SICPA

ZURICH

Risk Nexus

Supply chain integrity: executive summary

Most companies are exposed to supply chain risk. Often problems affecting supply chains are accidental, like the result of a fire at a supplier's plant, or due to a natural catastrophe. But when a supply chain is affected by fraud, such as deliberate tampering or the production of counterfeits, the risks quickly become much more complex: injury or even death can result. Compromised supply chains can destroy a carefully-cultivated brand, hurt trust, hit profits and land senior executives in jail.

Zurich Insurance Group and SICPA, a Switzerland-based company specializing in global security solutions, believe companies can increase their ability to safeguard against deliberate supply-chain 'infiltration,' such as that caused by counterfeit or tampered products. In a detailed study, they offer numerous recommendations and examples gathered in interviews with government and industry experts, enforcement specialists, risk managers and executives at large corporations.

Greed often the motive

Greed is often a key motive behind supply chain infiltrations; perpetrators may want to make money with shoddy, defective or counterfeit products.

Supply chain infiltration can mean producing counterfeit goods that look like established brands but don't work like them or put unsuspecting consumers at risk – counterfeit medicines, for example, or even fire extinguishers. Zurich highlighted in an earlier Risk Nexus publication, 'Counterfeit products: new risks in global value chains,' that we are currently witnessing an 'arms race' pitting counterfeiters against brand owners. In fact, organized crime groups in some cases apply highly sophisticated methods to produce and distribute counterfeit or tampered products, contributing to the exceptional growth of this type of fraud over recent years.

One key vulnerability identified in this study arises from 'blind spots' in complex supply chains. The study also notes that problems may often be found in emerging markets: in China, for example, in 2008, several companies were found to be selling dairy products containing melamine, an industrial chemical. The products included milk and infant formula, which were not only consumed locally but sold abroad, too. The usual analytical tests don't spot melamine, which can make milk appear to have a higher protein content. It can also cause kidney failure, resulting in death. The adulteration was possible using an astonishing level of technical sophistication. The sophistication was at such a high level that, if it had not been for a mass poisoning due to the use of melamine, no one likely would have noticed that the milk was watered down and the apparent protein content 'boosted' by adding the chemical.

While problems affecting parts of the supply chain are often associated with developing countries, they can also affect markets in places where people accept food safety as a given. The study cites, for example, a well-publicized case in Western Europe involving companies, some whose brands are household names, which bought beef from trusted suppliers. These companies were unaware that their meat suppliers had switched from producing the meat in-house, and were now sourcing it from third-parties. Some of the so-called 'beef' supplied by these sub-suppliers turned out to be horsemeat.

When criminals are involved in such activities, they often operate boldly. Often such crimes are so sophisticated that detecting them and determining their extent requires expert assistance.

Keeping abreast of complex supply chain risks

To counter these risks, the study recommends that companies map their supply chain from the level of raw materials all the way through to the end-consumer and analyze the related risk exposures in detail. Zeroing in on the flow of intermediate and finished products in the supply chain, companies should also examine their product security strategy. Analyzing 'blind spots' in the supply chain helps to develop strategies to increase the resilience of a company in the event that an infiltration incident occurs. The study offers a set of points of focus, areas that companies can include in tailoring a supply-chain risk strategy best suited to their individual needs.

Supply chain visibility requires mapping a company's network to really know who a company's suppliers and distributors are, and how supply streams create critical risk exposures and interdependences. This process also assumes that top executives are in charge of global strategic risk management. Advanced data analytics, or 'big data' can be used to visualize key delivery routes, simplify distribution networks, and enhance supply chain security by simplifying product traceability and recalls.

Managing 'traditional' supply chain risk exposures is also part of the process. Standard ways to do this include looking for weak points, such as placing too much reliance on a single supplier. Once all suppliers and sub-suppliers have been identified, these need to be monitored, and binding standards have to be enforced – in these efforts, some companies work with external companies specialized in fraud detection and protecting against such risks.

