Risk Nexus
Supply chain integrity: protecting companies’ blind spots
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Foreword</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>Executive Summary</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Section 1: Blind spots in supply chains: the friend of fraudsters</strong></td>
<td>5</td>
</tr>
<tr>
<td>1.1. Recent high-profile cases</td>
<td>5</td>
</tr>
<tr>
<td>1.2. Supply chain infiltration: the threats of tampering and counterfeiting</td>
<td>6</td>
</tr>
<tr>
<td><strong>Section 2: Strategic ‘puzzle’ of measures to protect supply chain integrity</strong></td>
<td>8</td>
</tr>
<tr>
<td><strong>Section 3: Preparing the organization to deal with the complexity of supply chain risks</strong></td>
<td>11</td>
</tr>
<tr>
<td>3.1. Supply chain visibility: mapping a company’s network</td>
<td>11</td>
</tr>
<tr>
<td>3.2. Big data to support supply chain risk management</td>
<td>12</td>
</tr>
<tr>
<td>3.3. Managing ‘traditional’ supply chain risk exposures</td>
<td>12</td>
</tr>
<tr>
<td>3.4. Monitoring suppliers and enforcing binding standards</td>
<td>13</td>
</tr>
<tr>
<td>3.5. Managing the risks in the logistics chain</td>
<td>13</td>
</tr>
<tr>
<td>3.6. A corporate strategy to protect intellectual property rights</td>
<td>14</td>
</tr>
<tr>
<td>3.7. Consumer outreach</td>
<td>16</td>
</tr>
<tr>
<td><strong>Section 4: Supply chain transparency: approaches to enhance product and supply chain security</strong></td>
<td>17</td>
</tr>
<tr>
<td>4.1. Analyzing the supply chain security threats</td>
<td>17</td>
</tr>
<tr>
<td>4.2. Situational awareness across the company</td>
<td>18</td>
</tr>
<tr>
<td>4.3. Identification of products or carriers</td>
<td>19</td>
</tr>
<tr>
<td>4.4. Inspection strategies: multiple security features</td>
<td>21</td>
</tr>
<tr>
<td>4.5. Traceability and tracking of intermediate and final products</td>
<td>22</td>
</tr>
<tr>
<td>4.6. General considerations about security technologies</td>
<td>23</td>
</tr>
<tr>
<td>4.7. A product security intelligence strategy</td>
<td>24</td>
</tr>
<tr>
<td><strong>Section 5: ‘Outside-in’ activities</strong></td>
<td>28</td>
</tr>
<tr>
<td>5.1. Engaging in public policy to protect supply chains</td>
<td>29</td>
</tr>
<tr>
<td>5.2. Alliances and pooled services to combat supply chain infiltration</td>
<td>31</td>
</tr>
<tr>
<td><strong>Section 6: Conclusion: The goal is a resilient supply chain</strong></td>
<td>33</td>
</tr>
</tbody>
</table>
Globalization and technological progress have significantly contributed to overall economic growth over the last two decades. However, they have also created new vulnerabilities for companies. For example, many companies have taken advantage of outsourcing and contracting suppliers abroad to reduce their production costs and tap into new pools of skills and resources. As a consequence, supply chains have become longer and increasingly complex against the backdrop of a dynamically changing global risk landscape.

Recent scandals have revealed dangerous blind spots in complex supply chains. High-profile cases have shown that adulterated and counterfeit products can even pose deadly threats to consumers, and have disastrous consequences for companies. Worryingly, there is growing evidence that any company can become a victim of such criminal attacks against the quality and safety of products.

To succeed, a company must find an affordable way to balance the need to tap into business growth opportunities, while managing the related risks in its supply chain, both upstream to the level of raw materials and downstream to the level of the end consumer. However, our research for this study has shown that many companies’ supply chain risk management strategies still lack important elements.

In this Risk Nexus publication, we discuss the key elements of strategy that can help companies ensure the integrity of their supply chains. We also offer examples of best practices and insights from experts at SICPA, a company specialized in providing security, including to governments, on a worldwide basis, and Zurich. This study follows an earlier Risk Nexus publication that highlighted new risks raised by counterfeit products in global value chains. Zurich has also, together with the University of St. Gallen, conducted a business project under the CEMS Master’s in International Management program. As part of this project, students interviewed a dozen academic and industry experts; some of their insights are included in this publication.

Many services and solutions already exist to manage supply chain risks, such as risk engineering to assess exposures and develop appropriate risk management measures. Product security solutions can protect intermediate and finished products, and insurance solutions can transfer certain risks to insurers’ balance sheets. A successful risk management strategy for complex supply chains combines these and other strategic measures to form a complete and effective framework.

The stakes for companies are high: profits, consumer trust and brand reputation are at risk. We hope that this report helps you to identify the gaps in your current supply chain risk management strategy and benefit from ideas on how to best address these risks.
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.

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.”
Section 1
Blind spots in supply chains: the friend of fraudsters

Many of today’s complex supply chains include obscure parts. If someone succeeds in infiltrating a supply chain through these ‘blind spots,’ it can have devastating consequences.

1.1. Recent high-profile cases

In 2013, the European food industry was shaken by one of the largest meat adulteration1 scandals in history.2 The story was widely reported in the media and caused huge damage to companies supplying and producing convenience foods and frozen meat products.3 The scandal broke after DNA tests revealed that some meat products labeled as beef contained a considerable proportion (in some cases 100 percent) of undeclared horsemeat or pork. Blind spots in supply chains were at fault. It turned out that some meat suppliers did not tell food company clients that they had changed their business model and were only packaging or boning the meat. Thus, unbeknownst to the end-producers, the meat was suddenly being supplied by different providers than previously. Investigations revealed that the horsemeat sometimes took a complicated route through sub-suppliers across several countries, obscuring its origin, before it reached its ultimate destination. Financial gains were believed to be the main motivation behind the fraud. The scandal underscored the fact that food supply chains can easily be infiltrated. In the wake of the scandal, many food companies introduced measures to make their supply chains visible from end to end, or stepped up existing monitoring programs. Even so, experts believe food fraud worldwide is getting worse, given the large number of high-profile scandals that have been uncovered of late. Other recent examples include seizure of 100,000 tons of smuggled frozen meat in China that reportedly dated back to the 1970s, providing fake rice made of plastic resin and sweet potato, fraudulently substituting peanuts for walnuts, or using banned dyes in South African supermarket products.4

Opaque supply chains can also make it easier to manufacture and sell dangerous products, including, for example, counterfeit pesticides. In 2008, the European Crop Protection Association (ECPA) in its report ‘Counterfeit Pesticides Across Europe,’ listed a number of major infractions.5 One example was the ‘great Spanish pepper scandal’ of 2006, a case in which traces of an illegal pesticide originating in China turned up on fresh peppers from the Almería region in Spain. This incident gained a great deal of media attention, caused serious financial losses, damaged the reputation of Spanish agriculture and undermined public trust in its food safety record. According to the ECPA, counterfeit products account for around 10 percent of pesticides used in Europe, up to 20 percent of those used in Russia, the Ukraine and India, and up to 30 percent of pesticides used in China. There are indications that the trade in illegal and counterfeit plant protection products has increased in the EU in recent years, according to a study commissioned by the Directorate General Health and Food Safety of the European Commission.6 The authors of this study also assessed the existing regulatory framework in the EU and found that this framework is not entirely satisfactory.

1The adulteration of food or beverages refers to making a product impure or weaker by adding a foreign substance.
6Ad-hoc study on the trade of illegal and counterfeit pesticides in the EU (2015), see the Executive Summary at http://ec.europa.eu/food/plants/pesticides/docs/study_on_illegal_ppps_summary_en.pdf
One person with whom we spoke for this study, who requested anonymity, also noted that counterfeiters are finding new ways to enter targeted markets with counterfeit agrochemicals. In 2015, more than 100 tons of mislabeled crop protection chemicals were seized in Eastern Europe. Customs declarations were forged stating that the products were laminate flooring. Originating in China, the products were seized on their way to illegal factories in Eastern Europe where they were, before being confiscated, to have been turned into fake crop protection products. Having traced the distributor’s agents, authorities performed raids on more than seven locations, including warehouses and illegal factories. The raids revealed repacking equipment such as fake labels and bottles with the look and feel of the brand owner’s products, and machines used to repackage the products. As this report was being written, court hearings were still going on against the individuals in this case.

