bsi. SCREEN
Supply Chain Risk Exposure Evaluation Network

Supply Chain Risk Insights

2019

Contents

Introduction

BSI recorded a myriad of complex emerging threats and challenges to supply chain security, corporate social responsibility, and business continuity globally in 2018. Marked ideological shifts in governance have given way to or exacerbated new dimensions of risk to the global supply chain. The ongoing prevalence of cyber threats and the evolving paradigm in addressing such threats continues to create new challenges and approaches to supply chain security. Despite these newer concerns, the threats and risks of previous years, such as ones caused by mass migration, corruption, and organized crime, remain ever-present. Finally, among these new and old risks, the advent of rewritten CTPAT Minimum Security Criteria alongside Brexit, represent other key developments for supply chain professionals in 2019.

Recent shifts in political ideology in the governments of Brazil, Mexico, the United Kingdom, India, and the United States are likely setting the stage for an eventful 2019. Newly-elected leadership in Brazil and Mexico are attempting to chart a new course in Latin America. The recently-elected president of Brazil has swiftly undertaken efforts that may pose corporate social responsibility risks for some industries operating in Brazil. Mexico's president is undertaking new initiatives to curtail the corruption that has historically underwritten organized crime, cargo theft, and oil theft in the country. The ramifications of such initiatives may have sweeping consequences for business continuity and cargo security. The U.S.-China trade dispute has resulted in new suites of concerns related to intellectual property protections and the relocation of relevant facilities for a host of businesses. Finally, the outcome of negotiations on Brexit remains opaque, creating ripples of uncertainty through supply chains operating within and through the United Kingdom and the European Union.

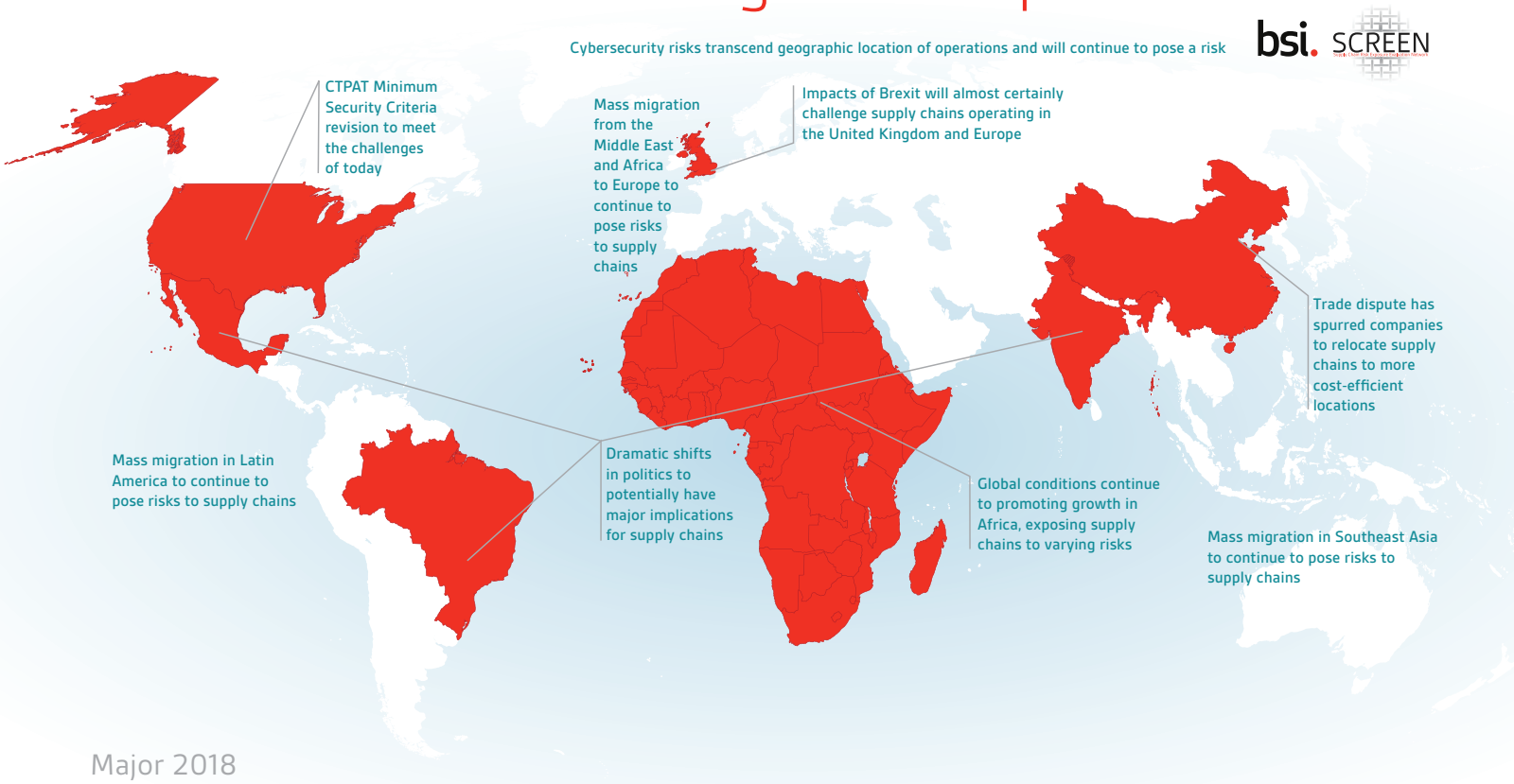
Amid these changes in political ideology globally, the continent of Africa stands poised to seize economically on the new landscape. The geopolitical competition of the United States, China, and Russia are likely to drive foreign investment to Africa this year. With the drive to integrate more of Africa into the global supply chain, similarly to the experience of Southeast Asia in recent years, companies must navigate risks to security, corporate social responsibility, and business continuity. In 2019, trade within and through Africa may drive solutions to exigent challenges on the continent of infrastructure, labor rights, and security.

Within this new global landscape, cybersecurity stands as an overarching and multi-faceted struggle for all parties throughout the supply chain. Securing data and facilities in a fast-paced and modular world connected by the "internet of things" is an emerging challenge that all supply chain professionals undertook in 2018 and continue to grapple with in 2019.

Within the United States, companies enjoying trade benefits under CTPAT will soon need to meet new criteria for certification, after almost two decades of largely unchanged requirements. As the revised criteria for CTPAT are unveiled, companies will need to undertake new efforts to achieve supply chain security and mitigate emerging risks.

BSI forecasts the evolving geopolitical landscape as a major engine of global supply chain security, business continuity, and corporate responsibility risks in 2019. The trends examined in the following report illuminate the persistent and ongoing challenges to global supply chains as well as the progress made against existing threats. Based on these trends, BSI has outlined best practices to countering and managing the new risk landscape.

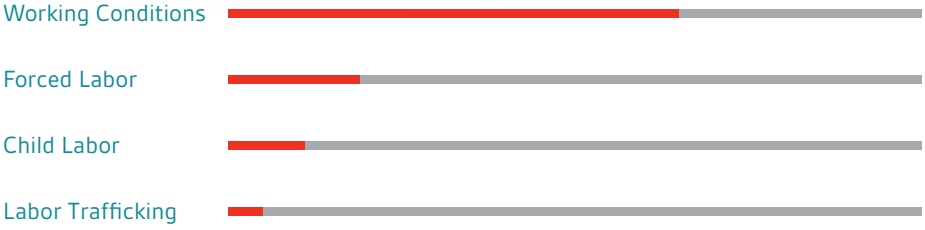
SCREEN Global Intelligence Report



Major 2018 BSI Threat Rating Trends

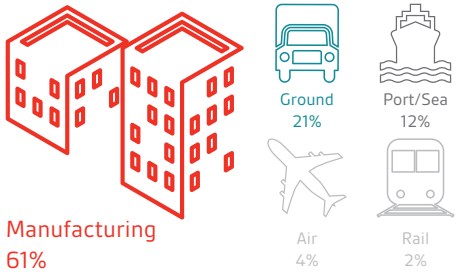
BSI SCREEN 2018 Incident Data Highlights

Top Labor Violations



Top Commodities Stolen

Top Modalities Disrupted by Strikes



CTPAT Minimum Security Criteria Revised to Meet the Challenges of Today

Companies certified under the U.S. Customs and Border Protection's (CBP) Customs Trade Partnership Against Terrorism (CTPAT) have enjoyed various trade benefits by meeting select security criteria that have remained unchanged for almost the last 20 years. However, noting the changing landscape of threats to supply chains around the world, CBP initiated a review of the Minimum Security Criteria (MSC) needed to be met in order to obtain certification under the CTPAT program. Now, after conducting the review of the MSC in partnership with industry leading professionals, CBP is expected to be close to implementing a new version of the MSC, presenting both prospective and existing certified companies with new challenges in the pursuit of ensuring that supply chains remain secure.

The Need for Revised Minimum Security Criteria

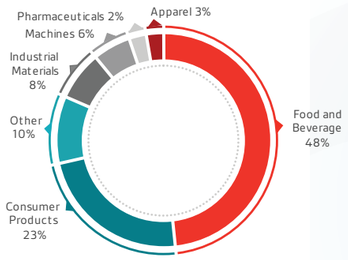
U.S. Customs and Border Protection set out to revise the MSC in order to elevate the security of and meet the evolving threats to supply chains and fulfil its mission of preventing illicit material from entering the United States. Although supply chains continue to face a set of threats that are ever-morphing in regards to tactics and sophistication, the core risks that companies face remain relatively static and relate back to the core goal of the CTPAT program, which is to prevent the entrance of illicit goods into the United States via supply chains.

One such core risk that continues to plague companies is the risk of smuggling, or unmanifested cargo introduction. BSI most commonly recorded seizures of unmanifested cargo, including illegal drugs, arms and weapons, and stowaways, from shipments of food and beverage last year. Smugglers most commonly targeted cargo trucks for operations, with a fair amount of incidents also involving sea container cargo shipments. Origin and destination data from 2018 also tended to follow the established flows of illegal drugs from South America to North America and Europe and within Asia as well.

