Western Michigan University

The Hilltop Review

Volume 9
Issue 1 *Fall*

Article 3

December 2016

The International Business Risk of Terrorism: A Pragmatic Framework for Assessing its Impact on the U.S.-Based, Small- to Medium-Sized Enterprise's Supply Chain Operations

Scott A. Lemons
Western Michigan University

Article 1

The International Business Risk of Terrorism: A Pragmatic Framework for Assessing its Impact on the U.S.-Based, Small- to Medium-Sized Enterprise's Supply Chain Operations

Scott Lemons
Haworth College of Business
scott.a.lemons@wmich.edu

Introduction

Fundamentally, the key to business success is superior efficiency and effectiveness relative to one's competitors. The globalization of markets—the ongoing integration and growing interdependency of countries worldwide (Cavusgil, Knight, & Riesenberger, 2017)—provides internationalizing firms the opportunity to augment efficiency and effectiveness via access to lower-cost inputs and new markets, among other factors. Rapid technological innovation—a significant enabler of globalization—has dramatically reduced the time required to transport physical

resources and to communicate information, thereby accelerating the internationalization of firms' value-chains. Major prospects exist to optimize use of inputs (i.e., efficiency) and increase sales growth (i.e., effectiveness).

Yet, the integrated, interdependent, global economies also expose firms to heightened risks. The firm must assess the various environments (e.g., economic, political, and cultural) worldwide across all of the countries or regions in which it operates, or is connected to, to identify what risks are relevant to its operations. The range of such risks is considerable; therefore, this subject paper focuses on a specific type of country risk: terrorism.

The business sector constitutes one of the primary strategic targets of contemporary terrorism because attacking it can cause severe and cascading economic damages to the targeted businesses (Sinai J. , 2016). Firms are vulnerable not only to attacks on their own assets, but also to attacks on their suppliers, customers, transportation providers, communication lines, and other elements in their eco-system (Sheffi, 2001). Essentially, the firm's integrated network of sourcing, production, and distribution, organized on a worldwide scale (Cavusgil, Knight, & Riesenberger, 2017), is especially vulnerable to the potential consequences of a terrorist attack. Accordingly, while the risk of terrorism precludes none of the firm's functional activities, particular attention is given to adverse implications for the firm's supply chain operations.

Literature Review

To provide a contextual basis for supply chain executives at U.S.-based, small- to medium-sized enterprises, a broad evaluation of contemporary commentary pertaining to country- and firm-level implications and corresponding approaches precedes a pragmatic risk assessment and mitigation planning framework. First, country-level considerations are assessed. Such considerations include adverse implications for the United States' economy, infrastructure, and national will. Subsequently, several country-level mitigation approaches are reviewed, including regulatory, diplomatic, and military approaches. The firm's understanding of country-level mitigation approaches is critical, not only to recognize the potential impact of political and legal environmental factors on the firm, but also to comprehend what role the firm may need to take in their application. Secondly, firm-level considerations are evaluated. In general, the firm-level adverse implications and mitigation approaches are more internally facing (i.e., pertaining to the firm's value-chain) than the country-level considerations. At the firm-level, logistical, supply network, and technological implications are of focus, followed by attention to the various strategic and operational risk mitigation approaches proposed by contemporaries.

Country-Level Considerations

Essentially, terrorists execute attacks by way of one or more of the following mediums: land, air, sea, or information technology. In the context of international business, the most concerning physical means is arguably an attack by sea. Nearly 80% of global trade is transported in ships' hulls

(Sakhuja, 2010). Accordingly, countries have invested significant resources in maritime infrastructure, containerized trade, energy supply chains, information technology-driven cargo movements and processes accelerating financial transactions in order to harness the benefits of globalization (Sakhuja, 2010). But, there are also associated risks: several studies of maritime security have identified vulnerability in the movement of oceangoing cargo in containers. Each transfer of a container from one party to the next is a point of vulnerability in the supply chain (Caldwell, 2008). Terrorists can target the container in two ways: (1) by tampering with a legitimate consignment, or (2) by assuming a legitimate trading identity and using it to ship a dangerous consignment (Marlow, 2010). The container could potentially be the Trojan horse for the terrorist (Traina D. J., 2010). Similarly, other physical means of an attack, by land or air, also present significant threats; however, contemporary literature suggests the global supply chain's foremost vulnerability to an attack via physical means is by sea.