1.2. Supply chain infiltration: the threats of tampering and counterfeiting

Such examples demonstrate that supply chain vulnerability creates safety risks for consumers and poses threats to companies’ reputation and profits. Typical forms of supply chain infiltration are counterfeiting – using the name of a brand without the brand owners’ permission – and tampering – that is, changing the composition of a product by adding a foreign substance. The term counterfeiting is sometimes also used for other infringements, such as patent violation, or using a design without permission.

Revenue, brand reputation and consumer trust at stake

There are many reasons why companies should worry about their exposure to supply chain infiltrations. For example, counterfeit products sold in the market might dramatically hurt sales.7 Flawed or sub-standard products could potentially lead to financial losses and business interruptions. The worst-case scenario, however, is when the health or the lives of consumers are put at risk. Complicated liability questions can also arise if customers suffer bodily injury or property damage due to tampered or counterfeit products. Such events can culminate in costly product recalls and legal cases. They can damage brand reputation. And the loss of consumer trust after a major tampering or counterfeiting incident can be devastating.

7 For an assessment of the economic impact of counterfeiting and piracy in different industry sectors, see the website of the European Observatory on infringements of Intellectual Property Rights, https://oami.europa.eu/ohimportal/en/webobservatory/quantification-of-ipr-infringement
Counterfeit products: new risks in global value chains

In Zurich’s Risk Nexus report, ‘Counterfeit products: new risks in global value chains’ published in 2014, Zurich highlighted the fact that counterfeiters are conducting a highly profitable illicit business by infiltrating global value chains in all industry sectors. The considerable growth of this type of crime over the last two decades has been made easier by the increasing availability of advanced production and packaging technologies, online sales channels, trade globalization, and the involvement of well-organized transnational organized crime groups. When analyzing companies’ awareness of the problem, our biggest surprises included learning that many companies of all sizes significantly underestimate their risk of becoming a victim. Counterfeiting today affects not only major brands, but increasingly also smaller ones. Our 2014 report also notes that today all industries – not just those producing luxury goods, for example – can be targets of counterfeiting. Consumer safety can be threatened by a range of counterfeit products, including electrical and electronics goods, consumer and healthcare products, agrochemicals and automotive parts. Among the most shocking examples are probably counterfeit safety devices such as fire sprinklers or fire extinguishers that are likely to malfunction. It is reasonable to assume that the publicly known, big counterfeiting and tampering scandals are only the tip of the iceberg of all supply chain infiltrations that happen around the world.

The majority of companies that do business globally suffer from lack of supply chain visibility and in most infiltrations, perpetrators exploit this. The 2014 edition of an annual survey conducted by the Business Continuity Institute found that roughly three-fourths of 525 companies interviewed, based in 71 countries, lacked full supply chain transparency, and only about a quarter coordinated and reported supply chain disruptions enterprise-wide.

In short, many companies have dangerous blind spots and need to better protect themselves against tampering and counterfeiting, since such incidents – when consumer safety, brand reputation and consumer trust are at stake – ultimately pose a threat to companies’ very existence.

Section 2
Strategic ‘puzzle’ of measures to protect supply chain integrity

Managing a global supply chain is already a challenging task per se. Supply from different production sites must be coordinated to satisfy unpredictable market demand. This requires good organization, plus a network of suppliers. Even without malicious interference, cases of severe unforeseen business interruptions and other disturbances have been well-documented. The dynamic nature of global risk requires companies to constantly revise and adapt supply chain risk management strategies. The risk landscape in which supply chains operate is increasingly interconnected and complex as new technologies come into play, crises of different natures including economic unfold, and extreme weather disrupts businesses across entire regions.

Figure 1: A simplified illustration of the network of a company with suppliers and sub-suppliers on the left and distributors on the right delivering the company’s products to consumers. Highlighted in black are some attempts to infiltrate this supply chain: a sub-supplier is providing a supplier with an illicit intermediate product, and a distributor, in turn, is delivering a finished product from an obscure source, indicated by a question mark, directly to consumers, for example through an online shop, and also to a distributor which then delivers it to consumers.

The job of risk managers and company executives becomes even more complicated when malevolent actors enter the picture. These individuals or organizations might try to compromise supply chain security as illustrated in Figure 1 by exploiting some legal, operational or technical weakness. What can a company do? In Section 6 of our previous study, Risk Nexus ‘Counterfeit products: new risks in global value chains’ we provided a list of recommendations to help regulators, governments and companies combat counterfeiting.

In this publication we are proposing a strategic approach – one that will help companies protect the integrity of their supply chains from both ‘traditional’ and ‘non-traditional’ risks, including infiltrations. All supply chain risk exposures can be managed through the usual process: risk identification, risk prevention, risk mitigation, risk transfer, and acceptance of the remaining risk.

A strategy to counter complex problems like threats to supply chain integrity requires a certain degree of sophistication, as illustrated in Figure 2 with a tangram. We envision here the strategy as resembling a dissection (or ‘transformation’) puzzle, consisting of pieces, which every company assembles to suit its individual needs. We group these pieces into three main objectives:

1. **Measures to keep abreast of the complex nature of supply chain risks**
   - Supply chain visibility: mapping a company’s network
   - Big data to support supply chain risk management
   - Managing ‘traditional’ supply chain risk exposures
   - Monitoring suppliers and enforcing binding standards
   - Managing the risks in the logistics chain
   - A corporate strategy to protect intellectual property rights
   - Consumer outreach

2. **Enhancing product and supply chain security**
   - Analyzing the supply chain security threats
   - Situational awareness across the company
   - Identification of products or carriers
   - Inspection strategies: leveraging the stacking of multiple security features
   - Traceability and tracking of intermediate and final products
   - General considerations about security technologies
   - A product security intelligence strategy

3. **‘Outside-in’ activities**
   - Public policy engagements to effectively protect supply chains
   - Alliances and pooled services to combat supply chain infiltrations

In the following sections we discuss some typical challenges companies need to overcome to increase supply chain resilience, and provide a number of examples of best practice and case studies illustrating ways to counter threats, address security gaps and ways that work to mitigate risks.
Figure 2: Illustration of the concept that from a set of risk management elements (left side), every company assembles its bespoke strategy (right side) that best suits its needs, giving the desired weight to each element, as indicated by different shades of the same color.

Staying alive and well – a lesson from living organisms

Even if not consistent in all details, a complex supply chain resembles to some extent a living organism. Raw materials, intermediate products and finished products flow from site to site in a fashion similar to a metabolic process, and are transformed.

Similar to the ‘puzzle-pieces’ approach proposed for companies in this publication, human beings also, over time build their own set of risk management strategies to stay alive and well, and adapt it on an ongoing basis to their individual situation. When using the human example as an analogy for supply chain risk management, we decide what we eat and drink and what we do not touch, and our sensory organs help us make these decisions based on physical and chemical measurements, rather than pure speculation, as we see, feel, smell and taste. We exercise, learn and adapt to the external challenges posed by our environment. Our immune system recognizes pathogens and other intruders in our body and neutralizes them. We vaccinate ourselves to be ready to quickly defeat particularly dangerous pathogens. The patellar reflex helps us to support a sudden load on our legs and not collapse, and its ‘local’ reflex arc bypasses the brain and involves only the spinal cord, ensuring a very fast reaction. More complicated risk management activities, such as running away from a life-threatening situation, require ‘global’ coordination steered by the brain as the central decision-maker. Foreign organisms in our intestinal track, like bacteria, provide chemical processes which our body cannot deliver on its own and thus enhance our digestive process. The populations of microorganisms that inhabit the human body regulate themselves in a complicated balance, which prevents harmful bacteria from settling in this environment. We also directly shape our environment with our hands and with tools, for example, by cleaning it to ensure hygiene and to prevent contamination. And last but not least, rules and norms of behavior can successfully extend the benefits of hygiene to an entire community.

13 We thank ManMohan S. Sodhi, professor at Cass Business School, and Otto Kocsis at Zurich for their ideas and discussions they had with us on this topic.
Section 3
Preparing the organization to deal with the complexity of supply chain risks

3.1. Supply chain visibility: mapping a company’s network

The first requirement for supply chain integrity is visibility. It is important that companies know who their suppliers and distributors are, where they are located, and which risk exposures they might contribute to.