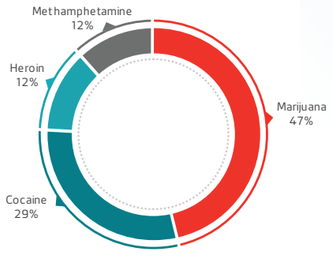
BSI has generally identified North America and Europe as the key destination regions for cocaine produced and exported from South American countries like Colombia, Peru, and Brazil. These longstanding trends have allowed for risk profiling to be used to help determine the risk of illegal drug introduction into cargo originating in South America, as shipments intended for North America and Europe typically incurred a higher risk of introduction. However, BSI recorded multiple discoveries of South American cocaine hidden in cargo shipments destined for Asia last year, representing a trend in destinations for illegal drugs produced in Latin America. BSI suggests that shipments intended for Asia should now be considered while risk profiling as the growing demand for cocaine in the region, particularly in Australia and China, suggests that these consignments face an increasing risk of illegal drug introduction.

Global Unmanifested Cargo Trends H1 2018

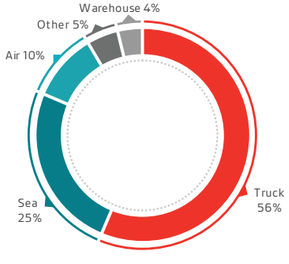
Top Targeted Commodities



Top Illicit Goods



Transportation Mode



bsi. SCREEN
Supply Chain Risk Exposure Evaluation Network

To Spain, Belgium and the Netherlands

To Mexico and United States

To Spain, Portugal, Belgium, Italy, and the Netherlands

To Turkey via the Balkan Route

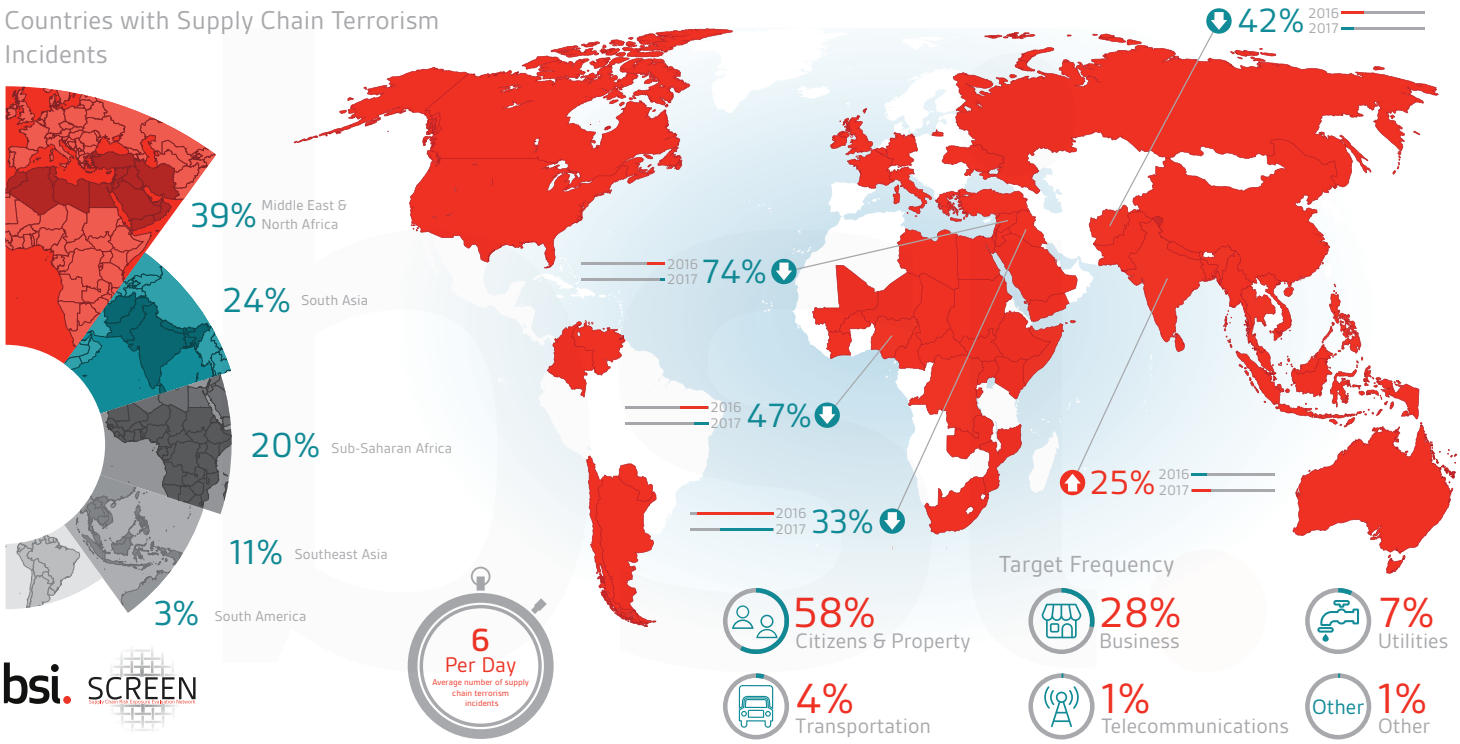
To UAE and Libya

To Australia and Malaysia

To Australia and Malaysia

Air Sea Truck

Global Supply Chain Terrorism Risk



Terrorism also remains an ever present risk to supply chains, although BSI has noted a decrease in the overall number of terrorist attacks involving or targeting the supply chain as of late. However, this overall drop in supply chain terrorist attacks has largely been confined to major hot spot countries such as Syria, Afghanistan, and Iraq. Generally successful coalition efforts to combat the spread of Islamic State (ISIS) has eroded the group's influence in countries such as the aforementioned Iraq and Syria, which has also largely driven down the total number of supply chain terrorist attacks recorded. However, the lack of similar anti-terrorism operations in some countries, such as India, the Philippines, and Colombia, have actually allowed for a consistent or even increased level of supply chain terrorism, highlighting the importance of programs such as CTPAT in the face of changing terrorism dynamics.

Ramifications of New Criteria for Established Organizational Processes

Companies that wish to become certified, or recertify, under the CTPAT program must now ensure that their respective supply chain meets the newly revised Minimum Security Criteria (MSC). The MSC can be organized by three primary focus areas, Corporate Security, Transportation Security, and People and Physical Security, which can then be broken down into multiple categories that each contain specific criteria. The revised MSC includes three new categories of criteria, Security Vision and Responsibility, Cybersecurity, and Agricultural Security, with the first two most likely to challenge company operations and the required protocols of business partners around the world.

Security Vision and Responsibility
The new Security Vision and Responsibility category of the MSC contains criteria that will require the creation of a cross-functional team, including representatives from all relevant departments, which will likely require companies to adjust the institutionalized processes for managing supply chain security. The key premise behind the introduction of this criteria is the continuity of supply chain security practices in the event of personnel turnover. However, the process of instituting organizational change is never an easy endeavor, and the requirement of now having departments such as Human Resources and Information Technology participate in the supply chain security process is likely to be difficult for a variety of reasons. Supply chain security is a relatively niche field of expertise, and it will likely be challenging to initially convince unfamiliar stakeholders, with their own line of un-related duties, to buy into the premise of a cross-functional team.

Perhaps the best tool that can be used to accomplish this goal is utilizing a cost-benefit analysis of obtaining demonstrate the potential financial benefits of incurring a reduced number of inspections for inbound shipments. Addressing the benefits to each component department of the cross-functional team can also help promote the successful implementation of the concept. For example, emphasizing how many competitors are members of the CTPAT program can help gain the buy in from key decision makers. Other departments, such as logistics, would likely benefit from reduced inspections and supplier mapping. Generally discussing how important certification is may help provide a sense of urgency in the creation of a cross functional team.

Another major constraint in successfully establishing a cross-functional team is time. The core team responsible for implementing CTPAT should carefully review the requirements and determine exactly which team – logistics, supply chain, human resources, and information technology – can assist with each part. Developing a specific list of questions and processes you need to ask each team beforehand can also ensure that time is not wasted and ultimately facilitate the creation and function of the team.

New Categories in CTPAT Minimum Security Criteria Revision

	Security Vision and Responsibility	Cybersecurity	Agricultural Responsibility
Requirement	Requires the creation of a cross-functional team, including representatives of all relevant departments	Requires comprehensive written IT security policies that are reviewed on a regular basis with frequently tested systems	Requires written procedures designed to prevent pest contamination
Reason	Helps prepare in the event of personnel turnover	Helps address vulnerability issues within systems to avoid exploitation including hardware malware and internal/external intrusion	Helps eliminate the threat of foreign animal and plant contaminates which may harbor invasive and destructive pests

Most firms currently have a few unrelated processes occurring, such as supplier assessments and risk assessments, that may not be organized and managed as a whole, with management backing. Assessing gaps at the corporate level first rather than starting with the suppliers will be important for developing a cross functional team.

Cybersecurity

The revised MSC also includes a new section entitled Cybersecurity, addressing an issue that continues to rise in importance given the vulnerability of systems to exploitation. Although most larger companies will already have IT security policies that are reviewed on a regular basis and systems that are frequently tested, smaller companies may struggle with some of these new requirements.

Internal information-gathering, a key component of effectively meeting this criteria, will likely be a challenge for any company. Determining when and how to report cybersecurity threats to the government and business partners is also a significant challenge, as the process is not truly defined in any standardize way. Most companies would prefer to keep this information internally, and must ensure that reporting lines are set up carefully to avoid any unintentional release of information.

The possibility of hardware compromise potentially leading to exploitation is another cybersecurity risk. Ensuring that policies and procedures take into account the risk of counterfeit and malicious hardware and software is one key method that can be used to help mitigate the risk of this exposure. Gaining insight into third and even fourth tier suppliers and their security practices is no easy feat for even companies with small supply chains, but doing so can also help alleviate the potential of following victim to hardware compromise.

Strengthened Criteria

Besides introducing new criteria, the revised Minimum Security Criteria (MSC) also includes strengthened versions of the existing requirements that will may also challenge a company's ability to certify.