Increasingly, terrorist groups are also utilizing information technology to carry out attacks. Terrorist groups and their supporters (as well as state sponsors of terrorism, such as Iran) now employ cyber weapons to inflict economic damage against their adversaries (Sinai J. , 2016). Potential targets include government agencies, stock exchanges, and other government and financial information systems. Further, not only are terrorist groups utilizing information technology to carry out cyber-attacks, they are also utilizing its offshoot of social media to spread propaganda. In effect, it has become increasingly unnecessary for terrorist groups to radicalize its adherents and sympathizers at physical sites around the world—arguably, a much easier prospect for counterterrorism units to regulate. Instead, propaganda spread via social media acts as a means to radicalize followers from a distance. In fact, a ten-year study found that approximately 90% of organized terrorism on the Internet is performed today through social media (Marcu & Balteanu, 2014). Followers are spurred into action, to conduct small-scale, local acts of terror (e.g., recent mass shootings in San Bernardino, CA, and Orlando, FL, in 2016). Additionally, terrorist organizations use social media for getting information about their enemies; soldiers of the United States, Canada and Great Britain [have been] trained to erase their personal data from social networking sites (Marcu & Balteanu, 2014).

Accordingly, disruption to maritime commerce, information systems, or other resources by means of terrorism would have significant adverse implications for the global economy, its supporting infrastructure, and the national will of its citizens. Let's explore these country-level implications and corresponding mitigation approaches.

Economic implications. Any slowdown or closure of a port has global repercussions as the gridlock would cause vessels to be unable to discharge, which in turn would cause ships to stop being loaded that are bound for the United States. Then the foreign terminals would begin to slow down because of the backlog, and finally the manufacturing industries would be forced to slow down production. Prices would soon surge to record-breaking levels on most commodities, and the end result would be an economic spiral downward for the global economy (Traina D. J., 2010). In a Booz Allen Hamilton sponsored simulated scenario, the detonation of weapons

smuggled in cargo containers shut down all U.S. seaports for 12 days. The results of the simulation estimated that the seaport closures could result in a loss of $58 billion in revenue to the U.S. economy along with significant disruptions to the movement of trade (Caldwell, 2008).

Likewise, attacks carried out by other physical means, such as by land or air, can also result in severe adverse implications for the economy. This was horrifically demonstrated in the aftermath of September 11, 2001, when al Qaeda's airborne attacks against the World Trade Towers not only caused the loss of life of some 3,000 civilians (the terrorists likely expected thousands more fatalities), but cost New York City's economy about $83 billion (in 2001 dollars) in total losses, including both direct and indirect costs (Sinai D. , 2006). A less quantifiable consequence is that resulting from an act of cyber-terrorism against significant financial systems, such as a major stock exchange, or a critical interconnected infrastructure, such as the United States power grid. However, research by the security firm McAfee and the Center for Strategic and International Studies (CSIS) posits a $100 billion annual loss to the U.S. economy and as many as 508,000 U.S. jobs have been lost as a result of cyber-crime (Kasturi and Sons Ltd, 2013); while difficult to connect to specific terrorist groups, these are staggering figures.

Infrastructure implications. A nation's critical infrastructure constitutes one of the primary strategic targets of contemporary terrorism because attacking its key sectors and assets can cause severe damage to virtually all sectors of the affected society (Sinai D. , 2006). Of crucial concern is a cyber-terrorism attack on the United States' infrastructure. The situation is alarming when one considers that America has many thousands of dams, airports, chemical plants, federal reservoirs, and power plants (of which 104 are nuclear), most of which have integral systems controlled by sophisticated computer systems or other automated controllers (White & Stratton, 2003). The potential implications are wide-ranging, as one weak link in an information system could provide a terrorist organization access to disrupt, or even potentially destroy, a primary enabler of commerce.

Correspondingly, a terrorist attack carried out by physical means (land, air, or sea) would have adverse consequences for the transportation infrastructure. Within days of the September 11, 2001 terrorist attack, manufacturers began to experience disruptions to the flow of materials into assembly plants (Sheffi, 2001). At sea, terrorists have successfully attacked a range of targets, from poorly secured platforms such as oil tankers and ferries to making forays against highly defended warships, port infrastructure and oil terminals (Sakhuja, 2010). As most global trade passes by sea and through ports, and then is ultimately transported by land locally, the ripple effect of a terrorist attack on maritime infrastructure would be substantial. It is instructive to note that such disruptions may not be caused by the attack itself, but rather by the government's response to the attack: closing borders, shutting down air traffic, and evacuating buildings throughout the country (Sheffi, 2001).