To address strategic risks, it helps to understand the company and its supply chain as a network, that is, beyond simply a collection of individual sites. To achieve the full visibility of a supply chain, as shown in Figure 3, the company’s sites, its suppliers and its distributors are mapped and the interconnections of the network ‘nodes’ are drawn, where flows of goods, financial streams, and other aspects of the supply chain come together. This provides a useful basis to appreciate the ‘normal’ complexity a company must master when addressing the common challenges posed by interconnected and global risks. On an organizational level, top management needs to be in charge of a global strategic risk management approach that coordinates the local functions of the individual nodes as appropriate.

Figure 3: A company’s supply chain network, as depicted in Figure 1, with the addition of the company’s structure and main production sites, which may be located in different places.
The goal of a company should be to become resilient, that is, be able to recover after a shock such as a supply chain disruption, and return to operating at full capacity as soon as possible."

3.2. Big data to support supply chain risk management

Advanced data analytics promises more efficient management of supply chains. High-potential opportunities include, for example, visualizing delivery routes, pinpointing future demand, and simplifying distribution networks.14

At the same time, big data can also enhance the security of supply chains, for example, by simplifying product traceability and recalls.15

However, beefing supply chains up with big data capabilities requires a sizeable investment and also poses a strategic challenge to companies. A survey by Accenture in 2014 found that many companies experience difficulty when it comes to creating the necessary structure and deploying relevant capabilities.

Companies need to develop a strong enterprise-wide analytics strategy, use big data to improve decision-making across the entire organization, and hire people with the necessary analytics skills to use the data to make decisions.16 These general considerations apply in equal measure to risk management operations tied to this process.

3.3. Managing ‘traditional’ supply chain risk exposures

Establishing supply chain visibility from end to end, that is, starting upstream with raw materials extending all the way to end consumers, reveals a company’s ‘traditional’ risk exposures. Checklists such as the Supply Chain Healthcheck17 developed by Zurich’s supply chain insurance experts can help in their assessment. Traditional risks include supply chain disruption after the failure of a critical supplier, for example. A complicated supplier network architecture can also hide critical sub-suppliers further upstream, so that, for example, the failure of a particular sub-supplier would interrupt several supply lines that do not seem interdependent (at least, at first glance).

The suppliers’ exposures to politically or economically unstable regions and to natural catastrophes can be assessed once the geographical footprint of the supply chain is known.

To manage critical supplier risk, individual exposures need to be assessed, and business continuity plans analyzed in detail. Risks limited to a particular place, such as earthquakes or political instability, can be minimized by a purchasing strategy that includes other regions not exposed to the same risks. Critical suppliers’ financial stability should be measured in a routine and timely, systematic way. Business interruptions, contingent business interruptions, political risks, product liability and product recalls are typical examples of risks that a company can partially transfer to the balance sheets of insurance companies. The goal of a company should be to become resilient, that is, be able to recover after a shock such as a supply chain disruption, and return to operating at full capacity as soon as possible.

However, theory is not always easy to implement in reality. The pressure of reducing short term costs and increasing efficiency typically poses challenges to building a company’s capacity to improve its resilience. Zurich’s risk engineers have, for example, found that many companies still manage risks attached to individual production sites separately, not taking into account, for example, the fact that these sites are closely connected through the production process. Such companies can easily fall prey to cascading failures that disrupt the supply chain, for example, when a problem at a production site means a critical component will not be produced for some time. If there is no redundancy in the production process and no backup solution, global production must be halted due to a single, local failure. But business interruption risk can be addressed by following the advice of specialized risk engineers. This approach typically costs only a fraction of what a business interruption can cost a company.


17The Supply Chain Healthcheck can be found in: Protecting profitability if the chain breaks – Supply Chain Management, Zurich Risk Insight, 2009, see http://www.zurich.com/NAV/donlyres/5CD68EDC-CC77-4f57-AFDC-B72EFEED010/risk_insights_supply_chain_mgmt_200906.pdf
3.4. Monitoring suppliers and enforcing binding standards

Once a company has precisely identified suppliers and sub-suppliers, the main risks these face, and how a failure of one of these would affect its profits, managing supply chain risks is the next step. As part of this process, suppliers need to be monitored to get critical information, including information about their financial situation. It may also include reviewing suppliers’ legal records to determine if they have ever been sued for intellectual property right infringement.

Companies should establish and enforce a framework of binding standards for suppliers. One excellent example of this is Nestlé’s supplier code, which ensures responsible sourcing in its activities worldwide. This code was approved by the company’s executive board in December 2013; it defines the non-negotiable minimum standards for Nestlé’s suppliers and sub-suppliers which must be met when conducting business with Nestlé. The four pillars of the code are human rights, safety and health, environmental sustainability, and business integrity. There are also additional mandatory requirements outlined in an appendix. To enforce these standards, Nestlé audits its 10,000 ‘tier-1’ suppliers. In 2014, 8,700 tier-1 suppliers were reviewed for the first time in this program, and 73 percent were found fully compliant with the supplier code.

Many companies also work with specialized fraud detection and protection companies to audit their suppliers: Société Générale de Surveillance (SGS) provides testing, inspection, certification and verification on a worldwide scale; Lloyd’s Register (LRQA) also provides independent business assurance services, including management system certification, validation, verification and training. There are also smaller, more specialized inspection companies: Inscatech for example, is specialized in food sector fraud intelligence investigations, forensically-based vulnerability assessments, supplier qualification examinations, validated supply chain mapping, and food fraud vulnerability control programs.

3.5. Managing the risks in the logistics chain

Shipping is the backbone of global supply chains. But conveyance and logistics hubs provide more than just a connection between two supply chain nodes. They increase risk exposures, including to natural catastrophes. According to an anti-counterfeiting adviser quoted in a survey by PricewaterhouseCoopers (PwC) in the UK, brand owners see the lack of know-your-client precautions in the shipping industry as a key factor contributing to transport and delivery of counterfeit goods to the UK.

In 2005, the World Customs Organization (WCO) adopted the SAFE framework of standards to secure and facilitate global trade. It is designed to thwart international terrorism, provide increased security to the global supply chain, secure revenue collection and facilitate trade worldwide. The SAFE framework is widely accepted by the international community and represents a milestone in managing logistics-chain risks. Its three pillars are: customs-to-customs network arrangements; customs-to-business partnerships; and customs-to-other government agencies co-operation. A key part of the SAFE framework is the so-called ‘authorized economic operator’ (AEO), defined as “a party involved in the international movement of goods… that has been approved by or on behalf of a national Customs administration as complying with WCO or equivalent supply chain security standards.”
These may include “manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors and freight forwarders.” An operator can request AEO status if the following criteria are met: compliance with customs requirements; a satisfactory system for managing commercial records; financial viability; holds regular consultations on matters of mutual interest; provides education, training and awareness; complies with the need to exchange information, provides necessary access and confidentiality; cargo security; conveyance security; premises security; personnel security; trading partner security; crisis management and incident recovery; and measurement, analyses and improvement. Once an operator has been awarded AEO status, it can benefit for example, from faster cargo release, reduced transit time and lower storage costs. Several customs authorities have introduced AEO programs, including, for example, EU member states. A related program is run by the U.S. government, the Customs-Trade Partnership against Terrorism (C-TPAT). National AEO programs might be different from one another, but gradually, bilateral agreements are being signed, for example, between the U.S. and the EU in 2012, offering reciprocal recognition.

The challenges of free-trade zones
Free-trade zones, which can be exploited by criminals, have become hotspots for supply chain infiltrations. There are approximately 3,000 free-trade zones in 135 countries. Their special status within jurisdictions allows for duty-free imports and simplified administrative procedures, providing incentives to international trade and foreign direct investment. This significantly improves the conditions for international trade. However, the 2015 Situation Report on Counterfeiting in the EU emphasizes that free-trade zones can be abused by criminals; there is limited regulatory oversight in these areas, and authorities often fail to gain complete information about the business operations conducted there. There is evidence that organized crime groups use free-trade zones to transship, repackage and re-label illegal goods. Sometimes counterfeit trademarks are not added to the products before they have arrived at a free-trade zone, which makes them much more difficult to detect. Counterfeit products might even be manufactured entirely in free-trade zones. The 2015 Situation Report refers, for example, to the Jebel Ali Free Zone in the United Arab Emirates as one well-known hub that might be used to disguise counterfeit products’ primary origin. It also warns that developing and expanding free-trade zones and ports will provide significant new opportunities for criminals. These might include Tánger Med in Morocco, one of the largest ports in the Mediterranean and in Africa, located right on the EU’s doorstep.