One strengthened criteria that BSI believes will likely challenge companies is the requirement for CTPAT members to have a written, risk based process for screening new business partners and for monitoring current partners, including checks on the financial soundness of the business partner and any potential for activity related to money laundering or terrorist funding.

A key factor in meeting this strengthened criteria is the ability to have insight into business partner financial practices, specifically in regards to contract management, which is likely to prove difficult for complex supply chains operating across global markets. Companies should work to determine whether business partners operate through intermediary companies or agencies rather than through direct payment streams and identify whether a company is incorporated in a tax haven but operating across multiple other jurisdictions.

Other issues can also compound the difficulty of ensuring the supply chain is free of ties to money laundering or organized crime financing. For example, third party contracts are often paid without sufficiently documented information on the nature of the business conducted, thereby complicating the process of identifying potential risks of illicit financial practices. Obtaining and maintaining proper documentation concerning business partner relationships is a major component of successfully complying with this piece of criteria. This process includes identifying the relationship with the business partner, including whether the entity is a one-off supplier, and ensuring evidence of legal operational status is obtained in the form of business registration numbers or other documentation. This latter process entails identifying parent companies and ownership structures.

Another potentially challenging component of the strengthened criteria is the provision that "CTPAT Members should have written procedures in place that address crisis management, business continuity, security recovery plans, and business resumption." Although this criteria is only listed as a "should" rather than mandatory component for certifying companies, this strengthened aspect of the MSC embodies the extent to which criteria has been strengthened, as it introduces a concept that is likely foreign to many supply chain security and trade compliance professionals. Despite this, it is very likely that these procedures are already outlined within a company and can simply be shared between relevant members of the cross functional team.

In the event that such protocols do not already exist, companies wishing to comply with this piece of criteria should conduct a proper risk assessment of business partners in respect to supplier criticality and geographic risk.

The disparity between the impacts of natural disasters in these two countries exemplifies the importance of not just looking at the probability that a business continuity incident will occur, regardless of whether the incident is natural or man-made, how resiliency must be factored into any risk assessment.

Although there are many new and additional requirements under the revised MSC that are likely to present companies with new challenges, many of the criteria, specifically the physical security requirements, are now much more prescriptive than they were in the prior version. This higher level of prescriptiveness will likely make it simpler to comply. In addition, security technology has become cheaper and easier to use in many cases, further enabling compliance. Despite the new challenges that companies will surely face once the finalized version of the revised MSC is released, the state of supply chain security in the United States will most certainly benefit from the new and enhanced criteria.

While conducting a business continuity risk assessment of the supply chain, it is important to note not just the exposure a business partner has to both natural and man-made disasters, but also the resiliency, or lack of, that could impact the overall level of disruption to the supply chain. A prime example of how resiliency can factor into supply chain disruptions is the contrasting level of preparedness for natural disasters that BSI noted between Japan and Indonesia last year. BSI rates the risk to natural disaster resiliency in Japan as Low, and although the country saw almost a record number of typhoons in 2018, there were only about 250 reported deaths. BSI did record some supply chain disruptions to ground and air transport, but the delays were generally only short term and operations resumed relatively quickly.

In Indonesia, however, which suffers from a High threat to natural disaster resiliency, BSI noted a much different impact from natural disasters due to detrimental levels of preparedness. The country experienced one major earthquake and a tsunami that resulted in about 1,600 deaths and long-lasting disruptions to all transportation modalities in the affected area. A major factor in why this incident resulted in so much more destruction and deaths was the failure of the government to maintain early detection systems, resulting in a lack of warning to citizens in the area.

Dramatic Shifts in Politics and Potential Implications for Supply Chains

BSI noted a dramatic shift in politics in countries around the world last year, with governments enacting policies that represent a major turnabout from previous ideology. BSI believes that this trend of disruptive policymaking will likely be an issue that will impact supply chains over the next year in both identified countries such as the United Kingdom, Brazil, and Mexico in addition to potentially new countries such as India.

In particular, the United Kingdom's exit from the European Union has created an atmosphere of confusion for supply chains and has already led some businesses to shift operations or regional headquarters elsewhere, seek alternative suppliers, and in some cases to stockpile pharmaceuticals. Likewise, the United States—China trade dispute similarly led companies to seek alternative suppliers or relocate parts of their supply chains to other countries that may increase their exposure to unforeseen risks.

There is potential for recent political shifts in other countries, such as Mexico and Brazil, to impact supply chains as well. Mexico's newly-elected president has pursued a policy of enhancing security and addressing corruption in the country, though it remains to be seen how effective this policy will be at addressing longstanding challenges such as oil theft and illegal pipeline tapping, institutionalized corruption, and overall supply chain security. Brazil's newly-inaugurated Jair Bolsonaro has so far enacted policies many see as endangering minority rights, and it is likely that similar policies that curtail the rights of workers and vulnerable classes will follow in 2019. Finally, India faces national elections beginning in April of this year. Recently, India experienced a heightened level of unrest among the working class, some of which was quelled by a reversal in policy regarding fuel imports. Similarly, India's Prime Minister, one of only two right-wing politicians to occupy the office, has experienced civil unrest as a result of disgruntlement with government policies. Given this recent dissatisfaction and upcoming national elections, it is possible that we will observe further unrest and a shift back to the center-left politicians who have historically held office in India.

Brexit

The United Kingdom's shift in policy towards exiting the European Union came on the heels of a national referendum on the decision in the summer of 2016. While there had been some supporters of leaving the European Union, the national referendum provided anti-EU elements within the government a platform to begin advocating more voraciously for the United Kingdom's exit. Details regarding the United Kingdom's exit from the European Union are becoming increasingly uncertain, particularly in light of several failed attempts to pass a European Union exit deal through parliament, confidence votes for the prime minister, and several resignations. United Kingdom Prime Minister Theresa May has faced an uphill battle to secure a European Union exit deal satisfactory to all parties almost from the beginning, and her most recent defeat in parliament casts doubts on her ability to secure concessions from the European Union in renewed negotiations over a Brexit deal. The United Kingdom is due to exit the European Union on March 29, 2019 at 11:00 PM local time, and with this date approaching fast, the United Kingdom's immediate withdrawal from the EU customs union, which will trigger required customs inspections, border security checks, and new regulatory requirements increases the potential for chaos to erupt for trade and supply chains.

Much of the uncertainty surrounding this process is borne of disagreements over the details of the deal that May secured with the European Union in late 2018. Of particular concern is the "Irish backstop measure" included in the deal. The measure would require that Northern Ireland, part of the United Kingdom, remain in the European Union Customs Union. This, in theory, would prevent a "hard border" from arising between Northern Ireland and Ireland (an EU member, but not part of the UK). Ireland's economy is heavily dependent on trade, and the implementation of border checks and other security measures that would come with the United Kingdom's exit would significantly disrupt their trade. For companies engaged in trade with the United Kingdom, or based within the United Kingdom and trading elsewhere, significant uncertainties for companies and their supply chains remain.

Implications of a No-Deal Brexit

As noted, the United Kingdom is scheduled to leave the European Union on March 29 - this means that the United Kingdom will no longer be part of the European Union Customs Union. This creates several potential issues. For companies based or headquartered in the United Kingdom and conducting business with other EU countries (and elsewhere); and for companies who maintain facilities or a portion of their supply chains in the United Kingdom, and the European Union or elsewhere (e.g. United States): there exists potential for discrepancies to arise between licenses, registrations, registration requirements and other similar work authorizations currently held by companies post-Brexit. For example, a company currently registered in the United Kingdom who is authorized to work in the European Union may require an additional license to operate in the European Union after Brexit. For companies based in the United Kingdom and selling to the European Union market, the United Kingdom government has issued guidance on this issue. However, other companies may face potential disruption following a no-deal scenario. Supply chain services, such as freight forwarders, may face similar licensing and registration issues if operating across borders. The exit from the European Union customs union will likely result in increased security, customs checks, and inspections at border crossings and ports of entry between the United Kingdom and European Union countries. Some of these checks do not currently take place, which can shorten companies' lead times, resulting in shorter or faster lines at customs checkpoints. Sources indicate that some companies in certain sectors may therefore operate on a "just in time" schedule, rather than planning lead times to account for customs checks. Instituting these inspections will likely result in significant delays, as cargo trucks will face long wait times at borders. Food sector representatives in particular voiced concern over this, given that raw and finished food products have short shelf lives – highlighting that significant delays in wait times are likely to result in disruptions to food supply chains.

Experts have recommended that companies closely examine the structures of their current supply chains and their locations, registration, and license requirements (e.g. visas for truck drivers where necessary, bills of lading, import/export licenses) they are required to meet, and lead times for product assembly, to assess the potential impact of a no-deal Brexit on their operations. Moreover, while wait times at borders are likely to be longer than pre-Brexit wait times, the United Kingdom is a World Customs Organization member, meaning that, at least regarding physical security checks on cargo, the United Kingdom will likely not physically inspect every cargo shipment entering the territory. Rather, customs officials are more likely to employ a risk-based targeting system, selecting cargo shipments of concern for physical inspection.

United States – China Trade Dispute

Since the election of US President Donald Trump, the government has enacted policies seen as protectionist or nationalist across many sectors. President Trump has withdrawn the United States from the Paris Climate Agreement, the Joint Comprehensive Plan of Action governing Iran's civilian nuclear program, and taken several steps to curtail immigration from certain nations. The United States approached the World Trade Organization in April of 2018 alleging China's theft of US intellectual property, with some estimates assessing that the United States loses as much as $600 billion per year in intellectual property theft to China. According to the Commission on the Theft of American Intellectual Property, while all industries are at risk, high technology sectors such as the semiconductor industry, biotechnology, and next-generation information technology are at particularly high risk of exploitation. In late 2018, the United States government began imposing tariffs on goods imported from China, and recently announced its intention to increase tariffs from 10% to 25% on approximately $200 billion worth of goods. The United States and China continue to hold dialogues to address the trade dispute and explore options for finding a mutually agreeable solution; however, the dispute is likely to continue in 2019.