National Will implications. Terrorist groups believe that if the public's national will is broken, then U.S. military power would be irrelevant (Harrison, 2007). Diminishing national will manifests itself in consumer behavior after a terrorist attack. When consumers feel less safe, it changes their

spending patterns. Businesses change their investment and employment plans. Essentially, a lack of confidence negatively impacts growth (Sinai J. , 2016). National will implications are generally a byproduct of every country-level consideration. For example, terrorist groups regard the financial sector as extensions of Western economic power and dominance (Sinai J. , 2016); so, a cyber-attack on the country's financial information systems aims not only to generate adverse consequences for the nation's economy and infrastructure, but also to impact the country's national will—citizen confidence in the strength of its country and identity—by targeting symbols of the country's national values and beliefs.

Regulatory approaches. Security for the global supply chain following September 11 has greatly improved (Traina D. J., 2010). The United States government has implemented multi-layered systems of security and taken regulatory action to minimize the prospect of another catastrophic terrorist attack. In an effort to strike a balance between the need for security and free-flowing maritime commerce, U.S. Customs and Border Protection (CBP), a component of the Department of Homeland Security (DHS) responsible for protecting the nation's borders at and between official ports of entry, oversees the Customs-Trade Partnership Against Terrorism program, known as C-TPAT (Caldwell, 2008). The program implemented several affective initiatives. The first initiative was the twenty-four hour rule, which required shippers to provide more information about the cargo and a definitive address for the consignee 24 hours prior to the loading of the shipment at a foreign port (Traina D. J., 2010). Basically, shippers must prepare a complete itemized list of its containerized cargo. This information along with current and strategic intelligence are the core elements of Automated Targeting Systems (ATS), a system that combines real time information from several CBP mainframe systems that filters this information and provides a risk based assessment (Traina D. , 2008). Further, the CBP has implemented the use of non-intrusive inspection (NII) technology and mandatory exams for all high-risk shipments (Caldwell, 2008). These initiatives or policies are all general and apply across the board; in that sense they focus on the general threat rather than any specific one (Marlow, 2010). Marlow's viewpoint is notable, as literature suggests the program has faced management and operational challenges. Yet, there are potential benefits for the firm, as C-TPAT also aims to secure the flow of goods bound for the United States by developing a voluntary antiterrorism partnership with stakeholders from the international trade community (Caldwell, 2008). The public-private partnership aspect of C-TPAT's approach receives further attention in the firm-level considerations section of this paper. Traina sums up the country-level, port-of-entry, regulatory approaches well by noting there is no silver bullet in the securing of [sic] trade, but these measures and new policies in the future will continue to provide layered risk management without impeding the flow of global trade (Traina D. J., 2010).

Regulatory measures have also been undertaken to address the contemporary concern of cyber-terrorism. For example, the Cyber-Security Research and Development Act was signed into law in 2002. Additionally, the SAFETY (Support Anti-terrorism by Fostering Effective Technologies) Act, which encourages the development and deployment of new anti-ter-

rorism products and services by providing liability protections for both the sellers and the users (Close-Up Media, Inc., 2013), was also signed into law in 2002 as part of the Homeland Security Act. In doing so, the government has created an environment conducive to anti-terrorism innovation, to continually modernize protection of critical infrastructure vulnerable to cyber-attacks. The social networks have taken measures against the terrorist and extremist groups as well, defining usage rules that prohibit the use of their services to promote terrorist activities…however, there are difficulties in implementing these measures due to the impossibility of monitoring in real time the large volume of information generated by users (Marcu & Balteanu, 2014). There is a major gap here, as Marcu and Baltenau go on to note that the countering of terrorism in social media requires fundamental reassessment at the political and strategic level and at the level of fighting against terrorism, taking in consideration the development of social networks, which should not be neglected (Marcu & Balteanu, 2014).

Diplomatic approaches. The complexity of the problem facing security providers and policy makers is that the combination of intersecting functional and institutional arrangements across the supply chain makes it almost impossible for a single actor within a single channel to effectively trace and monitor operations across different channels (Marlow, 2010). Therefore, the war on terror has required the full spectrum of diplomatic, economic, military, law enforcement, intelligence, and public opinion networks to work together. It has shown that common interests, values, and a coordinated approach are critical to combat common security concerns. Further, it has emerged that even a country as powerful as the United States needs international support to obtain intelligence, undertake surveillance, track terrorists, and physically reach its enemies (Sakhuja, 2010).