3.6. A corporate strategy to protect intellectual property rights

Protecting intellectual property rights (‘IP rights’ or ‘IPR’) is an important step in combating counterfeiting. Based on our interviews with industry experts, many small and medium-sized enterprises (SMEs) involved in international business have thus far failed to sufficiently protect their IPR. Some of these companies do not even know that there are effective ways to facilitate this process. Simon Schmid, a legal adviser who is part of the Swiss Federal Institute of Intellectual Property’s international trade relations team, told us that many SMEs lack a corporate IP strategy, especially one that would apply to foreign markets.
“We receive quite a lot of IP-related requests from SMEs that do business abroad but are not aware of the work a company must do to register IP abroad and to protect and enforce it,” he said. To assist companies in fighting counterfeiting and piracy, the Institute conducts training sessions and workshops for companies in Switzerland as part of its ‘Stop Piracy’ platform.

Protecting and enforcing IPR requires internal and external resources. Many companies seek legal support from specialized organizations. In Section 5, we cover these ‘outside-in’ activities in detail. For general guidance, there is useful information available online providing suggestions on ways to protect IPR, including those provided, for example, by the US-China Business Council.

Detecting patent hijackers and making use of IPR enforcement databases

Permanently monitoring patent applications enables companies to detect attempts by others to ‘hijack’ one of their patents in a timely way. Patent hijacking is sometimes used by devious counterfeiters or imitators to protect illicit activities, as they register as the ‘patent owner’ in a certain market. So-called ‘patent trolls’, in turn, may seek to make money by just filing lawsuits, or threatening to do so, against the original patent owner for patent rights they have ‘hijacked.’ According to Silvia Volponi, business unit patent officer at ABB, digitizing and automating patent processes has meant major improvements for companies monitoring these activities, for example, at the State Intellectual Property Office in China. However, patent offices in countries like Brazil and India are not yet digitized, which poses a big problem for companies seeking to monitor patent applications in these big markets.

There are also developments underway to make IPR enforcement databases more accessible. This will help in exchanging knowledge and for enforcement activities. For example, the Office for Harmonization in the Internal Market (OHIM), which is the EU’s official trademarks and designs registration office, is providing a single point of contact for companies, industries and European authorities to protect against trademark and design counterfeiting. IP owners can register their products in OHIM’s enforcement database. Police and customs officers of EU member states can access this tool to view information and product details, making it easier for them to identify counterfeiters and take appropriate action. The World Customs Organization has also set up the Interface Public-Members (IPM) platform, available online, which allows rights holders to share relevant product information with customs authorities. IPM is the only global security solution gateway allowing customs officers to verify the authenticity of products online. Through this platform, customs officers around the world can better understand how registered products are protected against counterfeiting and illicit trade.

ABB’s Silvia Volponi underscored that data about litigation involving IP-related cases, and more operational data, would be very useful; but these are not easily accessible or available in all countries.

---

29 See http://www.stop-piracy.ch/
30 See, e.g., www.uschina.org/reports/best-practices-intellectual-property-protection-china
32 See the website at http://www.wcoipm.org/
3.7. Consumer outreach

Manufacturers’ consumer outreach programs can help to secure the last leg of the supply chain. It is important to increase the public’s awareness that counterfeit products exist in all product categories. The general public should also be warned against buying counterfeits, making it clear that these are bad for society, the economy and the environment. Producers can also provide guidance through consumer outreach activities, raising public awareness about how to identify counterfeits or products that might have been tampered with, and/or alerting the public if a series of such products has been detected in a certain region.

A customer complaints hotline, mailbox or social media feature can also be used to collect consumer feedback. This can help companies to get information directly when, for example, flawed products appear that require closer investigation.

Crisis communication can make or break a reputation

Should infiltration occur, swift and honest communication underscoring a collaborative approach and clear desire to resolve the incident to the benefit of consumers is crucial. Statements for some scenarios can, to some degree, be prepared in advance, and we recommend this approach.

How difficult crisis communication can become is highlighted by the example of Fonterra during the 2008 Chinese milk scandal, described in more detail in Section 6. Fonterra is a large New Zealand dairy cooperative responsible for almost one-third of the world’s dairy exports. Fonterra owned a 43 percent stake in one of the largest state-owned Chinese dairy companies, Sanlu Group. Sanlu was forced to recall more than 10,000 tons of infant formula after finding it was tainted with melamine, an industrial chemical. The company was declared bankrupt by local authorities. Several of its top managers received long prison sentences. After at first defending Fonterra, saying it tried to alert authorities but had been blocked by Sanlu and local Chinese officials, New Zealand’s prime minister publicly chastised the company for not issuing timely warnings about the contamination. The New Zealand Herald, in an editorial, stated that “…the wording of its press release, so far from creating an impression of a company keen to show leadership, suggested a desire to distance itself from the crisis.” As far as perception among the general public is concerned, efforts to mitigate the scope of a crisis can be overshadowed by negative publicity, if the communication strategy is not optimal.
Once a company has established end-to-end supply chain visibility, identified key risks, and prepared the organization to keep abreast of the complexity of supply chain risks, the next major step in the risk management strategy is to take security measures to ensure that only the right products end up with consumers.

Appropriate security solutions need to be integrated into daily operations for both finished and intermediate products. This step can be referred to as establishing supply chain transparency; it requires looking at the goods inside the supply chain network. This can immediately deter the least sophisticated forms of infiltrations: once perpetrators are aware that the basic weak spots are addressed, they may turn their attention to ‘easier’ victims, at least until these, too, tighten up weak points.

4.1. Analyzing the supply chain security threats

A holistic analysis of the security situation is the first step toward implementing supply chain transparency. This exercise starts with defining what exactly is at stake in the event of a security problem: sales, reputation, and/or consumer health? Then the company should identify all relevant types of threats to which the supply chain is exposed, as discussed in the next paragraph. As a third key component, all compliance requirements and constraints imposed by regulations, industry standards or quality labels that apply to a given product must be taken into consideration.

Different types of supply chain threats due to infiltrations and ‘re-routing’ can be identified, as shown in Figure 4. Counterfeit products have already been introduced earlier in this publication as a threat to supply chains. At the product level, counterfeit parts or components and tampering are also issues related to infiltrations affecting upstream and downstream supply chains.

Beyond infiltrations, supply chain ‘re-routing’ can pose other threats:

- Gray or parallel markets, either local or cross-border, can represent a significant threat. One typical example is product diversion, which means that products intended for a given geography or distribution channel, typically offered at lower prices according to the brand strategy, are diverted without consent of the brand owner, to higher-priced areas.

- Unauthorized production is another risk closely associated with the growing trend of outsourcing in global manufacturing operations. In unauthorized production, the fraudulent product is manufactured on the same manufacturing line as the genuine product, but without the consent of the brand owner.
4.2. Situational awareness across the company

Security begins with detailed analysis and preparation. In the context of supply chains, this means knowing the key vulnerabilities and monitoring all relevant operations and external developments. Building and maintaining a record of relevant infiltration incidents is also a helpful way to assess local risk situations. But this still falls short of what is needed. Those seeking to perpetrate supply chains are opportunistic, and should be expected to find and exploit weaknesses in existing structures, processes and frameworks. As is often the case, attackers have an advantage over defenders, and barriers are usually low. Any company can become a victim, at any time and in any place. Companies should focus on addressing the most accessible weaknesses and minimizing potential damage of supply chain infiltration. Weaknesses will always exist, but companies can do a lot to make it more difficult for criminals to exploit them.

Making everyone in the company aware of the threat of supply chain infiltrations also requires getting the message across despite what could be a protective, corporate ‘silo’ mentality and penetrating communication barriers that might exist between different business units. Typical hurdles to communication in large companies include a division between corporate headquarters and regional, market-oriented business units. Establishing an ongoing collaboration between lines of business that do not usually interact with each other can be difficult. A shared responsibility for supply chain integrity can help to align management and production for better

**Figure 4:** An overview of different types of supply chain infiltrations and ‘re-routing’ that can lead to losses of revenue, brand reputation and consumer trust.
Any company can become a victim, at any time and in any place.