The tariffs imposed on Chinese goods is one of several protectionist policies implemented under the Trump administration. From the United States perspective, the alleged purpose of these tariffs is to create a balanced field between the United States and China in trade matters, and to address related issues such as intellectual property protection.

Potential Trade Implications

Continued tariff increases will likely increase costs for companies sourcing from China. In some cases, this has prompted companies to look to other Southeast Asian countries to source materials or relocate segments of their supply chain. However, operators should also take steps to weigh the costs of tariffs on Chinese-imported goods against the potential for increased risks to their supply chains in other Southeast Asian countries. For example, companies should ensure that they are fully aware of the increased exposure to the risks of child labor, forced labor, supply chain corruption, and natural disasters, for example, as each of these risks are prevalent in other Southeast Asian countries. Furthermore, companies should also consider the customs procedures of the prospective country; in some cases, a country may have more lax customs procedures or a higher risk of corruption, increasing the risk to cargo in alternative ways such as illegal drug introduction, theft, and stowaway introduction. If the trade disputes between the US and China are not resolved, we can expect an increase in companies moving their bases from China to other Southeast, South, or even Central Asian countries with similar industrial or labor capacity.

Some experts have assessed that the US-China trade dispute will result in an increase in trade between the US and other countries as the US and China decrease trading with one another. While this could result in positives for certain nations, particularly those whose economies are heavily trade-dependent, there exists potential for disruptions. For example, as mentioned previously, in countries where customs procedures are less mature or where officials are not accustomed to high volumes of trade, an increase in exporting could lead to higher risks. Security risks may be higher in cases where procedures are not adequate to prevent theft, stowaway or drug introduction, illegal arms introduction, etc. For countries whose customs systems are not accustomed to handling influxes in imports or exports, there may be significant delays or disruptions at border checkpoints, ports, and air freight centers.

Newly-Elected Presidents in Latin American Countries to Bring Potential Supply Chain Challenges

Mexico

Mexico's president, Andrés Manuel López Obrador, and his National Regeneration Movement (MORENA) party were sworn in on December 1, 2018. He has proposed initiatives aimed at addressing longstanding security challenges in the country, including organized crime, illegal oil thefts and pipeline tapping, and corruption. The first initiative, Obrador's National Plan for Peace and Security, aims to address organized crime through the creation of a national guard. The second initiative, aimed at tackling corruption in the country, aims to pardon past crimes committed by corrupt officials in exchange for ceasing corrupt practices. However, there are significant concerns against his decision to resist having an anti-corruption prosecutor. Despite Obrador's anti-corruption and security-focused rhetoric, BSI expects that security challenges will continue to affect businesses in the coming year, in particular in-transit cargo theft.

The implementation of a national guard required approval in the senate, as well as constitutional amendments to bring different elements of the armed forces together. Additionally, rather than a new approach to addressing these issues, the plan is similar to the existing security strategy, and the "militarized" approach to fighting organized crime which originally began in 2006, though this new approach is focused more heavily on a federal strategy rather than one led by state or municipal governments. Other security challenges identified as likely to continue in 2019 include the theft of oil and the act of pipeline tapping, particularly in states such as Guanajuato, Puebla, and Veracruz, which has serious consequences on the wider security environment for those operating in these states.

In January, a gasoline pipeline explosion in Hidalgo killed at least 91 people and injured many more. The explosion will likely spur increased government efforts to target corruption - particularly at high levels, which plague the country's state-owned petroleum company (whose credit rating was recently downgraded by Fitch. While the cause has not been definitively determined, officials from the state-owned oil company stated that the illegal tapping of the pipeline may have contributed. As such, the government is likely to increase its efforts to combat the illegal tapping of gas pipelines, as well as corruption within the state-owned company that may contribute to or facilitate such activities. While the strategy targeting corruption and oil theft is still developing, there are mixed signals on its successes thus far. There has been an observable decrease in thefts, according to official figures; however, cities where refineries are located, such as Salamanca in Guanajuato, are experiencing high levels of violence with record homicide rates. Where violence is connected to cartels and other organized crime, it is possible that increases in violence will affect cargo security and business continuity.

There are several steps businesses operating in Mexico can take to mitigate the risks of these issues in the country. More so than monitoring the overall situation at the state-level, BSI recommends that businesses ensure they are adequately monitoring their business partners located on the ground in Mexico and understand the complexity of risks they are facing in their local operating environment. This should ensure that targeted support is available where necessary to improve supply chain resiliency. Additionally, companies should ensure that they conduct risk lane analysis, identify and understand localized route risks, and have plans in place to ensure business continuity in instances where security issues, strikes, and other situations threaten to disrupt said continuity.

Brazil

One of the most dramatic swings in political ideology last year occurred in Brazil, where the new administration began to implement policies diametric to those in force. Brazil's new president, Jair Bolsonaro, took office in January 2019, after having represented Rio de Janeiro in the Chamber of Deputies from 1991 through 2018. During his campaign, the retired military officer made numerous claims that drew public criticism, including derogatory comments towards minority groups in Brazil, support for loosening firearms regulations, and statements that some construed as tolerant or even accepting of sexual assault. Thus far, Bolsonaro has enacted executive orders impacting the rights of minority groups in Brazil indicating the potential for disruption to supply chains in Brazil in the areas of corporate social responsibility and business continuity. Additionally, the looming uncertainty over pension reform under Bolsonaro is likely to dominate his first year in office.

One of Boslonaro's controversial executive orders transfers the responsibility of identifying indigenous territories from the Ministry of Justice to the Ministry of Agriculture, which is led by Tereza Cristina, a member of the agribusiness caucus which previously opposed land requests made by native communities. There is potential for this policy to contribute to deforestation, negatively impacting environmental issues in the country. Bolsonaro supports the agribusiness sector in Brazil, and some experts have noted that illegal loggers in the country have increased their illegal deforestation operations in sections of the Amazon during his campaign and the first month of his presidency. According to one non-governmental organization focused on environmental issues, illegal deforestation rates tripled during the last few months of Bolsonaro's campaign.

A second executive order removed Lesbian, Gay, Bisexual, and Transgender (LGBT) issues from the list of responsibilities of the Human Rights Ministry, but has thus far not reassigned the issues to another agency. BSI has previously identified the likelihood of this leaving the LGBT community in Brazil vulnerable to discrimination within the country. This vulnerability has the potential to expose companies to higher reputational risks if they are unaware of such discrimination within their supply chains.

Bolsonaro has also taken steps to loosen regulations to access firearms in order for citizens to better defend themselves. However, this will likely fuel violence and social unrest, particularly due to the tensions between various social factions in Brazil, as observed in the state of Ceara's increased levels of violence. There is potential for increases in social violence and/or civil unrest to lead to disruptions in business continuity, particularly if groups stage mass demonstrations or begin to target supply chains either for theft, amid the challenging economic climate, or targeted against elements of the security forces.

Operators located in or doing business with partners in Brazil should remain aware of the potential for these and future policies to impact their supply chains' corporate social responsibility. The human rights situation in Brazil has, according to some metrics, been on the decline for the past several years, and it is possible that the presidency of Bolsonaro will contribute to the worsening of these conditions in the country. BSI recommends that companies mitigate their exposure to corporate social responsibility risks by taking a more active role in performing due diligence on business partners located in Brazil in order to fill potential gaps left by the government's removal of some regulatory requirements. As these conditions worsen, companies should also consider the potential for unrest to occur, particularly in the form of demonstrations, protests, and strikes which could impact business continuity in the country, either directly or indirectly.

India

Given recent shifts in politics around the globe, it is clear that these political events have implications for supply chains worldwide and have the potential to affect other countries looking forward into 2019. Facing national general elections in April and May, India represents another country in which we may observe a shift in politics with subsequent effects on supply chains. While Indian Prime Minister Modi is not the first right-wing politician to hold the office of Prime Minister, of India's 14 Prime Ministers, only two have been right-wing. Nine, on the other hand, have been center-left party representatives. Given the close temporal proximity to India's national elections, it is possible that the backlash to Modi's policies from many of India's working class will lead to a shift to a left-leaning political party. There is also the potential, in the interim, for the government to pass further policies that India's workers see as harmful to their interests, sparking new protests against the government.

It is also possible that the government will face renewed protests across India in the lead-up to national elections. While workers have expressed their dislike of many recent policies, the upcoming national elections have the potential to inspire individuals or groups, particularly those that feel a sense of deprivation or who feel that government policies unfairly impact their lives, to stage demonstrations to express their discontent. This carries with it the potential to inspire others to demonstrate, or to encourage voters to elect a national government with different political leanings from the current one.

Overall, the political and human rights situation in India appear to be experiencing improvement relative to previous years. However, in 2018, India experienced protests following increases in fuel prices as well as perceived inaction on the part of the government to address the problem. Following the protests, which were originally called for by the main political opposition party, the government loosened fuel import regulations. The regulation stipulated that Indian companies transport and insure imported fuel, and loosening the regulation appears to have reduced the occurrence of strikes over fuel. Following the strike, the government loosened regulations on fuel taxes which BSI assessed is likely to reduce the risk of future strikes over fuel taxes.

Representatives and affiliates of the International Trade Union Confederation (ITUC) in January of 2019 called for a nationwide strike ahead of India's national elections planned for April and May. The strike will be aimed at low wages, but representatives of the ITUC have also publicly stated that the government has issued policies designed to discourage or prohibit collective bargaining and otherwise damage workers' rights in the country. Similar sources also alleged that many of India's workers perform informal work and contend that collective bargaining is necessary to ensure and protect their rights. However, the government, according to the representatives of ITUC, does not support such actions.

Will 2019 Finally be the Year of Growth in Africa?

Africa is often considered to be one of the last few markets left untapped in the world, a prime location for manufacturing and other business in general to expand. Although the identification of Africa as a major frontier has been made repeatedly over the course of the last several years, businesses have yet to truly make any headway in cracking the untapped potential of the continent. Several recent factors, however, have the potential to finally fulfill the prophecy of explosive development in Africa.