An example is the Container Security Initiative (CSI), which placed CBP staff at designated foreign seaports to work with its foreign counterparts to inspect high-risk cargo for weapons of mass destruction before the cargo is shipped to the United States (Caldwell, 2008). This has been implemented through bilateral agreements allowing both nations to send inspectors to the other country to inspect containers (Marlow, 2010). Specifically, the program has placed officers in 58 foreign ports to work with customs officials of the host countries to inspect almost 90 percent of the cargo (Traina D. , 2008). States have established a number of maritime arrangements that pivot on joint operations, multilateral exercises, intelligence sharing, training, and capacity building (Sakhuja, 2010). The U.S. Customs and Border Protection (CBP) agency has offered reciprocity agreements with all the participating states and some have taken advantage of this opportunity. In addition, CBP shares information with all the participating states (Traina D. J., 2010).

Dr. Joshua Sinai proposes a *Framework for Critical Infrastructure Resilience to Terrorism* in which diplomatic collaboration is necessary. He contends that the overall strategic goal of homeland security is for a nation to build up its resilience to terrorism by effectively implementing six mission areas: the pre-incident components of (1) anticipation, (2) preparation, (3) prevention, and (4) protection, and the post-incident components of (5) response and (6) recovery (Sinai D. , 2006). The aforementioned regulatory

and diplomatic initiatives primarily address the anticipation, preparation, and prevention elements, which are of primary concern in the context of this paper. Dr. Sinai concludes that these are exceedingly complex, difficult, and costly missions that require coordinated, integrated, and focused efforts from all sectors in society, involving a country's federal government, state and local governments, the private sector, the population, and the international community (Sinai D. , 2006).

Military approaches. Popular wisdom repeatedly recites that the war on terrorism is unlike any past war. But popular wisdom has not yet adapted to the most fundamental way in which this war is different. In fact, it is not so much a war as it is a new era of continuous danger (Sheffi, 2001). The threat of cyber-terrorism makes the prospect of a singular military approach impractical. Of most critical significance is military presence, as opposed to military force, near home-country ports of entry and critical waterways around the world. Appropriate positioning of Navy warships and other military assets assists the previously discussed regulatory and diplomatic approaches. The effectiveness of the drone strike and/or boots on the ground approach is questionable; while arguably necessary, its use in a vacuum does not appropriately address and mitigate adverse implications for the country's economy, infrastructure, or national will.

Firm-Level Considerations

The preceding evaluation of national-level considerations provides context for the environmental factors and adverse implications facing the firm, as well as for the suggested approaches to assess and mitigate the risk and impact of a terrorist attack on its supply chain operations. But, how prepared is the firm? Helferich and Cook note the following: The typical large U.S. corporation has given disaster preparedness a low priority because of competing business issues, the lack of recognition of the true level of disaster vulnerability, and an assumption that the service and government sectors are responsible for disaster response. The threat of more terrorist attacks creates a powerful motivation for management to explore the processes to secure the performance of the commercial supply chain (Helferich & Cook, 2002). As this subject paper caters to small- to medium-sized enterprises, it is arguable that such firms give less consideration to the threat of terrorism than its larger counterparts due to the proportionately fewer resources available to utilize for such a purpose. Yet, as previously noted, firms are vulnerable not only to attacks on their own assets, but also to attacks on their suppliers, customers, transportation providers, communication lines, and other elements in their eco-system (Sheffi, 2001). Therefore, regardless of size, the use of resources to assess the firm's individual situation is paramount. Additional resources for mitigation purposes will depend on the results of such an assessment. Accordingly, executives must gain an understanding of firm-level considerations via evaluation of contemporary viewpoints pertaining to logistical, supply network, and technological adverse implications and their corresponding strategic and operational risk mitigation approaches.