4.3. Identification of products or carriers

Once the stakes involved are understood – along with the potential threats and constraints – and shared with all stakeholders, technologies to implement supply chain transparency can be put in place. But it is important to keep in mind that choosing the right security technology can only be done at the very end of the analysis, once the security situation has been carefully analyzed in its entirety, taking a holistic view.

One could consider several approaches to secure ingredients and products in the supply chain. A technology strategy to tackle the security threats revealed by the initial analysis is usually achieved by combining a bespoke selection of technical security solutions. Combining security elements increases the protection level against counterfeiters. The lifetime of a ‘stacked’ (multiple) security solution against counterfeiting can be longer than that of a single security solution if some of the covert security elements remain confidential for a longer period of time.

Authentication

Authentication features make it possible to recognize if a product is genuine. These are often printed or glued on the product or its packaging. An overt security mark (see Figure 5), is, by definition, visible with the naked eye. Covert features are invisible and can only be read with special devices. In the case of a purely digital approach to printing the authentication mark, an overt way to secure the mark is, for example, to include an area with micro text. This text is visible to the naked eye but can only be read with a magnifying glass. Covert measures might include embedding in the print some invisible information that will be revealed only with a special device. Such digital ‘watermarks’ provide a certain level of security.

Digital product authentication can be upgraded. Material security includes the ink or the substrate of the mark (the material that the ink will be applied to) and can provide further types of security features. For example, overt/semi-covert features have some elements visible to the naked eye and others that are revealed only by a simple filter. A very robust type of covert feature includes markers that can be used to serve as evidence of origin in court, and they are therefore referred to as forensic.

Fingerprinting is another broad class of material security that can be conveyed by the print, the substrate or even the product itself. The idea behind fingerprinting is to authenticate products in a manner similar to fingerprint recognition. Such methods can be used not only to recognize packaging, but also to directly identify the product.

In some cases, for example, with oil and gas products, an ingredient can be added to the product. To ensure a reliable form of authentication, the ingredient can be recognized with special devices. This approach is called in-product marking and is very useful for products where packaging is not present or bears a high risk of being counterfeit. An example of this are tracers for oil and gas products, which can be identified by chemical analysis, such as those provided by Tracerco, a UK-based industrial technology company. In-product marking is more difficult to implement in pharmaceutical and food products.
Preventing product tampering
Authentication methods can help to prevent counterfeiting. But sometimes authenticating the packaging as genuine may not suffice, as packaging might be re-used or refilled. Protection against tampering can be addressed, for example, by introducing seals or labels that carry a material security feature. These anti-tamper seals can be printed separately. They are then applied on the package and have to be broken to open it. An alternative approach to prevent tampering, for example, might be to add a shrink sleeve that must be removed to open a bottle.

Enabling secure identification of a product
Identification refers to tying the product or its package not only to a proof of authenticity, but also to a serial number or code that makes this product more specific, or even unique. Typical examples might use the barcode or the quick response (QR) code. When such codes are applied in a non-unique way, for example, using one code for all products, for one production batch or for one shipment, they do make it easier to track across the supply chain, or provide the end customer with information. But they are not very secure because reproducing one of them is rather easy. When each product carries a unique code, however, the level of functionality and security increases. When the actual codes applied to the products are randomly selected from a very high number of possibilities – for example, if the code is a number with several digits – it becomes more difficult for a counterfeiter to generate a valid code. The idea of a unique code for each product is referred to as serialization and is one of the key trends in the pharmaceutical industry. The highest security level is achieved when the code itself is combined with material security features that make counterfeiting even more difficult.

Figure 5: Different ways to provide secure identification of a product.
4.4. Inspection strategies: multiple security features

Authentication can be performed by people at different stages of the supply chain. Checking the product’s authenticity can be regarded as an inspection and performed with various tools, depending on the security features selected. An inspection can also include using identification to verify that a product is indeed found at the location that would be expected from a supply-chain management point of view. A particular and very formal type of authentication requiring special tools used in certified laboratories is performed based on forensic markers designed to serve as evidence in court.

Figure 6: Different ways to inspect a product.

In principle, authentication can be carried out by everyone in the supply chain. For quick ‘yes or no’ validations, semi-covert features and very simple validation tools can be widely distributed. Due to the relative simplicity of this approach, such authentication has a rather limited impact on supply chain transparency. A much bigger impact can be achieved when trained inspectors, including customs officers, are able to authenticate products with a specific device that reads covert features. Such features not only determine if the product is genuine; they can also send information to a database telling where the inspection was performed, how many fake products were discovered, and other relevant information.

An inspection can be made very secure when both the identification and the authenticating device make use of technology from a single provider that is difficult to reverse engineer.

As already mentioned, building a high level of security into a product is achieved by stacking multiple security elements. The exact strategy and number of built-in features can be defined on a case-by-case basis and tailored to threats that already have been identified. For example, typical stacking of security features can include a QR code with an embedded digital watermark, printed with ink containing a material, covert security feature, which is surrounded by an overt print. Covert features built in
Every end user is a potential inspector. However, the number of available authentication tools for end users is limited.

A particularly intriguing concept is the idea that every end user is a potential inspector. However, the number of available authentication tools for end users is limited. With the naked eye, customers can rely on overt features to authenticate whether a product is genuine. The relatively recent development of smartphones provides users with a powerful tool that can read product info and generate a lot of valuable data for the manufacturer, such as the place of purchase and how the product is used. Customer engagement to perform such ‘inspections’ can be motivated either by the intention of double-checking the product’s authenticity, or for marketing purposes, for example, giving out ‘loyalty points’ to customers who scan the product tag. In sum, a good system should be simple and convenient for consumers, and too complex for fraudsters.

An important part of product and supply chain security involves determining the number of inspectors and where they should operate along the supply chain. There is no one, single good approach for inspection architecture. It must be designed on an individual basis to meet the specific goals the company has defined in a security threat analysis.

4.5. Traceability and tracking of intermediate and final products

Tracking, regardless of whether an intermediate or final product is involved, requires knowing where the product is at any given time on its path through the supply chain. Tracing refers to the knowledge of where and through what regular supply chain events the product has traveled. The information needed for tracking and tracing can be obtained using the identification and authentication tools described in the preceding paragraphs.

A product’s authenticity is just one piece of information relevant to any ‘inspection’. Knowing where, when and by whom the product was inspected are also important pieces of information. All this information can be gathered automatically when the inspector is equipped with a tool that can authenticate the product, capture all additional information and send the data to a central repository. Full supply chain transparency can be achieved by setting up an appropriate inspection strategy: For example, starting with the quality control of intermediate products, working with inspectors in distribution warehouses, customs validation and retail stores inspectors, the supply chain can be mapped in some detail. If necessary, engaging end customers to provide inspection data can provide an additional layer of information that can be used to good advantage.

Large amounts of data are obtained through inspections and tracking individual products. Information technology tools and algorithms that implement ‘big data’ approaches can then provide analysis and intelligence on many aspects of the supply chain, including tracking and tracing. This can be used to help to spot where counterfeit products might be found in significant numbers. The information can also reveal product diversions, or help reconstruct where products from a given batch have been sold if targeted recalls are necessary. Such capabilities are based on the most advanced levels of supply chain transparency.
4.6. General considerations about security technologies

Establishing supply chain transparency should be considered an investment that can be part of the mandatory costs of doing business. Up to half of total cost of ownership comes from setting up ground inspections and taking proper legal protection. When security technology is implemented with the right strategy, it can help reduce costs by acting as a deterrent. This encourages a virtuous cycle that can defray the cost of such investments and, by maintaining security, even generate positive returns.

A more direct look at return on investment is illustrated with an example with a high level of customer engagement, where the inspection rate is high. Assuming 500,000 genuine units are produced, with a retail price of USD 100, and that 35 percent of total units on the market are fake, the total market value, including the value of the counterfeits, is roughly USD 80 million. If the company’s sales margin is about 30 percent, this amounts to about USD 15 million – approximately USD 8 million is missing from the legitimate brand owner’s pocket because genuine products are displaced by counterfeits. These numbers are just an illustration. The numbers can be much bigger in cases involving high-value, high-volume or highly counterfeit markets. In any case, if 25 percent of counterfeits can be eliminated by supply chain transparency, a significant direct recovery is possible via new sales – USD 2 million in the example above. For an initial investment of, say, USD 200,000 for deploying a supply chain transparency solution, this means that a short-term return could be 10 times the initial investment. In general, when the supply chain transparency approach is well aligned with the security threat, and all financial returns are effectively measured, a return on investment in the range of 5 to 10 can be expected in markets with a high level of fraudulent activity.