From a geopolitical perspective, China and Russia have been steadily increasing influence in Africa, a fact that the United States government has noted and decided to counter by enacting the Better Utilization of Investment Leading to Development (BUILD Act), which will almost certainly lead to increased investment in the region. Other global issues, specifically the trade dispute between the United States and China, has spurred companies to relocate supply chains to more cost-efficient locations.

Although other countries in Asia are appealing alternatives to a degree, surging wages and persistent human rights challenges may lead companies to instead bypass these nations for the even more cost-effective Africa. However, companies that begin to move operations to Africa must be wary of risks not typically encountered in supply chains traditionally based in Asia, challenging both security, business continuity, and corporate social responsibility professionals.

The Global Conditions Promoting Growth in Africa

Business expansion in Africa is not going to be an overnight phenomenon; however, geopolitical issues including a renewed sense of combatting growing Chinese and Russian influence in Africa by the United States combined with the trade dispute between the United States and China have the potential to spur companies to more rapidly enter African markets.

Geopolitics Driving Foreign Investment in Africa

Both China and Russia have been steadily increasing influence in Africa the last several years, which has pushed the United States to counter in a way that is likely to increase the appeal of the region for private sector investment. China continues to execute its Belt and Road Initiative, a term used to describe the Asian country's set of massive, multibillion dollar investments, in countries around the world. Beginning around 2013 and spanning about 70 countries, the bulk of China's investment surge is concentrated in Africa and generally takes the form of infrastructure projects. The Chinese government continues to issue loans to countries around the world as part of a strategy to not only bolster local interests but also as a form of so-called "debt-trap diplomacy," a term used to describe the fact that many of these countries are failing to make payments to China for issued loans. The current hypothesis is that the Chinese government is intentionally issuing risky loans to countries knowing full well that it can then leverage these debts to exert geopolitical influence.

The Security and Business Continuity Risks of China's Belt and Road Initiative

While the majority of countries taking part in China's BRI projects may have initially welcomed the massive loans that come without the number of conditions typically applied by the International Monetary Fund, governments and particularly citizens of some countries have grown to realize the potential impact of these projects, creating both security and business continuity risks to supply chains. Malaysia is perhaps the most recent example of this about face in regards to Chinese investment, with the country's government announcing the cancelation of a $20 billion rail project. Elsewhere, countries with historic animosity toward China, such as Vietnam, have seen anti-China protests take place after announced investments. In Vietnam in particular last year, protestors vandalized factories that were perceived to be owned by Chinese companies. Protestors in the country only made this determination based on the

language of company signs and, in the process, mistakenly targeted facilities owned by Taiwanese, South Korean, Japanese, and Singaporean companies due to similarities in the appearance of languages, disabling some factories for several weeks.

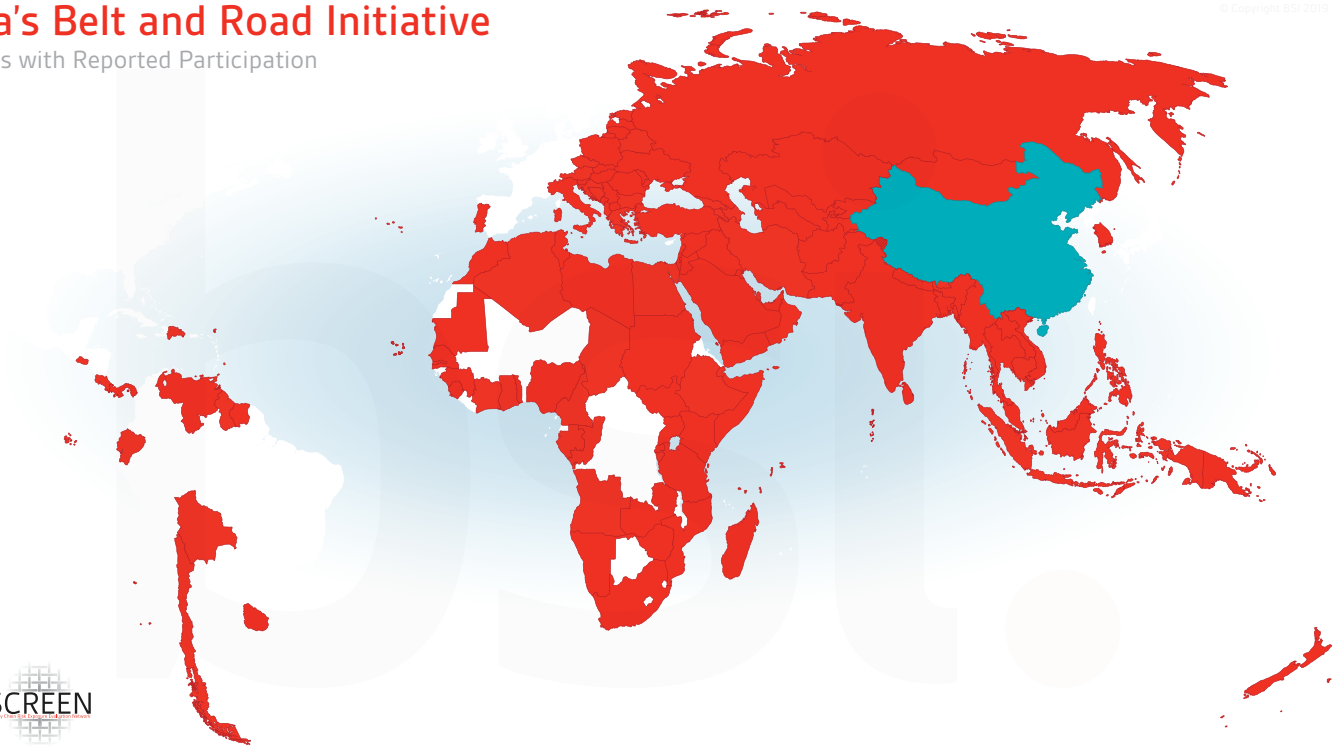
Not all of the risks relating to China's BRI are business continuity in nature, with a major attack on China's consulate in Pakistan late last year demonstrating the potential, albeit likely peripheral, security risks to supply chains in BRI countries. Seaport acquisition and development has been a key component of China's Belt and Road Initiative, with maritime shipping lanes essentially making up the Road portion of the country's strategy. Over the past year, Chinese companies have closed a significant number of deals for either purchasing controlling stakes in major seaports or beginning construction for new facilities such as a deep water seaport in Gwadar, located in Baluchistan, Pakistan.

Besides having a significant amount of mineral and natural gas reserves, Baluchistan is also home to the Baloch Liberation Army, a separatist insurgent group that led terrorist groups around the world for carrying out the most supply chain terrorist attacks in the past several years. In November of last year, several BLA members attempted to assault the Chinese consulate in Karachi, resulting in several deaths to Pakistani security forces responding to the attack. In response, Pakistani forces increased security around the Chinese personnel operating Gwadar port.

This attack highlights the potential for similar incidents to occur around the world wherever China has built a strong presence. Groups opposed to growing Chinese influence may carry out attacks targeting Chinese-owned companies or infrastructure, which may impact supply chains using such facilities. Attacks of this nature could also lead to secondary business continuity risks should security increase at Chinese-owned facilities, such as major seaports

China's Belt and Road Initiative

Countries with Reported Participation



Russia is similarly making inroads into Africa, albeit on a smaller scale and through different means. The Russian government has also been steadily increasing its influence in the region by signing more formal military agreements with a host of African countries in addition to providing informal military assistance to countries like Sudan and the Central African Republic, all while still maintaining some financial investment. Much like China's Belt and Road Initiative, Russia appears to be spreading its influence to Africa as both a means of establishing a presence outside of the homeland but also to secure sources of critical minerals and other natural resources.

Noting the actions of China and Russia in Africa and seeking a way to counter the two nations' growing influence, the United States government enacted the Better Utilization of Investment Leading to Development (BUILD Act). Enacted on October 5 of last year, the BUILD Act will create a new agency tasked with directing U.S. foreign investment for projects such as energy, ports, and water infrastructure. By doing so, the U.S. government hopes crowding-in private investment will support developing countries, expanding economies and increasing political ties. In more general terms, the new piece of legislation will likely act as a catalyst for private sector investment in Africa as a means of countering Chinese and Russian influence.

U.S.-China Trade Dispute Accelerating Supply Chain Relocation From China

The ongoing trade dispute between the United States and China is arguably accelerating the relocation, or at least the consideration of relocating, supply chains to more profitable countries. Wages in China have been steadily rising over the last several years, and the current trade situation with the United States has not made doing business in China any more affordable. As a result, companies are beginning to seek alternative locations for manufacturing operations. Although the most logical location to house primary manufacturing operations would be another country in Asia due in part to the proximity to China, which would likely remain a key source for inputs. However, wages across other major Asian countries have similarly been increasing, quickly elevating the appeal of African nations as an even more affordable location for manufacturing.

Wages have risen dramatically throughout Asia, with major increases recorded in China in particular. As a region, Eastern Asia has seen a 53 percent increase in real wages between 2008 and 2017. For the same time period, Southeast Asia recorded a 31 percent real wage growth while South Asia saw 36 percent growth. Much of the wage growth in Asia has been driven by worker protests, particularly last year where BSI recorded labor strikes in major manufacturing countries including Bangladesh, India, South Korea, and Cambodia. The demand for wage increases by workers in Asia adds another reason for why companies may look elsewhere to relocate manufacturing operations.

In contrast, North Africa saw only 13 percent real wage growth between 2008 and 2017, and only 14 percent growth in Sub-Saharan Africa. It is this discrepancy in wage growth combined with the likely incentive of the BUILD Act that could lead companies looking to relocate from China to bypass other traditional manufacturing hubs in the region for the more affordable Africa.

Trade Benefits to Also Potentially Spur Relocation to Africa

One country that has already seen an influx in relocated manufacturing is Egypt, with Chinese apparel manufacturers reportedly setting up facilities in the African country in order to avoid U.S. tariffs and also exploit the trade benefits of being located in a Qualifying Industrial Zone. Reports from last year indicated that Chinese companies are attracted to Egypt not only for its shorter shipping times to both the United States and Europe as well as its much lower wages, but also because the country is a part of the Qualifying Industrial Zones program. Under this program, which was established by the United States in 1996, companies that source at least 10.5 percent of a product from Israel can then finish production in Egypt and enjoy tax exemptions from the United States ranging between five and 40 percent. Other free trade agreements that Egypt have signed further strengthens the country's appeal as an alternative destination for manufacturing.

