalties for willful violations on restricted items, prison for up to 20 years per violation, $11,000 in civil penalties, $250,000 in potential administrative penalties up to revocation of export privileges or debarment. Numerous exporters and intermediaries incur substantial fines every year for doing business with denied parties.

So who needs to be concerned? It's a long list: shippers, intermediaries and carriers, including forwarders and customs brokers in addition to exporters; manufacturers, suppliers and distributors for screening both internally and as goods are transported; financial institutions, including online banks, investment firms, payment processors as well as intermediaries; human resources and accounting for screening employees, vendors and subcontractors. And before you think that screening is only applicable for companies that transact business internationally, think again. At a minimum, all companies should screen customers, prospects, employees, vendors and suppliers.

Despite a genuine willingness among companies to screen, part of the challenge is in matching technology capabilities with risk parameters and business needs. For companies with a low volume of business transactions, a web-based solution for individual searches could work well. Those with a medium level of transactions need to review thousands of customers/prospects against a selected range of denied and restricted parties. Companies with a high volume of transactions could benefit from a solution that proactively scans master customer data every time a new entry is made in a denied party list.

Are You Complying with Customs Regulations?

Security activities also include screening and validating of the contents of goods being shipped. With the focus on global trade content intensifying, companies must do more to better manage data and improve overall levels of compliance for goods and security filings. This includes more accurate item classification and better research methods, collaborative trade content processes and validations, better management of changing regulations and global compliance trends, effective data use/reuse in company and partner systems, and a reduction in duplicate processes across countries and regions. Advance notification of contents to destination countries is another requirement, which is addressed by various legislation.

In today's extremely active regulatory environment, maintaining effective controls to ensure proper management of global trade content is more important than ever. Most import penalties for shippers arise from improper classification, valuation or country of origin determinations. Depending on the violation, U.S. import penalties may include up to 100% of the merchandise value or up to two years imprisonment for false classification.

Although global export control reforms have modernized classification and licensure, the changes have added complexity and increased the need for internal controls. For instance, today there are fewer restrictions and more dual-use goods worldwide compared to more restrictions in the past on exported technology. As well, today there are more frequent updates to restricted party lists than ever before.

Knowing the trends is only part of the equation. Companies must target inefficient compliance-related practices with technology-based alternatives that can help reduce risk and duty spend, increase visibility and achieve higher rates of trade compliance. To support global operations, multinational shippers, customs brokers, third-party logistics providers (3PLs), freight forwarders and multimodal carriers need comprehensive solutions to build and maintain complex classification databases of regulations, rulings, duties and more. Data resources must be updated rigorously and classification procedures refined regularly.

What About Your Data Security Policies?

As the mounting number of data breaches attest, cyber-crime is a critical threat of potentially exponential proportions. No industry is exempt from attack. Some of the largest and most high-profile breaches to date include Target, JPMorgan Chase, Anthem and Sony. According to a report from insurance firm Allianz, the financial toll of cyber-crime is estimated to reach $108 billion annually in the U.S. and to cost the global economy $445 billion annually. On top of the damages that data loss may cost a company, the cost to its reputation may be enough to end the business altogether.

With costs this staggering, data privacy and protection is an element of supply chain security that companies cannot afford to ignore. Data is the lifeblood of modern supply chains and ensuring its security is critical to business operations.

Increasing interconnectivity, globalization and the commercialization of cyber-crime are catalysts for both the frequency and severity of attacks. As supply chains move toward even greater collaboration and connectivity between parties, and comprise organizations with a progressively more global focus, managing the impact of these trends on data security will be vital.

In addition, supply chains are fueled more and more by real-time data to operate with greater efficiency, provide excellent customer service and save costs. Any disruption of supply chain processes, then, even for a few minutes, has the potential to spur a major business interruption and take a significant toll on the bottom

line. Data security is a balancing act for enterprises as they further integrate supply chain partners. While the knee-jerk reaction may be to severely restrict access, leading supply chain operators are focusing on modern technologies that drive deeper levels of security (e.g., encryption) but still facilitate collaboration.

As technology evolves on multiple fronts, older systems and devices may create vulnerabilities, especially when they rely on outdated operating systems and unsupported software. For legacy systems that are still supported, patching and staying up-to-date is essential. This is easier said than done with systems spread out across a wide geography.

Companies also need to use secure communication protocols when exchanging information with employees as well as third parties. While technology has no "silver bullet" for cyber security, modern systems and devices, more sophisticated monitoring tools, improved processes and greater employee awareness can all help companies in the supply chain to develop a robust security culture and reduce risk.

However, technology alone is not the solution. What may be more difficult to engineer is the cooperation required across the enormous range of supply chain partners worldwide—shippers, intermediaries, carriers, ports and government agencies—to achieve the secure and timely exchange of all of the content needed to drive the global supply chain.

Scott Sangster is the vice president, Global Logistics Network at Descartes.