The role of security standards and certifications

In environments where supply chain security standards are in place, the overall complexity of supply chain risks can be managed to some extent. But this is often not the case. Industries where threats are on the rise are in the process of drafting standards, but this can be quite a long process. If the requirements imposed by future security standards are not yet defined, then security solutions should be designed that are flexible enough to be adapted to the official standards once they are in effect, and the solutions should include some degree of openness and interoperability based on current, existing standards.

Beyond standards, products can also be certified with quality labels at the country, state or industry segment levels to testify that the products meet standards. A brand can adopt, and affiliate itself with such labeling by complying with the required conditions. Beyond logos, the certifying body is also in charge of all paper certificates verifying that a product conforms to standards. But such labels typically do not help to ensure transparency of value chains; they usually have none of the security features described here. Thus, a fake quality label can be easily reproduced and attached to a counterfeit product. The idea of printing the logo with security features or adding a serialized identification for end consumers to verify that the product complies with standards would help to ensure product quality and end-to-end supply chain transparency.

The total cost of ownership includes both the direct and indirect costs of a product or solution.
4.7. A product security intelligence strategy

Successful product security intelligence allows companies to detect something amiss, respond and communicate with key stakeholders. Ensuring the legitimate supply chain’s integrity also requires a strategy to provide product security ‘intelligence,’ meaning here, information-gathering, assessment and evaluation processes to make tactical and strategic decisions. This function is designed to allow an efficient, effective response to supply chain threats. It needs to be implemented within an organization at the global level where strategic supply chain risks are also managed. In many companies these intelligence functions are staffed with professionals with a background in law enforcement and intelligence-gathering.

It is impossible to systematically respond to every single issue or event that raises suspicion. Companies must develop their own approach to identify those areas requiring action. This means not only monitoring their own activities, but also keeping surveillance on suppliers, distributors and retailers, and tracking consumer behavior and response. Successful supply chain intelligence lets companies detect a serious incident, respond to it internally in an appropriate way, and communicate with the relevant external stakeholders: for example, customs authorities, the public and consumers, policymakers and regulators.

Supply chain intelligence operations need to overcome internal information barriers within an organization; they should span many business units and functions, including product security, anti-counterfeiting, brand protection, product quality, legal and compliance, public and government affairs, communications, technical operations, and many more areas. Beyond those at the top of the organization, these networks also need to include regional top management.

As an example of how this might work, the global head of security risk for a large pharmaceutical company, a former police officer and task force officer for the U.S. Federal Bureau of Investigation (FBI), shared these insights on the comprehensive intelligence strategy his company uses. It has built a global network of more than 200 employees who have sufficiently high security clearance to know all overt and covert security features used to protect the company’s products. They are equipped with the necessary authentication tools to rapidly identify a fake or tampered version within a short time, anywhere in the world. The company also has an impressive range of additional analytical capabilities, to enable it, for example, to track biological or chemical traces included in the counterfeit products back to a specific region. Thus, the company can supply evidence to the authorities to help them identify the source of infiltration. When putting together a counterfeiting case, the security head emphasized that companies must be aware that some authorities, for example in China, place restrictions on investigations by private companies.

Detection and investigation

The experts we interviewed agreed that in all industry sectors, there is a pressing need to enhance efforts to identify, detect and report counterfeit and tampered products. Generally, companies rely on various sources for incident reports. Customers reporting flawed products via a complaints hotline are one key avenue of detection. Many companies also run their own sales and re-sales markets surveillance programs. Other crucial information can come from customs and police, and from competitors.
Gathering and providing information through public online platforms is another way to gain information, and there are already such sites available. The Counterfeit Report, an online resource for counterfeit product alerts, news, and press releases, is equipped with a search option for products, and accessible to both consumers and companies. However, Craig Crosby, who publishes The Counterfeit Report, told us that manufacturers had been less open to this channel than consumers, because many companies feared being stigmatized by ‘false positives’ – incorrect allegations of fakes – and that such a platform could be misconstrued as a form of quality control, and could also be abused by users. The Illicit Trade Monitor is another website that, through news and reports, raises awareness about the magnitude and ramifications of illicit trade, including counterfeits.

E-commerce has become a battleground in the fight against counterfeits

Online sales of counterfeit goods have grown dramatically over recent years. In the 2013 survey by PwC, respondents said they are more likely to search online than in physical markets or abroad for counterfeit medicines and auto parts. The vice president, government affairs, for the U.S. Electronic Retailing Association, Bill McClellan, told us that collaborating with large e-commerce platforms is key, as these provide significant channels to exchange counterfeits. Marc Schaedeli, former group risk manager at Nestlé, told us that in the food and beverages sector, counterfeit products are, to a large extent, marketed and sold through e-commerce channels.

However, e-commerce platforms may not take responsibility for illicit goods sold through them according to Craig Crosby from The Counterfeit Report. In some cases, illicit products can simply be relisted after they were flagged. According to Craig Crosby, the regulatory environment, though not yet fully developed, would still be sufficient to prevent lax enforcement practices, but he believes many claims are interpreted in favor of e-commerce platforms.

The High Court in England has recently made a landmark decision in favor of brand owners against websites that advertise and sell counterfeits: Richemont, the owner of luxury brands including Cartier, IWC and Montblanc, has been granted a blocking order that requires the five largest internet service providers in the UK to prevent access to third-party websites that advertise and sell goods that infringe upon Richemont’s trademark rights. It can be expected that other brand owners will apply for such blocking orders in the UK and in other countries within the EU, to close the most offending sites.

---

36 See the website at https://thecounterfeitreport.com/
37 See the website at http://www.illicittrademonitor.com
Exchange of operational information and intelligence

All experts at multinational companies with whom we spoke for this study said that exchanging more operational information and intelligence – that is, practical, case-related information that is relevant for the surveillance, intelligence and law enforcement communities – would help to protect the integrity of supply chains. Operational information can be exchanged vertically (along the supply chain) or horizontally (among competitors). Details of specific counterfeiting or tampering cases can be very helpful for investigations, including the name of the product, the time and place where a new counterfeit product turned up, and the main suppliers or production regions. But the time and quality of the data are crucial. Because of its sometimes biased nature, confidentiality and protection of operational information are a concern. The data should also be verified and constantly updated.

The horizontal exchange of information amongst competitors requires those involved to trust each other, and might also be limited by antitrust laws and regulations, as Stefan Bühler and Peter Hettich, professors at the University of St. Gallen said in interviews. Antitrust laws prohibit information sharing involving prices, quantities, regions, companies’ approach to changes in value-added tax, or applications for a public tender. Discriminatory behavior, or appealing to groups boycotting a supplier, is also not acceptable practice. Facts – what really happened in connection with a supplier, for example – can usually be shared, but this should first be discussed with local lawyers. Companies should also be aware that joint sanctions against a supplier can backfire if the supplier has strong political ties, particularly in emerging markets, or is important for the national economy. Vertical exchange of operational information is usually less of a problem, but matters pertaining to national regulations, criminal law and competition law should also be checked with local lawyers.
Coordinating supply chain intelligence among companies

Substantial synergies can be obtained by sharing supply chain infiltration information and coordinating enforcement actions. For example, if a counterfeiter has faked a product of Company A, it is relatively easy for him or her to also fake a similar product made by Company B. Coordinating intelligence can help both companies to identify the counterfeiter, support local authorities in closing down its operations, and hamper distribution of counterfeit products. We highlight two successful approaches from different industries showing how supply chain intelligence can be shared:

• The **Pharmaceutical Security Institute (PSI)** is a membership organization of the 28 largest pharmaceutical companies in the world.⁴⁰ The goals of the PSI are to protect public health, share information on the counterfeiting of pharmaceuticals and initiate enforcement actions through appropriate authorities. We were told by a head of security risk of a PSI member company that this is an extremely useful platform for the industry in coordinating against counterfeitors. Every case of counterfeiting that affects a member is reported within this organization. The security and anti-counterfeiting specialists of the member companies meet semiannually. There is always an antitrust attorney involved to ensure that no antitrust laws are violated.