New Location, New Risks?

Shifting manufacturing operations to Africa may be more cost-effective compared to staying in China or choosing another Asian country, but relocating would also incur different challenges for supply chain professionals, with significant and often interconnected security, business continuity, and corporate social responsibility risks all posing a threat.

Security

Supply chains relocating to Africa would have to contend with a wide range of security risks, including cargo theft and smuggling, often compounded by rampant corruption found among security and customs personnel in many countries. Although both of these risks can be found in most Asian countries as well, it is the relatively unchecked risk of terrorism in Africa that sets the operational environment apart from that of Asia.

In 2018, BSI recorded cargo theft incidents in Africa that often involved hijackings of cargo trucks or thefts from relatively unsecure facilities, suggesting an overall lower level of standard security practices may need to be significantly augmented. In addition, corrupt security and customs personnel are known to at a minimum frequently request bribes and often participate in theft schemes outright.

Besides the risk of cargo theft, BSI also noted an increasing threat of smuggling in several countries in Africa last year as traffickers increasingly use the region as a transshipment point for illegal drugs or seek to take advantage of low-level conflicts and the subsequent markets for illicit weapons. African countries situated along the western and northern coasts in particular have become frequent transshipment points for Latin American illegal drugs intended for European markets, highlighting the need for maintaining container integrity protocols.

It is the risk of terrorism in Africa, however, that sets the region apart from that of Asia, where terrorism may occur but in a more limited form than that witnessed in part of the African continent. Countries in Africa account for approximately 23 percent of all supply chain terrorist attacks in the world, underscoring the risk to business operations in the region. With multiple major terrorist groups operating in Africa and a largely insufficient capacity to combat, the potential exists for supply chains to be disrupted, used to carry out, or targeted by attacks.

Corporate Social Responsibility

From a corporate social responsibility perspective, the economic conditions combined with the lack of inspection and enforcement capacity in many African countries increases the chance that labor violations will occur. However, the core labor rights risks present in Africa do not widely vary from those that occur in Asia countries; child labor, forced labor, discrimination, and poor working conditions are risks to supply chains whether in Africa or in Asia.

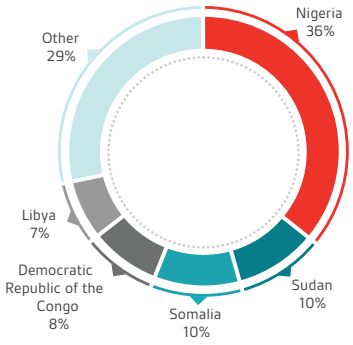
What differentiates the risk in Africa in comparison to Asia is the frequent turnover of political regimes in many countries, which could stymy efforts to provide consistent worker health and safety protections. Widespread corruption is also another factor that can hinder the enforcement of human rights protections in Africa.

Business Continuity

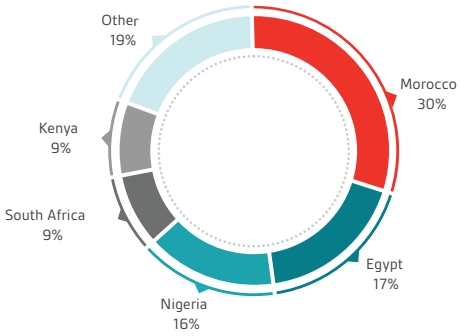
Although Africa largely does not have the same type of exposure to natural disasters that Asia does, the extant risk of man-made disruption has the potential to disrupt supply chains in a similar manner. Deficiencies in road, rail, and seaport infrastructure often create significant delays to shipments in the region, while other extraneous factors including low-level conflict, inefficient practices and technology, and bribery and corruption further contribute to man-made disruption to supply chains in Africa.

No matter the location of manufacturing, supply chain operations will face some sort of risk. It is therefore critical to understand not only the current risks in an area of operation, but also to remain informed of any new challenges that might arise in the ever-changing world. Knowledge of these risks will then allow for appropriate mitigation strategies to be instituted.

Top African Countries for Supply Chain Terrorist Attacks



Top African Countries for Smuggling Incidents 2018

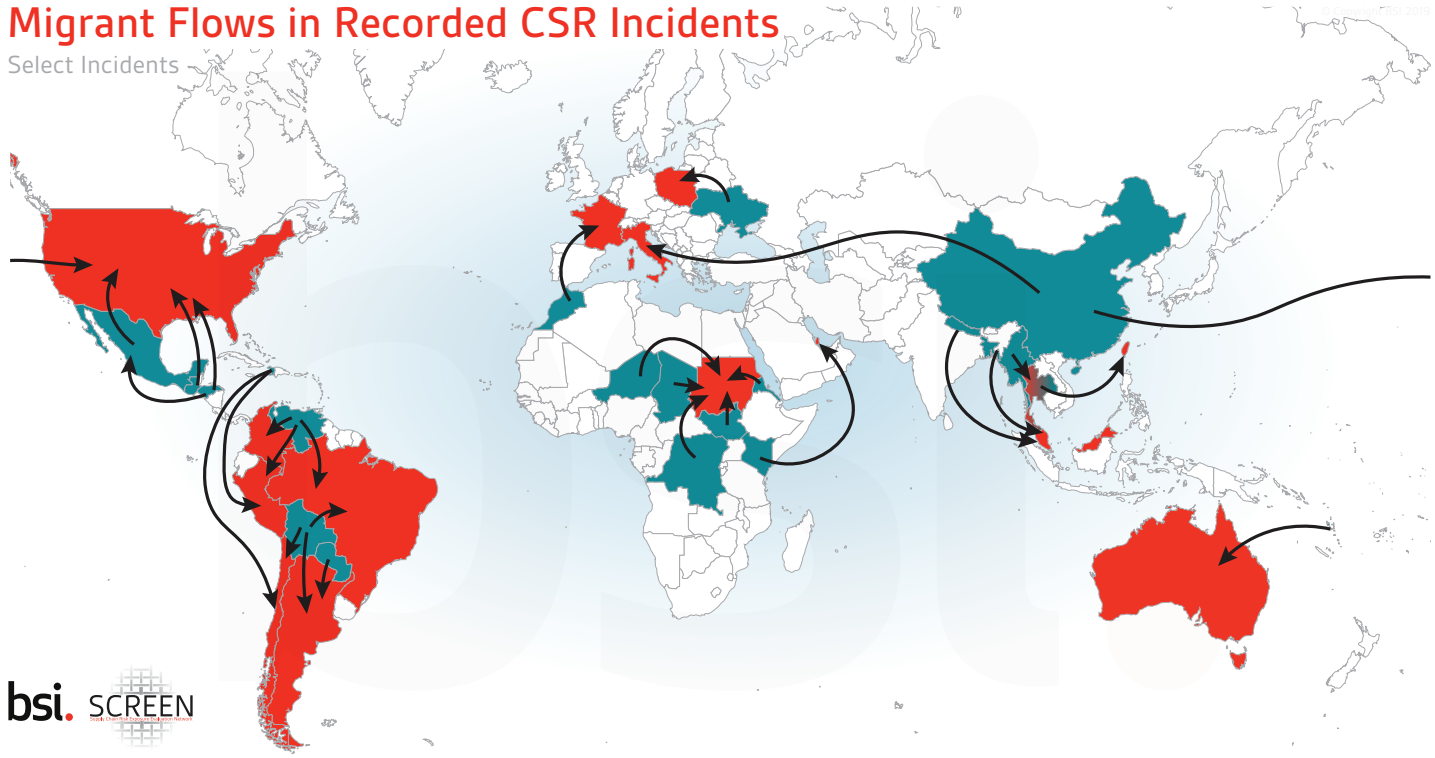


Ongoing Mass Migration to Continue to Pose Security and Corporate Social Responsibility Risks

Conflict and both political and economic conditions continue to drive mass migration around the world, presenting supply chains with the double-edged challenge of countering security and corporate social responsibility risks. In 2018, BSI noted an increase in stowaway and labor exploitation risks stemming from migrants traveling along three major flows: Central to North America, Intra Southeast Asia, and Africa and the Middle East to Europe. Despite the upcoming adoption of anti-slavery legislation in several countries this year and continued pressure to maintain supply chains free of labor rights abuses, it is very likely that ongoing mass migration will continue to pose a risk to companies in 2019.

Security Risks

Stowaways remain a threat to supply chains around the world, with domestic pressures, whether it be conflict, political, or economic, driving migration worldwide. There are three main flows of migrants that BSI has noted for an increased risk of stowaways last year that are likely to continue to pose similar challenges throughout 2019, as the many conditions spurring these mass migrations are not likely to be rectified in a short amount of time. These migratory flows include Central to North America, intra-Southeast Asia, and Africa and the Middle East to Europe.

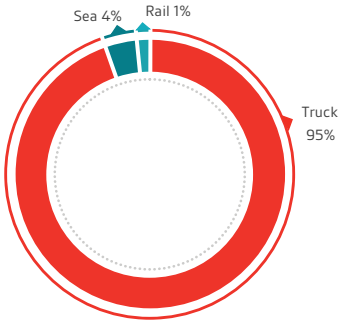


BSI has noted that migrants continue to perceive supply chain transportation modalities, particularly the trucking modality, as a successful means of entering their intended destination countries. As a result, migrants around the world targeted cargo trucks over any other transportation modality in 2018, including sea and air transportation. Beyond the perception of being relatively more comfortable means of travel, the use of cargo trucks by stowaways is a trend that can be explained primarily by the global flows migrants and the typical level of security inherent to each transportation modality.

It is easier for migrants to stowaway in one of the thousands of cargo trucks that head for the preferred destination country than it is to identify an appropriate air or sea shipment and then attempt to infiltrate several additional layers of security or employees in order to accomplish the same introduction. The vast number of cargo truck shipments entering a country also lessens the chance that customs inspections will detect stowaways.