Logistical implications. The role of logistics has become increasingly

important for companies due to longer and increasingly complex supply chains (Christopher M. , 2011). Some argue the supply chain's complexity is both its vulnerability and its strength (Harrison, 2007), as multiple modes of transportation may be available to the firm if a terrorist attack were to target one of the modes; that said, the attack itself is not the only consideration. Measures taken by the US and other governments to improve homeland defense have burdened the global transportation system, creating longer and less reliable lead times (Sheffi, 2001). Firms must realize adverse implications may result from the attack, as well as the country's response to the attack. Additionally, the firm's supply chain practices, such as outsourcing, single sourcing…and inventory reduction (Christopher M. , 2011), potentially increase its susceptibility to adverse consequences. Today's global and highly efficient supply chains lack buffers to protect against such disruptions (Konig & Spinler, 2016). Notably, the culmination of these dynamics may have severe adverse consequences for the firm—particularly, its supply chain logistics. For example, a terrorist attack against a firm's supply chain might cause widespread disruption to customer delivery capabilities, leading to a loss of short-term revenue and creating a service failure (Closs, Speier, Whipple, & Voss, 2002). In effect, the longer the supply chain, and the larger the number of countries it travels through, the greater the potential impact to the firm's logistics activities. Firms may experience loss, damage, or delay of cargo as well as loss of visibility of such cargo. Further, much depends on the firm's foreign market entry strategy. The exporting firm relies heavily on the maritime supply chain for movement of goods, whereas firms that use a foreign direct investment internationalization strategy may have more flexibility, depending on the location of the terrorist attack and the firm's facilities.

Supply network implications. As organizations increase their reliance on integrated supply chain networks, they become more vulnerable to their suppliers' disaster risk profiles (Lockamy III, 2014). Since September 11, many US (as well as European) companies are reconsidering the wisdom of using overseas suppliers. Offshore suppliers may be less expensive, but they require longer lead-time and may be more susceptible to disruptions in the transportation system (Sheffi, 2001). The firm's supply network is generally impacted due to adverse implications for the firm's logistical activities; however, unlike other impacted groups (such as customers), the supply network may not be as insulated by intermediary buffer inventory and other assets. Further, poor infrastructure and/or unstable political environments in offshore outsourcing countries may be less capable of mitigating or adequately responding to a terrorist attack.

Technological implications. The firm's information technology infrastructure is of upmost concern. For the past two to three years, cyber-attacks and related incidents have been entering the global risks landscape as among the most likely and most potentially impactful risks – in North America, cyber-attacks ranks as the most likely risk by far (World Economic Forum, 2016). Attacks launched in cyberspace involve the use of various methods of exploiting the weaknesses of the computers' security, including cyber viruses, stolen passwords, and secret entry software that allow the intruders to penetrate the systems without being detected (Marcu & Balteanu,

2014). Firms with sensitive intellectual property, responsibility for critical resource generation and/or distribution (such as electricity and water), or asset management responsibility for significant financial instruments are at notable risk. Furthermore, as firms increasingly rely on sophisticated, interdependent, and connected information systems, any technological disruption could adversely impact the firm's supply chain operations.

Strategic and operational approaches. Perhaps there is nothing the firm needs to undertake to mitigate the impact of a terrorist attack on its supply chain operations, as John Harrison suggests by noting that continued emphasis on intelligence sharing, aggressive military and police operations, and restricting terrorist access to funds and other materials will be sufficient to secure society as well as the supply chain (Harrison, 2007). Most contemporaries disagree, however, and recommend a variety of approaches for the supply chain executive's consideration.

The country-level regulatory approaches portion of this subject paper alluded to the prospect of leveraging public-private partnership to minimize the threat of terrorism to ports of entry within the global supply chain. To expand, C-TPAT aims to secure the flow of goods bound for the United States by developing a voluntary trade community comprised of importers; customs brokers; air, sea, and land carriers; and other logistics service providers (Caldwell, 2008). C-TPAT is a voluntary initiative, where organizations that choose to participate by increasing security in the supply chain will most likely receive less scrutiny of incoming cargo (Traina D. J., 2010). Essentially, the government seeks to improve overall supply chain security by improving member firms' security methods—enticing them to do so via incentive.

Other scholars also suggest firms embrace public-private partnership. Sheffi notes, recognizing the important role that government will play in the new era, and recognizing that government cannot do it alone, that corporate executives need to start considering the government, both federal and local, as a partner in corporate life (Sheffi, 2001). To elaborate on Sheffi's overall strategic approach, to prepare for another attack he recommends firms analyze investments in three main categories: (1) supplier relationships and awards, (2) inventory management criteria, and (3) knowledge and process backup (Sheffi, 2001). He goes on to recommend improvements in shipment visibility, improved collaboration between trading partners and across enterprises, better forecasting through risk pooling, and further assumption of security roles and responsibilities.