• The **Federation of the Swiss Watch Industry (FH)** has a small team that monitors online sales of Swiss watches worldwide.⁴¹ The FH also trains and supports enforcement authorities in the seizures of fake Swiss watches. With around 500 member companies, the FH represents about 90 percent of the Swiss watch industry and can unlock synergies for a national industry, including both large and smaller companies. The FH’s intelligence services are especially helpful for SMEs that lack the resources to conduct these operations on their own.

---

⁴⁰ See the Institute’s website at http://www.psi-inc.org/
index.cfm
⁴¹ See the Federation’s website at http://www.fhs.ch/eng/
homepage.html
Engaging in public policy and alliances, and pooling services to combat supply chain infiltrations, are crucial ‘outside-in’ activities. But our research showed that typically only large companies have the capacity to deal with a broad range of activities, including unilateral surveillance and intelligence operations, consumer outreach, public policy engagements, legal services in foreign markets, and ensuring the support of authorities in enforcement and seizure operations. Such activities can also be delegated to third parties such as industry associations or private organizations.

Figure 7: Schematic diagram of a company, its suppliers and distributors, facing possible cases of supply chain infiltrations, as shown in Figure 1. Here, all actors and stakeholders belong to the same legal, political and business environment. If a company adopts appropriate ‘outside-in’ activities, it can exert some influence on this environment to make infiltration more difficult, as indicated in the diagram.
5.1. Engaging in public policy to protect supply chains

Policymakers need to find the right balance between allowing entrepreneurial freedom and ensuring business activities don’t infringe on the rights of those living in a society, especially in emerging markets. From a risk management point of view, it is crucial that policymakers understand what consequences their decisions have on the overall risk landscape. Private sector engagement in public policy can help improve laws and regulations to ensure supply chains are better protected, creating significant value for society and the economy. Some public policy issues that should be high on the agenda of companies and associations in dialogue with policymakers include:

**Intellectual property rights**

Protecting intellectual property rights (‘IP rights’ or ‘IPR’) is a controversial topic in markets where imitation is considered an acceptable form of competition. In some emerging economies, making fakes provides employment and export revenue, at least in the short run. However, in the long run, excessive IPR infringements undermine crucial drivers of economic growth, including the capacity to innovate and/or the reputation of business partners in certain regions.

In China, IP ‘leakage’ reduced European manufacturers’ potential profits by 20 percent, and the U.S. government estimates that China accounted for nearly 80 percent of all IP thefts from U.S.-headquartered organizations in 2013, amounting to an estimated USD 300 billion in lost business.42 In view of the size of the losses due to IPR infringements, it is obvious that Western companies and governments are pushing for global acceptance of their IPR protection standards.

**Consumer health and safety, and links to IP**

While IP discussions traditionally focus on the opposing interests of developed and developing countries, there is greater consensus regarding the importance of protecting consumers. The Center for Medicine in the Public Interest estimates that between 200,000 and 300,000 people die each year in China due to counterfeit or substandard medicine, and these are only the reported cases.43 Taking this and other estimates into account,44 it may be assumed that today about a million people die per year due to fake medicines. The World Health Organization states that only about 20 percent of its 191 member countries have a well-developed approach to drug regulation, but about 30 percent either have no drug regulation or regulate drugs only on a very limited basis. The remaining 50 percent fall somewhere between these two extremes.45 The private sector plays an important role in supporting sound legal and regulatory frameworks governing healthcare markets where regulation is still evolving, especially given that counterfeit medicine is still not getting adequate priority on many political agendas in these countries, based on what we learned from healthcare experts we interviewed.

Better enforcement of IPR in all industry sectors can reduce the risk of supply chain infiltration and lead to higher-quality, safer products. Following a series of major supply chain infiltration scandals in China, authorities have taken measures to protect consumers by tightening national standards and laws governing consumer protection and IP.

Supply chain integrity: protecting companies’ blind spots
campaign to combat IPR infringement and combat the manufacture and sales of counterfeit goods and shoddy commodities. In 2011, China created a ‘Leading Group’ whose mission is to fight nationally against IP infringement and counterfeiting. This government-driven initiative comprises 29 Chinese authorities, aiming to improve coordination between them. While the ‘Leading Group’ does not include private companies, the private sector can be involved in certain cases, as described in the example of Swiss-Chinese bilateral dialogue cited here.

The Swiss-Chinese bilateral dialogue on IP
The free trade agreement between Switzerland and China entered into force in July 2014. Seven years earlier, the countries began a bilateral dialogue on IP. The discussions were coordinated on the Swiss side by the Swiss Federal Institute of Intellectual Property (IPI), an agency that serves as a contact for companies in matters related to IP rights. Working group meetings are held annually, with discussions with Chinese authorities on both government and industry levels. Swiss companies, and recently also Chinese companies, joined the discussions.

Simon Schmid from IPI’s legal services unit, who has moderated this dialogue for the past several years, said the idea of an industry roundtable at the meetings was first put forth five years ago, and the roundtable is now a standing item on the agenda at these meetings. The IPI contacts Swiss companies through national industry associations such as Economiesuisse, Swissmem, Interpharma and FH. Some Swiss companies are also directly involved. IPI is also managing the office for Stop Piracy, a multi-stakeholder platform that works to increase awareness of counterfeiting and piracy in Switzerland.

The Swiss Embassy, the IPI and the Swiss Chinese Chamber of Commerce in China (Swisscham) have set up an informal mechanism on the internet that allows Swiss companies to lodge complaints about IPR infringements. Complaints can be submitted electronically to Swisscham. Cases with merit are passed on to the Office of the Chinese IPR Leading Group.46

The Swiss-Chinese dialogue on IP is an excellent example how public policy engagements can foster valuable international collaboration that engages both the public and the private sector, and helps to improve supply chain protection.

46 For more detailed instructions, see the website of the Swiss Chinese Chamber of Commerce in China, http://cn.swisscham.org/bei/ipr-mechanism
Secrecy of security technologies
Covert security features, as discussed in Section 4, rely first and foremost on secrecy. Criminals are either unaware of their existence or at least unable to fool identification tools. In-product markings include covert security features such as chemical markers added in minute concentrations to products like liquids or gases. But in some industries regulations require that ingredients added to a product, even if the product is a security feature, must be disclosed, even if they are added in a concentration that is within the accepted level of impurities. Such regulations may be counterproductive if they make a suitable, harmless and affordable security solution ineffective. In such situations, companies and industry bodies should engage in a dialogue with policymakers to highlight the benefits of such ‘markers’ to detect fraud, and the damage that could arise from products that have been tampered with, or are a concentration that is within the accepted level of impurities. Society, the economy and the environment could all benefit from allowing certain ‘markers’ to be used.

Effective enforcement of laws and regulations
Lax enforcement of laws and regulations also poses a significant hurdle in the fight against counterfeits. Anti-counterfeiting efforts in China have suffered for some time from over-reliance on ineffective enforcement. Some of our interviewees mentioned complaints that judges were often biased in favor of counterfeiters, supported by local officials, and there was a lack of experience in dealing with IP-related cases. Corruption further encourages a lax approach to enforcing laws. And perpetrators quickly adapt to changes in enforcement practices. For example, after a successful law enforcement intervention in China, the networks that produce counterfeit pesticides found a new way to circumvent the rules, and switched from ‘market-ready’ products to chemicals imported into the EU in bulk as unlabeled products, which is not illegal. These are then repackaged and labelled inside the EU.47

Yves Bugmann, head of the legal division at the Federation of the Swiss Watch Industry (FH), confirmed that the primary challenge FH faces in China is ensuring laws that have recently been put in place are enforced. This concern goes beyond the watch industry. He emphasized that an enhanced global organization to take care of counterfeiting issues is needed, especially for engaging with policymakers, and to provide support on the ground, facilitating cooperation between the public and the private sectors.

5.2. Alliances and pooled services to combat supply chain infiltration
Many of those with whom we spoke emphasized the fact that very few companies make full use of legal frameworks already present in some emerging markets. For example, many companies could benefit much more from China’s enhanced enforcement capabilities. Building alliances and pooling services to combat supply chain infiltration could help. Third parties like industry associations or private organizations can give companies information about legal systems, safety regulations and processes in key markets, and support companies with related services. Section 4.7 provides two such examples of how industry associations can provide support.

