Chapter 13
Malicious Supply Chain Risk: A Literature Review and Future Directions

Scott DuHadway and Steven Carnovale

1 Introduction

Managing supply chain risk is an important component of supply chain management and is generally defined as "the likelihood of an adverse and unexpected event that can occur and either directly or indirectly result in a supply chain disruption" (Garvey et al. 2015, p. 619). Risks can vary from major disruptions due to natural disasters, supplier bankruptcy, quality failures, fraud, etc. In order for firms to develop a resilient supply chain, it is important that they are able to correctly interpret supply chain risk and adapt operations to meet those risks (Ambulkar et al. 2015; Pettit et al. 2016). Thus, research in this area has explored much in terms of how to effectively manage risks that are, implicitly, from inadvertent causes such as weather-based disruptions or accidental supply failures through a variety of process-focused (i.e., procedural recommendations/techniques to mitigate risk) research. However, much opportunity remains to explore the role of relational risk associated with other companies or individuals in the supply chain engaging in malicious behaviors that can lead to disruptions. With that in mind, it is important that researchers recognize a type of risk that has received limited attention in the literature, which we identify as malicious supply chain risk. We define malicious supply chain risk as the risk a firm has as a result of an individual or organization making a deliberate decision that can lead to harmful outcomes on the firm and its extended supply chain. Examining *malicious risk and disruptions* is worthwhile, considering how relatively unexplored they are. Accordingly, the following sections will explore these areas in detail.

S. Carnovale (✉)
Saunders College of Business, Rochester Institute of Technology, Rochester, USA
e-mail: scarnovale@saunders.rut.edu

S. DuHadway
Portland State University, Portland, OR, USA
e-mail: duhadway@pdx.edu

G. A. Zsidisin and M. Henke (eds.), *Revisiting Supply Chain Risk*, Springer Series in Supply Chain Management 7, https://doi.org/10.1007/978-3-030-03813-7_13

2 Literature Review

Though this area has received little attention, we note that the research on risks associated with malicious behavior has been increasing over the past few years. The evidence suggests that companies are increasingly facing crises from product harm that results in a product recall (Liu et al. 2017). Despite these increases, there is limited research which explores the motivation to engage in fraudulent actions at an organizational level (Arnold et al. 2012). For example, some studies have explored aspects of disruption risk related to intentional behavior in some way, including threats from theft, piracy, terrorism, contamination, counterfeiting, and product tampering (McGreevy and Harrop 2015), preparing a supply chain for premeditated attacks on facilities (Parajuli et al. 2017), how to monitor fraud risks in the supply chain (Vollmer 2015), and issues related from profiting from product-harm crises in competitive markets (Rubel 2018), among others.

While much of the research in this area explores specific threats/risks, there is some research that advances strategies for managing these types of risk. DuHadway et al. (2017) explore key differences in how to manage intentional disruptions (similar to the concept of malicious risks defined in this chapter) as opposed to traditional disruptions, suggesting that mitigating intentional disruptions requires relationship-based approaches, while recovering from disruptions requires the ability to restructure a supply chain. Other research suggests that manufacturers must build forms of relational governance to safeguard against the relational risk of partners (Cheng and Chen 2016). Additionally, research which identifies the antecedents of similar (malicious) disruptions or opportunistic events has found that power asymmetry/imbalance culture can lead to malicious risks (Villena and Craighead 2017; Madichie and Yamoah 2017).

Perhaps, the literature stream most closely connected to malicious risks is that which explores opportunism, or "self-interest seeking with guile" (Williamson 1985). Opportunism is often thought of as the calculated efforts of an exchange agent to mislead or otherwise obfuscate, or distort, a transaction (Williamson 1985). Perhaps, a more applicable way to frame the impact of opportunism, particularly as it relates to malicious risks, can be described as a partner within an exchange relationship not acting in the best interests of the opposing partner (Doney and Cannon 1997). In this case, there is a breakdown of trust in the relationship. Trust is typically broken down into two critical constructs: credibility and benevolence (Morgan and Hunt 1994; Doney and Cannon 1997; Ganesan and Hess 1997; Huang et al. 2008; Suh and Houston 2010). Credibility is the belief that the supplier will fulfill its promises while being reliable and consistent in its commitments (Dwyer et al. 1987; Morgan and Hunt 1994; Ganesan and Hess 1997). Credibility, with respect to the supply chain literature, is a critical component to relational exchange (Ganesan and Hess 1997). Benevolence is the belief that a partner in an exchange relationship will not act opportunistically if given the chance (Doney and Cannon 1997; Ganesan and Hess 1997). Researchers have given serious emphasis to the development, formation, and management of trust. Given this emphasis, trust is a fundamental underpinning for

Fig. 1 Examples of malicious and traditional risks. Adapted from DuHadway et al. (2017)

the development of the working dynamics between firms. Using opportunism as a basis, we can identify several behaviors that fit with malicious risk and that have seen some exposure in the literature (Fig. 1).

2.1 Examples of Malicious Risks

Consider the two major automotive recalls of Takata air bags and the Volkswagen emissions scandal. The Takata airbag recall, which was the largest automotive recall in history, occurred because Takata switched their production to using ammonium nitrate instead of tetrazole in their airbag design to cut costs and then lied to their customers regarding the safety of the new compound being used (Trudell et al. 2014; Trudell and Fisk 2016). Takata "routinely manipulated results of airbag inflator tests" (Trudell and Fisk 2016). Data indicating the risk of the air bags was deleted, and customers were unaware of the risks that Takata knew and understood. Takata engaged in malicious behavior to advance their interests at the expense of their supply chain partners.