Sheffi's last point ties in with Closs, Speier, Whipple, and Voss' A Framework for Protecting Your Supply Chain, which outlines ten security competencies the firm should institute. The text notes, security competencies are created through the development of security capabilities such as infrastructure, processes, assets, and resources that achieve and maintain supply chain security. Security competencies include: 1) Process Strategy; 2) Process Management; 3) Infrastructure Management; 4) Communication Management; 5) Management Technology; 6) Process Technology; 7) Metrics; 8) Relationship Management; 9) Service Provider Collaboration Management; and 10) Public Interface Management (Closs, Speier, Whipple, & Voss, 2002). Effectively, the authors offer a framework to guide implementation.

Another perspective is that of Chang, Ellinger, and Blackhurst, who present a succinct comparison of the characteristics of the different supply chain mitigation strategies that are identified in the extant SCRM literature: redundancy vs. flexibility, buffering vs. bridging, hedging vs. control, and increased capacity vs. increased responsiveness (Chang, Ellinger, & Blackhurst, 2015). Fundamentally, each dichotomy is a mirror to the others. Redundancy approaches focus on limiting or mitigating the negative effects of risk by increasing product availability by keeping some resources in reserve to be used in case of a disruption (Chang, Ellinger, & Blackhurst, 2015), whereas flexibility approaches involve building organizational and inter-organizational capabilities to sense threats to supply continuity and to respond to them quickly (Zsidisin & Wagner, 2010).

Conversely, Christopher and Holweg propose adjusting the traditionally rigid supply chain model to one of *structural flexibility*, which refers to the ability of the supply chain to adapt to fundamental changes in business environment (Christopher & Holweg, 2011). The authors outline approaches that exhibit structural flexibility, such as dual sourcing, asset sharing, flexible labor arrangements, rapid manufacture, outsourcing, and use of alternate distribution channels, all of which merit consideration to counteract the adverse implications of a terrorist attack. There are other strategic approaches, such as Hale and Moberg's secure site location decision process (Hale & Moberg, 2005). Yet, as Sinai notes, terrorist threats do not affect all businesses alike (Sinai J. , 2016). The applicability of each risk mitigation approach is quite dependent on the individual firm's situation. Accordingly, supply chain executives should consider a pragmatic risk assessment and mitigation planning framework to evaluate the firm's individual situation.

A Pragmatic Risk Assessment and Mitigation Planning Framework

Contemporaries suggest a combination of public-private partnerships to proactively reduce the likelihood of a terrorist attack, and the implementation of operational redundancies (assets and infrastructure) to minimize its impact to ongoing business operations. While perhaps these approaches may be appropriate, supply chain executives require a framework to adequately assess the firm's individual situation. Accordingly, the following managerial framework adapts existing and presents new risk assessment and risk mitigation planning approaches for the supply chain executive's pragmatic use. The framework progresses through three phases: 1) the *business aspects evaluation* phase wherein firm-level attributes are weighed; 2) the *supply chain aspects evaluation* phase wherein supply chain characteristics are assessed; and 3) the *mitigation planning* phase wherein the business and supply chain aspects output the suggested level of intensity the firm's mitigation plan should assume.

1. Business Aspects Evaluation

Assesses, by way of numerical weighting, firm-level attributes that influence the firm's susceptibility to adverse implications resulting from terrorism.

1.1 Business category (b). As Sinai points out, certain business cat-

egories are of greater risk to terrorist attack than others. These include transportation (aviation, ground and maritime), energy (nuclear power, oil and gas facilities, and chemical plants), financial institutions (such as stock exchanges and banks), tourism (hotels and restaurants), and shopping malls (Sinai J. , 2016). Based on this context, assign a value to this aspect between zero (0) and ten (10), where zero (0) represents the lowest risk-level and ten (10) represents the highest level of risk.

1.2 Customer distance (d). Not dissimilar to the business category, the firm's *distance* from the customer is also of concern. For example, service industries such as tourism are generally fulfilling customer requirements more closely in terms of space and time than low-tier manufacturers of goods, which may be several levels removed from the end consumer. There are additional security cost and brand equity considerations the short customer distance firm must consider. Therefore, assign a value to this aspect between zero (0) and five (5), where zero (0) represents a long customer distance and five (5) represents a short customer distance.