Sourcing knowledge and services
The benefits of sharing information about publicly-disclosed supply chain infiltration incidents can be enhanced by using online platforms such as The Counterfeit Report. Industry associations can provide access to regulators, government bodies and local lawyers who are familiar with specific industries and markets. Many services can be pooled, such as e-commerce monitoring, enforcing IP rights in physical and online markets, or providing hotlines to report IPR infringements. Databases such as OHIM’s enforcement database for IP in the EU, or the global IPM platform against counterfeiting of the World Customs Organization, as discussed in Section 3.6, also provide enforcement authorities with crucial sources of knowledge.

Industry associations
Industry associations can play a crucial role in strengthening supply chain risk management. They can promote dialogue to raise awareness of risks and possible solutions, and facilitate cooperation. Policymakers and government authorities are sometimes also more willing to engage with a representative third party like an industry association than an individual company. In this regard, the FH can serve as a role model for other industry associations. As discussed in Section 4.7, the FH provides a cost-efficient center of competence for supply chain integrity tailored to the specific needs of the watch industry, which is especially valuable for small and medium-sized companies.

Independent and non-governmental organizations
Some services that protect and inform on supply chain risk can be offered across different industries. One example of this type of organization is React,48 a Netherlands-based non-profit organization. For an annual fee, React assists its over 200 members, which include some of the world’s biggest companies, in the fight against counterfeit trade with a broad range of services, including knowledge sharing, supporting customs enforcement, monitoring markets and the internet, providing training seminars, and working with service providers abroad, such as law firms. As part of its internet-related services, React uses web crawlers to detect suspicious offers, asks hosts to remove them, and tries to identify and pursue the sellers. The International AntiCounterfeiting Coalition (IACC),49 based in Washington, D.C., is another non-profit organization that offers services similar to those provided by React, building on a member base of more than 250 companies and organizations.

Other organizations that work to combat counterfeiting and piracy include the International Chamber of Commerce’s Business Action to Stop Counterfeiting and Piracy (ICC BASCAP), the Anti-Counterfeiting Group (ACG) and the Global Anti-Counterfeiting Group network (GACG). Unlike React and IACC, these organizations focus more on information exchange, research and lobbying, as well as training and educating authorities. ICC BASCAP and GACG have very exclusive membership access policies. INTERPOL, the world’s largest international police organization, is very much focused on large-scale enforcement operations, coordinating actions of police in various countries, as opposed to providing operational support to an individual company that has experienced supply chain issues.

48See the website at http://www.react.org/
49See the website at http://www.iacc.org/
Section 6
Conclusion: The goal is a resilient supply chain

There is no absolute security for supply chains; there will always be weaknesses to exploit. Prevention is important, but companies also need to be prepared to respond to an infiltration incident at any time and in any place.

As already discussed in this study, the goal is for companies to become resilient, meaning they can absorb shocks, recover, and become operational again as soon as possible. To sum up, corporate resilience needs to extend to withstanding the shocks caused by criminals who infiltrate supply chains.

One example, already cited in this study, was the melamine scandal in China in 2008 that caused deaths, mass health problems and public outrage. It involved watered-down dairy products (including infant formula) adulterated with the industrial chemical. Melamine, normally used as a plastics stabilizer, was added to give milk the appearance, at least, of having a higher protein content. Some two dozen Chinese dairy companies sold the adulterated products. The contamination caused 300,000 babies to suffer kidney problems, such as kidney stones or other damage, tens of thousands of them were hospitalized, and six babies died as a result, according to the government.50 For risk managers the alarming aspect of the melamine fraud was that criminals exploited a weakness in tools widely-used in quality control. The common analytics tools measured the protein content of milk only indirectly, namely by determining its nitrogen content. Melamine, a nitrogen-rich chemical, was only identified after an investigation of mass poisoning analyzed the dairy products using more sophisticated tests. The adulteration was possible using an astonishing level of technical sophistication.51 Without a case of mass poisoning, the problems would have gone undetected.

In 2008, another major case was reported that exploited a weakness in the analytics process, affecting a product in the healthcare sector. A contaminated blood thinner, heparin, produced in China, caused 81 deaths in the U.S. and also caused problems in other countries including Germany.52 Here, too, traditional quality control tests could not detect what was, most likely, a contaminant that had been added deliberately. It took highly sophisticated analytical tools to even spot the contaminant.53

These examples from highly-regulated industry sectors that are subject to regular scrutiny make it clear that infiltration can happen even when significant prevention measures are employed. Since product counterfeiting and tampering are problems that affect all industry sectors, not only the ones mentioned in the recent scandals, all companies should be wary of supply chain infiltrations. Companies must understand the highly diverse nature of these threats and the alarming extent to which supply chains are exposed. Being prepared and putting the right risk management strategy in place can ensure that, when necessary, companies are capable of mounting an effective response to these threats.

We hope that this publication helps companies to enhance supply chain risk management strategies to better protect their sales, brand reputation and consumer trust.

---

50 Chinese figures show fivefold rise in babies sick from contaminated milk, The Guardian (2008), see https://web.archive.org/web/20081205093042/http://www.guardian.co.uk/world/2008/dec/02/china
53 Oversulfated chondroitin sulfate is a contaminant in heparin associated with adverse clinical events, Marco Guerrini et al., Nature Biotechnology 26, 669 - 675 (2008), see http://www.nature.com/nbt/journal/v26/n6/abs/nbt1407.html

Supply chain integrity: protecting companies’ blind spots 33
Acknowledgements

The authors would like to thank the following experts for their insights and support: Ronald Brohm, Managing Director at React; Yves Bugmann, head of the legal division at the Federation of the Swiss Watch industry; Prof. Dr. Stefan Bühler, Professor of Applied Microeconomics at University of St. Gallen and Deputy Chairman of the Swiss Competition Commission; Craig Crosby, publisher of The Counterfeit Report; Prof. Dr. Peter Hettich, Professor for Law of Regulated Markets at University of St. Gallen; Dr. Joachim Hofmann, Senior Trademark Lawyer at Syngenta; Bill McClellan, Vice President Government Affairs of the Electronic Retailing Association; Anna Mejlerö, Security Intelligence Specialist at Syngenta; Mireille Saliba, Business Unit Head at a large pharmaceutical company; Marc Schaedeli, at the time of the interview Group Risk Manager, Nestlé; Simon Schmid, legal adviser at the Swiss Federal Institute of Intellectual Property; Hans Schwab, CEO of TechTrace; Silvia Volponi, BU Patent Officer at ABB; and Dr. Andreas Wittmer, Managing Director of HSG-Center for Aviation Competence and Vice Director at the Institute for Systemic Management and Public Governance at University of St. Gallen.

Our thanks also go to our colleagues for valuable insights, comments on the text, and support. From SICPA: Frederic Albinyana, Christine Macqueen and Christophe Renard; from Zurich: Robert Gremli, Tilman Hengevoss, Christian Hott, Philipp Hoyer, Otto Kocsis, David Swaden and Nick Wildgoose.

We especially thank Christophe Hilbert, Shanti Lourdenadin, Marius Obrist, Katharina Schramm and Tarik Terzic for the contributions they provided to this publication as part of a business project under the CEMS Master’s in International Management program. They conducted primary and secondary research activities with Zurich and developed strategic insights in the context of counterfeit products and supply chain integrity.

About Zurich Insurance Group: Zurich Insurance Group is a leading multi-line insurer that serves its customers in global and local markets. With about 55,000 employees, we provide a wide range of general insurance and life insurance products and services. We serve individuals, small businesses, and mid-sized and large companies, including multinational corporations, in more than 170 countries.

About SICPA: SICPA is a provider of security inks as well as secured identification, traceability and authentication solutions, on a worldwide basis to companies and governments. With high-technology security inks at the core of its expertise, the company protects the majority of the world’s banknotes, security and value documents and offers solutions and services to governments and industry, ensuring product authentication, traceability and protection as well as tax reconciliation. www.sicpa.com

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.

This publication may not be reproduced either in whole, or in part, without prior written permission of Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Switzerland and SICPA S.A., Av. De Florissant 41, Prilly, Switzerland. Zurich Insurance Company Ltd and SICPA S.A. expressly prohibit the distribution of this publication by or to third parties for any reason. Neither the Zurich Group nor SICPA S.A. accept liability for any loss arising from the use or distribution of this presentation. This publication is for distribution only under such circumstances as may be permitted by applicable law and regulations. This publication does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.

Zurich Insurance Company Ltd
Mythenquai 2
8002 Zurich
Switzerland

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