Risks in the logistics chain also need to be addressed: logistics hubs increase risk exposures. This is especially true in free-trade zones, which may offer criminals easy inroads into supply chains. Some bodies are active in helping to mitigate these risks, which can also be associated with terrorists: the World Customs Organization (WCO) has adopted standards that include those aimed at increasing global supply chain security.

Protecting intellectual property rights in the relevant markets is required to take legal action against counterfeiters. However, especially small and medium-sized companies often fail to take the necessary precautions to protect intellectual property when doing international business.

Keeping close contact with consumers is another way to spot problems and learn where they might arise; customer hotlines, a dedicated email address and social media can help. Companies must also respond quickly and credibly when a problem arises. Especially when a problem puts consumers at risk, the way a supply chain crisis is handled could literally make or break a company.

Enhancing product and supply chain security

Measures to make companies more resilient to supply chain risk include taking a close look at all parts of a supply chain, doing a 'security threats analysis,' and increasing 'company-wide awareness.' It is crucial to select a security technology solution only after a holistic analysis of what is exactly at stake, which security threats should be addressed, and what the related constraints, direct costs and indirect costs are. Technology can be used to verify product authenticity and prevent tampering. Multiple security features can be included in an inspection strategy and can rely on a variety of different markers, which raises the level of security. Some security features can also help to trace products as they pass through regular supply chain events, and some help to track products at any given time; this can be applied to both intermediate and finished products. Other security features can attest to provenance in legal disputes.

Among the general considerations about security technologies, the study makes the case that investment in supply chain security can more than pay for itself, sometimes many times over. Companies also need to have a product security intelligence strategy, which includes surveillance, gathering information about criminal supply chain infiltrations, determining threats that need to be addressed, sharing information within a company, and collaborating with law enforcement authorities when infiltrations are detected. Compiling such information can also help authorities identify the source of supply-chain infiltration.

Beyond internal controls

Beyond engaging with a company's own internal resources, policymakers need to be educated regarding the risks of product counterfeiting and tampering and how the legal and regulatory frameworks can help to discourage them. Key public policy issues in this context include the need to protect intellectual property rights to foster innovation as a key economic driver, and above all, to ensure consumer health and safety.

Alliances and pooled services can help to combat supply chain infiltration. For example, the study notes that a Swiss-Chinese public-private organization holds regular meetings with Chinese authorities, moderated by the Swiss Federal Institute of Intellectual Property; members include industry associations and Swiss and Chinese companies. Specialized not-for profit organizations can provide members with services and work to detect and combat counterfeiting. One such example is React, based in the Netherlands. Another is the International AntiCounterfeiting Coalition in the U.S.

There is no absolute security for supply chains; there will always be weaknesses to exploit. Prevention is important, but any company can become a victim, at any time and in any place. To sum up, corporate resilience needs to extend to withstanding the shocks caused by criminals who infiltrate supply chains. The goal is for companies to become resilient, meaning they can absorb shocks, recover, and become operational again as soon as possible.

Disclaimer

This publication has been prepared by Zurich Insurance Company Ltd and SICPA S.A. and the opinions expressed therein are those of Zurich Insurance Company Ltd and SICPA S.A. as of the date of writing and are subject to change without notice.

This publication has been produced solely for informational purposes. The analysis contained and opinions expressed herein are based on numerous assumptions. Different assumptions could result in materially different conclusions. All information contained in this publication has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any of its subsidiaries (the 'Zurich Group') or SICPA S.A. as to their accuracy or completeness.

This publication is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Persons requiring advice should consult an independent adviser.

The Zurich Group and SICPA S.A. disclaim any and all liability whatsoever resulting from the use of or reliance upon this publication. Certain statements in this publication are forward- looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by other factors that could cause actual results, developments and plans and objectives to differ materially from those expressed or implied in the forward-looking statements.

The subject matter of this publication is also not tied to any specific insurance product nor will it ensure coverage under any insurance policy.

Zurich Insurance Company Ltd
Mythenquai 2
8002 Zurich
Switzerland

SICPA S.A.
Av. De Florissant 41
1008 Prilly
Switzerland