1.3 Level of connectivity (n). Another business aspect the executive must consider is how dependent the firm's operations are on connectivity. In this sense, connectivity refers to the firm's level of reliance on information technology to conduct business, which if impacted, would create significant challenges to ongoing operations or business continuity in the event of a terrorist attack. Further, as Sheffi points out, corporations with several warehouse management systems, multiple order entry systems, or several incompatible manufacturing and financial systems, are more vulnerable than companies who standardized their operations and can move personnel and processes between locations if a single location goes down (Sheffi, 2001). So, both the level of connectivity and the deviations between the connected systems must be considered. Assign a value to this aspect between zero (0) and five (5), where zero (0) represents the lowest risk-level and five (5) represents the highest level of risk.

1.4 Level and type of internationalization (i). As reviewed, the focal firm's level of globalization may correlate to increased operational risk. Further, differing levels and types of risk may result from the firm's foreign market entry method. For example, the exporting firm relies heavily on the maritime supply chain for movement of goods, whereas firms that use a foreign direct investment internationalization strategy may have more flexibility, depending on the location of the terrorist attack and the firm's facilities. While they may have more control, numerous interconnected facilities worldwide may expose the firm to threats unique to specific country or regional environments. Via critical self-evaluation, assign a value between zero (0) and ten (10), where zero (0) represents the lowest risk-level and ten (10) represents the highest level of risk.

1.5 Calculate the business aspects sum (BAS). Add each of the preceding attribute values to calculate your firm's numerical business aspect risk level. The lowest possible value is zero (0) and the highest possible value is thirty (30).

=Business category(b) + Customer distance(d) + Connectivity(n) + Internationalization(i)

2. Supply Chain Aspects Evaluation

Assesses, by way of numerical weighting, supply chain attributes that influence the firm's susceptibility to adverse implications resulting from terrorism.

2.1 Supply chain complexity (c). Essentially, the supply chain executive must assess both the length and the depth of its complete supply chain. The greater the number of countries it travels through, the more entities with which is interacts, and the more differentiated the product and service offerings, the greater the risk to the organization. Assign a value between zero (0) and ten (10), where zero (0) represents the lowest complexity and ten (10) represents the highest complexity.

2.2 Resource use strategy (r). Evaluate the firm's general practice regarding inventory and capacity. Does the firm buffer inventories and plan for excess capacity? Or, conversely, does the firm generally seek to maximize inventory turns and utilization of capacity? Assign a value between zero (0) and five (5), where zero (0) represents the former and (5) represents the latter.

2.3 Supply network characteristics (s). Assess aspects of the firm's supply network, such as its ratio of offshore suppliers to local suppliers, the nature of contractual agreements with such suppliers, and its use of dual sourcing. Then, assign a value between zero (0) and five (5), where zero (0) represents low risk relative to the preceding, and other, considerations (i.e., low offshore to local supplier ratio, strong contracts, and abundant use of dual sourcing), and five (5) represents high risk relative to these characteristics.

2.4 Reliance on transportation infrastructure (t). Conduct an analysis of the firm's transportation methods to ship and receive goods. Consider breakdown by mode, such as land, air and sea, as well as by distance covered—are transports generally local, regional, national, or international? Give attention to frequency of shipments and receipts, as well as its relative importance to the overall operation. Assign a value between zero (0) and ten (10), where zero (0) represents the lowest risk and ten (10) represents the highest risk.

2.5 Calculate the supply chain aspects sum (SCAS). Add each of the preceding attribute values to calculate your firm's numerical supply chain risk level. The lowest possible value is zero (0) and the highest possible value is thirty (30).

=Complexity(c) + Resource use(r) + Supply network(s) + Transportation(t)

3. Mitigation Planning

Lastly, add the business aspects sum (BAS) to the supply chain aspects sum (SCAS) to derive an overall numerical risk level (ONRL). See Table 1 for the suggested level of intensity the firm's mitigation plan should assume, and recommended action, based on the total.

ONRL = Business aspects sum (BAS) + Supply chain aspects sum (SCAS) References

Limitations and Conclusions

Table 1. Mitigation Planning – Suggested Response Level

ONRL	Suggested Response Level	Recommended Action
25-30	Intensive	Allocate significant resources to address.
20-24	High	Identify highest risk areas to address.
16-19	Moderate	Conduct cost-benefit analysis first.
12-15	Low	Consider based on available resources.
0-11	None	Negligible risk level - no action required.