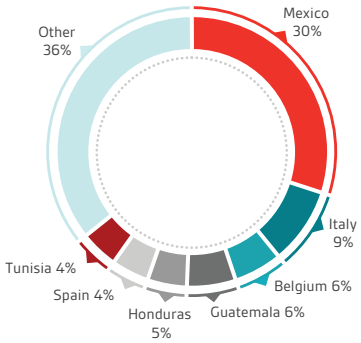
Additional analysis of stowaway incidents collected by BSI last year revealed a higher frequency of compromised food and beverage shipments compared to other industries. However, it does not appear that migrants around the world are specifically targeting these shipments due to the product type. Instead, it is likely the combination of a higher volume of food and beverage shipments and a generally lower level of security that is responsible for the high rate of stowaways.

Modality in Recorded Stowaway Incidents 2018



It is more likely that poor security practices, and not supply chain corruption or organized crime, is contributing most to the risk of stowaway introduction into cargo in Europe. According to data collected by BSI in 2018, most incidents of stowaway introduction into cargo in Europe involved the discovery of between one and five (33 percent of incidents) and six and ten stowaways (32 percent of incidents). Incidents involving more than ten stowaways made up the remaining incidents of stowaway introduction. This data, along with inherent security risks of the European cargo truck industry including insecure soft-sided trailers and a lack of secure parking locations, suggests that most cases of stowaway introduction in Europe do not involve insider participation. It is more likely that these instances of stowaway introduction are the result of migrants exploiting weaknesses in security practices rather than corruption in the supply chain. However, the possibility for insider participation still remains. According to BSI data, most stowaways entering the supply chain in Europe are destined for countries such as the United Kingdom, France, and Belgium.

Origin of Stowaways 2018



In order to mitigate the risk of stowaways, companies should keep abreast of current migratory flows in order to gain an understanding of risk exposure and ensure that supply chains have appropriate levels of security. Incorporating geographic risk intelligence, including knowledge of the most frequently exposed transportation modalities and commodities in a location, can provide companies insight into the overall exposure of their supply chain to the risk of stowaways breaching shipments. After assessing a supply chain's level of exposure, companies can then implement many of the same security measures used to combat more general types of smuggling. These measures can include avoiding stopping in insecure locations, or utilizing team drivers to ensure that containerized shipments are not idling for an unnecessary amount of time. Following strict container integrity protocols can also ensure that stowaways cannot easily access the cargo hold. Lastly, conducting background checks on drivers and any other individual that may touch the supply chain can help to mitigate the chance that corrupt employees would allow migrants to access cargo shipments.

Corporate Social Responsibility Risks

One theme that BSI continues to note in collected incidents of labor violations is the exposure of migrants to such offenses. Approximately half of all corporate social responsibility (CSR) incidents recorded by BSI last year involved migrants. As conflict and political or economic conditions continue to drive migration around the world, the often desperate need to earn an income to support their family leads many of these vulnerable individuals to situations in which they are exploited for labor.

BSI has noted several geographical factors that can be used to assess the risk that migrant labor exploitation will be used in legitimate supply chains. The obvious factor is whether a country has a large population of migrants or lies along one of the primary migration routes. BSI has determined that economic and civil unrest in neighboring regions is frequently associated with informal or unlicensed recruitment and employment of migrants. Another influential factor is the absence of legal protections and official citizenship status for migrants in host countries, which can prevent victims from lodging complaints through official channels. BSI has also noted a higher frequency of abusive employers in these instances withholding official identification documents that essentially holds migrants hostage in fear of being prosecuted for illegal entry.

Some countries around the world have noted the increasing risks to migrants in the workforce, and labor exploitation in general, and have either enacted or are formulating new legislation to combat the issue. The Qatari government, for example, lifted a provision that previously required migrant laborers to obtain permission from their employers before being allowed to leave the country. Elsewhere, Australia passed its own Modern Slavery Act while Canada iterated a commitment to creating similar legislation.

However, BSI has noted regression in other countries that could increase the risk of migrant labor exploitation. Brazil is one such country, where budget cuts are jeopardizing significant progress in combatting issues like forced labor by resulting in less resources available to carry out inspections. The Brazilian government also attempted to change the legal definition of forced labor to a more generalized statement that would have likely prevented authorities from rescuing some victims as they were no longer in situations legally classified.

Although the above geographical risk factors are important to understand and can be used to assess the potential for migrant labor exploitation within a supply chain, it will also take a thorough understanding of the supply chain to truly assess the risk of migrant laborer exploitation. For example, most cases of migrant labor exploitation that BSI has recorded involved unskilled work like agriculture or apparel manufacturing, a fact that can indicate whether a company or business partner faces potential exposure.

Migrant Workers in BSI-Recorded CSR Incidents 2018

Other factors such as the maturity of supplier practices and whether or not the business partner works with recruitment agencies may also indicate a certain level of risk. In particular, when it comes to migrant labor, there is a very strong possibility that multinational companies with large global supply chains are working with migrant workers subject to fees or debts by recruiters. Recruitment agencies frequently charge workers exorbitant costs and fees in the form of loans that are paid off by workers over the course of their employment contract. These debts can take months or years to repay, trapping these workers in a form of debt bondage. In many cases, companies do not have any means of engaging these recruitment agencies except potentially through a business partner, creating a significant challenge for implementing systematic, large-scale methods of managing these risks.

Mapping out a supply chain in itself is no simple undertaking, but it is a critical step in managing the risk of migrant labor exploitation. Other methods such as supplier training and transitioning business partners into a recruitment model in which an employer pays the associated fees can also help combat the risk of migrant labor exploitation, an issue that BSI believes will likely remain a key issue for supply chains in 2019.

Supply Chain Security: The Nexus of Physical Security, Cybersecurity, and the Human Factor

In recent years, cybersecurity has become an issue of growing interest in nearly all sectors. Cybersecurity cuts across all sectors, all levels of a company, and it is unlikely that the issue is going to fade in importance any time soon. On the contrary, it is likely that cybersecurity will become an issue of increasing attention in 2019, particularly with regards to supply chain security. While cybersecurity has drawn considerable attention as what seems to be a new dimension of security, it merely highlights the deep connections between physical security, the security of networked systems, and the human factor. A vulnerability in one of these dimensions necessarily creates vulnerabilities in the other two. Complex, global supply chains involving multiple business partners multiply these potential risks and vulnerabilities.

Physical Security

Much of the focus of cybersecurity is devoted to network security and is based in the digital realm. However, the cyber world and physical world are interconnected, and this has important implications for all sectors, including supply chain. In addition to security in the cyber world, companies and governments should also be concerned with the physical security protecting their networked devices, data centers, and other facilities such as ports.

The physical security of networked or internet-connected devices can have important ramifications for supply chains if not held to a high standard. Poor security of such devices creates a vulnerability which malicious actors will likely locate and exploit, whether gaining access to logistical information, personally identifiable information of employs or clients, or other data important to companies. In addition, many companies consider their data to be as important as their product in many instances- and should therefore take measures to ensure that their data centers and other locations important for IT systems are physically secured. A lapse in physical security could allow a malicious actor to gain access to the even the most digitally-secured facility.

In addition to internet-connected devices and data storage facilities, other venues such as ports are also at risk of a cybersecurity breach as the result of a vulnerability in physical security. In one case, a criminal group involved in smuggling cocaine was able to exploit lax physical security at port facilities in Antwerp, Belgium and install software allowing them to track shipments containing cocaine.

The Human Factor

Similar to physical security, the human factor in cybersecurity can lead to glaring vulnerabilities in the overall security of supply chains. The human factor can contribute to vulnerabilities through a lack of general awareness of common risks, insider threats, and social engineering. For example, poor training of all employees- not just IT or security-related employees- in basic cyber and information technology security measures such as phishing emails can lead to the loss of important data. Employees, particularly highly-placed or well-known employees, can be vulnerable to more targeted attempts to gain information or access through spear phishing attempts which are geared more directly towards a certain individual.

Insider threats, another potential vulnerability in the human-cyber-supply chain nexus, can come from a several sources, whether a malicious actor within a company or facility, or an unwitting participant. Malicious insider threats can take different forms, such as someone who seeks employment specifically to exploit their access, someone currently employed who has been recruited by an outside malicious actor because of their access, or even a disgruntled ex-employee. In the past, BSI has recorded incidents of warehouse or other facility employees exploiting their access to facilities and/or knowledge of procedures. Cyber adds a new dimension to this in that, as discussed above, physical vulnerabilities can cause cyber vulnerabilities. Those with the necessary access can abuse their privilege by stealing important data on clients or other sensitive information, or they can access logistical data in order to facilitate a theft of cargo or supply chain terrorism, for example.

Disgruntled (ex-) employees can create another vulnerability in the system. There have been well-documented incidents of recently-fired employees retaining access to certain facilities or systems after having been fired, either due to oversight or due to slow procedures. If ex-employees retain such access, particularly in an unsupervised setting, they could attempt taking revenge through stealing data or otherwise exploiting their privileged access to systems. Another issue regarding insider threats, discussed further below, are those that are unwitting participants to such occurrences. One example would be an employee who is not well versed in the basics of cyber and IT security, and falls prey to a phishing email.

Finally, humans working in relevant organizations can be particularly vulnerable to social engineering attempts. Malicious individuals wishing to gain access can be excellent manipulators, playing on another person's willingness to help, moral values, etc. in order to gain access to an otherwise inaccessible area. For example, one professional penetration tester was able to implant malware on a company's computers without ever needing to access the computer himself; he simply posed as someone on their way to a job interview and whose suit and resume were ruined by spilled coffee. He asked the receptionist at the company to print him a new copy from his flash drive, after detailing his stressful morning and coffee-spill. The flash drive then planted the malware onto the company's computer system.

While many of these examples could be from any company in any sector, this does not lessen the importance of vigilance. All of these issues are ubiquitous, and all aspects of a company's supply chain face these risks and vulnerabilities. However, these issues may be particularly difficult for supply chain security managers. Not only must companies with complex global supply chains manage these vulnerabilities in their own companies; they must also worry about every business partner at every step in that supply chain and whether they adequately address these vulnerabilities as well.

The Private Sector, Government, and Geopolitics

Cybersecurity also exposes the link between the private sector, governments, and geopolitics. One of the biggest current examples is perhaps the theft of United States intellectual property (IP) by China, and others. The economic and technical dominance of the United States on the global stage is tied not only to actions taken by the government, but also by United States companies involved in a number of key sectors, such as electronics. The recently-proposed bill to establish an Office of Critical Technologies and Security, put forward by US Senators Marco Rubio and Mark Warner, calls necessary attention to this issue. Not solely the domain of cybersecurity, this particular issue cuts across cybersecurity, intellectual property, trade and economics, and national security. This area is one in which the effects of geopolitical events and relations between nations can be felt in the private sector, both in businesses engaged in national security-related work and those that are engaged in economically important sectors.

Countries in eastern Asia, for example, have long sought to overtake the United States technical primacy; China in particular has a history of stealing or attempting to steal important technical data and other information. According to the United States Defense Security Service, which conducts surveys of industry involved in classified government projects, the electronics industry is heavily targeted by actors in East Asia. Often these actors exploited commercial entities affiliated with their countries' militaries, and often employ tactics centered on cyber and human exploitation.

It is important to realize that, particularly in the cyber age, entities do not experience these threats and vulnerabilities in a vacuum; federal and state government entities are connected with private sector businesses, and often times regulatory entities are also involved. The deep interconnected nature of these entities means that a vulnerability in one is a vulnerability in the others as well. Private sector businesses, particularly those engaged in national security-related work, can create potential vulnerabilities for governments—after all, businesses involved in classified or cleared projects for government clients have their own supply chains involving webs of suppliers. This interconnectedness also demonstrates that geopolitics often involve more than government actors; for malicious actors (whether sponsored by a foreign government or acting independently), the private sector is a rich field of potential targets.

Policies to effectively mitigate these threats will necessarily require cooperation between all relevant actors; that is, federal and state governments, regulatory bodies, private sector businesses. The Rubio-Warner Senate bill seeks to address the vulnerabilities at this nexus of issues, and it will be increasingly important for governments globally to coordinate efforts not only between government entities (federal to federal, federal to state, state to federal, and state to state), but between government entities and the private sector.

Mitigation Measures and Conclusions

BSI has a number of recommendations for companies wishing to mitigate the risk these threats pose to their operations. Companies' supply risk assessments should necessarily include an assessment of cybersecurity risk, and companies should ask a number of related questions. How do vendors and manufacturers review hardware and software obtained from suppliers? What policies and procedures are in place should they receive counterfeits? These are issues that should be taken into consideration in the process of managing suppliers.

BSI also recommends that companies assess which of their suppliers hold the most data and how sensitive the data is, and schedule audits and assessments accordingly. That is, suppliers that hold large amounts of sensitive data should be audited regularly, and suppliers holding less sensitive data could receive less frequent audits. General data protection should also be on companies' minds, because security teams at companies tend to capture large amounts of data on individuals but do not generally track it well. BSI recommends that security teams be cognizant of: what type of information they collect (e.g. visitor names, employee information, CCTV footage), whether the data is collected for a clearly defined and necessary purpose, how long the data will be retained or stored, the privacy regulations in their country and whether they are conducting privacy impact analyses. Perhaps most importantly, are companies properly protecting the data that they gather on individuals with both physical measures as well as information compartmentalization procedures?

While the increasing ubiquity of cyber issues appears to be a new phenomenon—indeed, it does create new problems that require new solutions, it also serves to underscore the interconnectedness of physical security, the human factor, and the cyber domain. The complex and diffuse nature of modern global supply chains further complicates this issue, and means that companies and governments will need to pay acute attention to the minute details of their supply chains in order to anticipate and mitigate potential threats. The security of a supply chain, both physically and digitally, is only as strong as the weakest link in the chain. Determined, malicious actors are also creative; they may employ pretexts which seem legitimate, meaning companies should be aloof and ensure proper due diligence is performed. Finally, it is important to note that the introduction of cyber to supply chains does not render human threats obsolete; in fact, it creates a new vehicle for such threats.

Special Contributors

Ryan Lynch

Head of Advisory & Sustainable Supply Chains

Ryan Lynch works with organizations across multiple regions and industries to design creative solutions to drive organizational improvement and to identify, mitigate and remedy supply chain risk. He has designed Responsible Sourcing programs for multinational brands, and has conducted trainings & Code of Conduct audits in factories & farms throughout the U.S., China, Philippines, India, Pakistan, Vietnam, Nepal, Taiwan, Indonesia, El Salvador, Honduras, Guatemala & Turkey. Ryan leads BSI's strategy regarding ethical recruitment and combating migrant labor abuse, including the development and delivery of the Supply Chain Slavery Gap Assessment, the Supply Chain Trafficking & Slavery Patterns Index and innovative skills development and supplier improvement programs. Ryan is also a member of the US Customs & Border Protection Commercial Operational Advisory Committee on Forced Labor and the Advisory Board of the Rutgers University's Center for Innovation Education Design Thinking program.

Contact at Ryan.Lynch@bsigroup.com

Tony Pelli

Senior Supply Chain Risk Advisor

Tony is an experienced supply chain risk consultant with a broad range of specialized skill sets, including experience in conducting end-to-end, enterprise-level supply chain risk assessments for clients and their supply chain partners. Tony has led assessments where he models, quantifies, and mitigates the risk of cargo theft, counterfeiting, and other supply chain threats, and has assessed over $50 billion in trade in a wide range of industries over the past three years. Tony has designed loss prevention and physical security assessments, mapped and assessed security and business continuity risk in supply chains for Fortune 500 companies, and assisted in the design and implementation of supply chain security plans, policies, and procedures. Tony has a degree in History and International Affairs from the University of Georgia.

Contact at Tony.Pelli@bsigroup.com

Philippa Williams

Supply Chain Risk Advisor, Latin America

Philippa is a Supply Chain Risk Advisor with BSI Group based in Mexico City. She works with multinationals, governments and international organizations, providing bespoke risk management solutions across complex supply chains with significant security, social responsibility and business continuity challenges. Key areas of risk focus include developing anti-corruption and bribery programs across complex supply chains, supply chain security analysis and development of local/global programs, analyzing the introduction of illicit goods into supply chains and developing mitigation techniques for overall supply chain corruption. Philippa specifically focuses on security and social risk advisory work in Latin America and has worked on supply chain risk mapping and investigations throughout the region, with significant expertise in Mexico. She is a fluent Spanish speaker and holds an MA in Conflict, Security and Development from the War Studies Dept. at King's College London, a BA Hons from Trinity College Dublin.

Contact at Philippa.Williams@bsigroup.com

Kimberly Rodriguez

Supply Chain Risk Associate

Kimberly Rodriguez has focused her career in the business and human rights space, supporting the development of sustainable sourcing programs for companies across multiple industries. She has experience conducting current state analyses of sustainability and human rights programs in the private sector, benchmarking assessments against customer requirements and industry peers, and developing and delivering awareness trainings on corporate responsibility risks such as modern slavery and human trafficking. She has also led an international team of auditors in conducting an onsite factory assessment of company practices surrounding the hiring and employment of migrant workers.

Kimberly has an MBA from the NYU Leonard N. Stern School of Business and a BA in Political Science from NYU Abu Dhabi.

Contact at Kimberly.Rodriguez@bsigroup.com

SCREEN
Supply Chain Risk Exposure Evaluation Network

SCREEN Intelligence

Supply Chain Risk Exposure Evaluation Network (SCREEN), is BSI's web-based, comprehensive global supply chain intelligence system. SCREEN is the most complete, publically available Supply Chain Security, Corporate Social Responsibility, and Business Continuity intelligence and analysis resource used to measure country level risk factors through BSI's 25 proprietary country level supply chain risk ratings. SCREEN's unique, proprietary global supply chain risk data and analysis helps organizations identify and understand where their supply chain risks exist. SCREEN generates trade interruption updates, BSI-authored special reports on major disruption incidents and trends, countermeasure programs, and risk mitigation best practices to help protect supply chains worldwide. SCREEN's intelligence provides organistaions with full transparency of country risks and helps them to make intelligent risk-based decisions that drive resilience.

Interactive Risk Maps

Each proprietary risk indicator is conveniently displayed for over 200 countries through SCREEN's global risk mapping views. For every indicator, a country is assigned a rating of Low, Guarded, Elevated, High, or Severe. This rating system allows users to quickly identify and categorize the threats to their supply chain and address them quickly.

Spotlight News

SCREEN's Spotlight News provides data and analysis on the most pressing global incidents on a daily basis. Each update encompasses a general summary of the incident and BSI's own analysis of the incident. The analysis provides the risk rating of the associated country and the explanation of the rating to help you better understand the country level threats and trends.

Automated Notifications

SCREEN provides users the ability to stay current and up to date with breaking news and changing conditions around the world that impact the integrity of their supply chain. Users are able to subscribe to the notifications for specific locations and subject areas that concern them the most.

Custom Report Builder

SCREEN's custom country report builder provides users with more control over the areas that are represented in the report. Users can easily pull and compare reports for multiple countries, threat assessments and commodities tagged throughout the SCREEN system instantly.

Additional Solutions and Services

Supplier Compliance Manager (SCM): BSI's automated self-assessment and audit analysis solution that quantifies and tracks supplier risk and compliance through various assessment methods to ensure your supply chain, brand and reputation are protected.

Training Services: Our customizable training services help develop a deeper understanding of supply chain security, corporate social responsibility and business continuity risks and how to quickly respond and proactively manage them.

Auditing Services: Our services provide organizations with complete visibility into their suppliers' practices and procedures worldwide. Our audits provide your organization cost-effective assurance that your suppliers are not exposing your brand.

Advisory Services: BSI's experienced risk management professionals leverage their knowledge and SCREEN intelligence to help organizations effectively identify, manage and mitigate risk and develop robust management programs.

bsi.

4150 Drinkwater Blvd. Ste 160, Scottsdale, AZ 85251
Tel: +1 480 421 5099
supplychain@bsigroup.com
bsigroup.com/supplychain