The preceding framework is intended for pragmatic use, hence its simplicity. The inherent simplicity of the framework, however, may limit its use in actual practice. The framework was developed via culmination of observed research and the author's practical experiences as a supply chain executive. Accordingly, a wide range of country- and firm-level considerations are reviewed to cater to a wide audience of executives in various industries and contexts. The framework, in turn, serves to help shape the user's thought process, especially regarding risk assessment. A limitation is the potential for one or two aspects to disproportionately skew the overall numerical risk level. The reader must recognize this possibility, and adjust accordingly. Further, the reader is expected to utilize the information herein as a basis for further research, upon proper identification of the firm's most prevalent risks. While the paper considered a broad review of literature, some adverse implications and mitigation approaches received more attention than others.

In conclusion, if the key to business success is superior efficiency and effectiveness relative to one's competitors, and the globalization of markets provides internationalizing firms the opportunity to augment these factors, such firms must give proper attention to the risks prevalent in international business, not least of which is the country risk of terrorism.

References

Caldwell, S. L. (2008). Supply Chain Security: U.S. Customs and Border Protection has Enhanced its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices. Washington, DC: United States Government Accountability Office.

Cavusgil, S., Knight, G., & Riesenberger, J. (2017). International Business: The New Realities. Hoboken, NJ: Pearson Higher Education.

Chang, W., Ellinger, A. E., & Blackhurst, J. (2015). A Contextual Approach to Supply Chain Risk Management. International Journal of Logistics Management, 26(3), 642-52.

Christopher, M. (2011). Logistics and Supply Chain Management (4th ed.). Harlow: Pearson Education.

Christopher, M., & Holweg, M. (2011). "Supply Chain 2.0": managing supply chains in the era of turbulence. International Journal of Physical Distribution & Logistics Management, 41(1), 63-82.

Close-Up Media, Inc. (2013). Contemporary Services Garners SAFETY Act Designation by the United States Department of Homeland Security. Jacksonville: Close-Up Media, Inc.

Closs, D., Speier, C., Whipple, J., & Voss, D. (2002). A framework for protecting your supply chain. Logistics Management, 47-9.

Hale, T., & Moberg, C. R. (2005). Improving Supply Chain Disaster Preparedness: A Decision Process for Secure Site Location. International Journal of Physical Distribution & Logistics Management, 195-207.

Harrison, J. (2007, March 22). Low threat, low impact. The Business Times Singapore, 26.

Helferich, O., & Cook, R. (2002). Securing the Supply Chain: Management Report. Oak Brook, IL: CLM Publications.

Kasturi and Sons Ltd. (2013, July 23). Cyber Crime Costs World Economy Up to $500 b/year. Businessline.

Konig, A., & Spinler, S. (2016). The Effect of Logistics Outsourcing on the Supply Chain Vulnerability of Shippers. International Journal of Logistics Management, 27(1), 122-41.

Lockamy III, A. (2014). Assessing disaster risks in supply chains. Industrial Management & Data Systems, 114(5), 755-77.

Marcu, M., & Balteanu, C. (2014). Social Media-A Real Source of Proliferation of International Terrorism. Annales Universitatis Apulensis: Series Oeconomica, 16(1), 162-9.

Marlow, P. (2010). Maritime security: an update of key issues. Maritime Policy & Management, 37(7), 667-676.

Sakhuja, V. (2010). Security threats and challenges to maritime supply chains. Disarmament Forum, 3-12.

Sheffi, Y. (2001). Supply Chain Management under the Threat of International Terrorism. International Journal of Logistics Management, 12(2), 1.

Sinai, D. (2006). A Framework for Critical Infrastructure Resilience to Terrorism. The Journal of Counterterrorism & Homeland Secruity International, 12(2).

Sinai, J. (2016). New Trends in the Terrorist Threats Against the Business Sector. Journal of Counterterrorism and Homeland Security International, 21(4), 1.

Traina, D. (2008). The Container Revolution: Increases Security Challenges. The

Journal of Counterterrorism & Homeland Security International, 58-61.
Traina, D. J. (2010). Thwarting Terrorism Through Layered Security And Hardening The Supply Chain. Journal of Counterterrorism and Homeland Security International, 16(2), 58-61.
White, R., & Stratton, S. (2003, August 20). Nation's Risk for Cyberterror is Scary. Milwaukee Journal Sentinel.
World Economic Forum. (2016, January 15). Global Risk Report, how we are thinking about cyber dependence, cyber attack, data theft, cyber terrorism, cyber war, dark web, state sponsored attacks... Progressive Digital Media Technology News.
Zsidisin, G., & Wagner, S. (2010). Do perceptions become reality? the moderating role of supply chain resiliency on disruption occurrence. Journal of Business Logistics, 31(2), 1-20.