Volkswagen engaged in deceptive practices which ultimately led to a recall for their vehicles which used software to deliberately cheat emissions testing, causing an estimated 59 premature deaths (Barrett et al. 2015), and a financial settlement of over $15 billion in the USA (Fisk et al. 2016). Interestingly, in both of these cases safeguards were in place (airbag inflator tests to verify safety and the emissions testing procedures) to prevent problematic behavior, yet the firms intentionally circumvented such process controls and engaged in malicious behavior for their own self-interest.

In 2013, it was found that beef lasagna contained horsemeat of varying percentages, with some of them containing 100% horsemeat (Brown 2013). It is challenging to think that the introduction of horsemeat into the beef supply chain occurred through some inadvertent or accidental measure, particularly given that differentiating between a horse and a cow is rather simple. At some point in the supply chain, someone made the decision to substitute a horse for a cow and sell it as beef and did so intentionally, likely because it saved them money. Even though beef and horsemeat might be reasonably comparable, the act of deception in the supply chain is what serves to motivate the exploration into malicious risks. If our supplier says, "This is beef"—should we not be able to rely on that statement? And if we do decide that we are not ready to trust our supplier, how can we protect ourselves from when suppliers decide to deliberately deceive us, or when our suppliers themselves have been duped? The issue of product deception and fraud very quickly becomes a supply chain issue, particularly because the ramifications of deceptive behavior have far-reaching effects on all members in the supply chain.

There are examples of firms who have taken the appropriate quality control measures to protect their supply chain who have been impacted by deliberate deception of a supplier. The lead-based paint toy recalls from 2007 which Mattel experienced are notable because Mattel established and paid for a testing facility, thus taking what would normally be appropriate measures to ensure that the materials coming into the supplier's facility were of appropriate quality. However, their supplier intentionally avoided the testing facility (Woo 2008). Accordingly, we need to rethink the way we manage a supply chain to limit our exposure to malicious risks. Traditional process-based approaches can be ignored or circumvented.

Malicious risks can take a variety of different forms, including falsifying data, supply chain fraud, counterfeit manufacturing, digital security threats, intellectual property theft, contract breach. A 2012 study found that 33% of the 1215 fish samples collected at restaurants, sushi vendors, and grocery stores were labeled incorrectly (Warner et al. 2013). Supply chain fraud has been identified as the "single most exposed area" of fraud (Bhide 2012, p. 16). Counterfeit manufacturing has become a large problem in the automotive supply chain, and examples of their impact on manufacturers and consumers are not difficult to find. Daimler seized 1.6 million counterfeit products in a single year (Daimler 2017). Mislabelled counterfeit plastic parts in Aston Martin vehicles have led to major recalls (Wowak and Boone 2015; DuHadway et al. 2017).

Much of the research on supply chain disruptions has explored it from the perspective of managing it via process-based controls. For example, research on automotive recalls has explored it from a process-based view (Shah et al. 2017), but there is evidence of a number of recalls which happened even though "specific measures were undertaken by the firms to avoid such issues," suggesting that "efforts to improve quality performance of vendors may not be effective" (Agrawal and Muthulingam 2015, p. 350). So, how then should we manage these types of risks? Some strategies involve different approaches. For example, Babich and Tang (2012) suggest deferred payment outperforms inspections as a more effective way to eliminate opportunism such as product adulteration.

If we are relying on process-based controls, we are inherently relying on trust as a protection mechanism to ensure that such procedures are followed. While trust can be good, consider the dark side of trust as well. To highlight this dark side of trust, consider the example provided in the book *Turtles of the World* (Bonin et al. 2006). The authors explore a number of different species of tortoises, finding that in some species an interesting symbiotic relationship emerges between the turtles and some local finches. The finches eat the small bugs and parasites that live on the turtles, particularly in hard to reach places such as under the head and neck of the turtle. This behavior involves a turtle signaling to the bird by raising up on its front legs and letting the bird crawl underneath him to eat the insects. However, some of the turtles have tasted the dark side and learned that by suddenly dropping itself onto the bird, it can catch the bird under its shell, crushing it and providing a good source of nourishment in the form of newly tenderized protein. Although this example is quite extreme, trust in relationships is exhibited in similar ways. It slowly develops over time as expected behaviors emerge which can form mutually beneficial relationships. Yet, if one party decides to start playing unfairly, it can have dramatic consequences on the other involved parties.

3 Managing Malicious Risks

We explore three traditional approaches for managing risk: detection/avoidance, mitigation, and recovery. These three phases of risk management represent before, during, and after a disruptive event has occurred (Fig. 2).

Detection can serve as an early warning system or can help to dodge a disruption completely. If the disruption is unavoidable, it can ensure that good plans are in place to manage the disruption once it occurs. For example, take the recent example of bitcoin's price volatility (Sapuric and Kokkinaki 2014). Such fluctuations in price have led to shortages of video cards and incredibly high prices, as one of the ways that bitcoins can be gathered is through electronic mining which is most efficient using high-end graphics cards. However, due to the fluctuation of prices of bitcoins, the demand is highly uncertain and difficult to predict. Being able to observe early market trends can help firms avoid underproducing or over-producing products leading to either a disruption or a surplus of product that needs to be liquidated at a lower price.

A number of detection and avoidance mechanisms exist, including quality management (Lee and Whang 2005), information sharing (Sheffi 2001; Kleindorfer and Saad 2005), supplier audits and supplier development (Giunipero and Eltantawy 2004), and security assessment and management practices (Finch 2004). Even though there are many different mechanisms for detection, effective detection which comes from information sharing, supply chain visibility, and supplier integration can detect or prevent a variety of disruptions (DuHadway et al. 2017). Another effective mechanism to limit malicious risks is transparency. For example, blockchains have been suggested as a potential avenue for increasing transparency with smart contracts

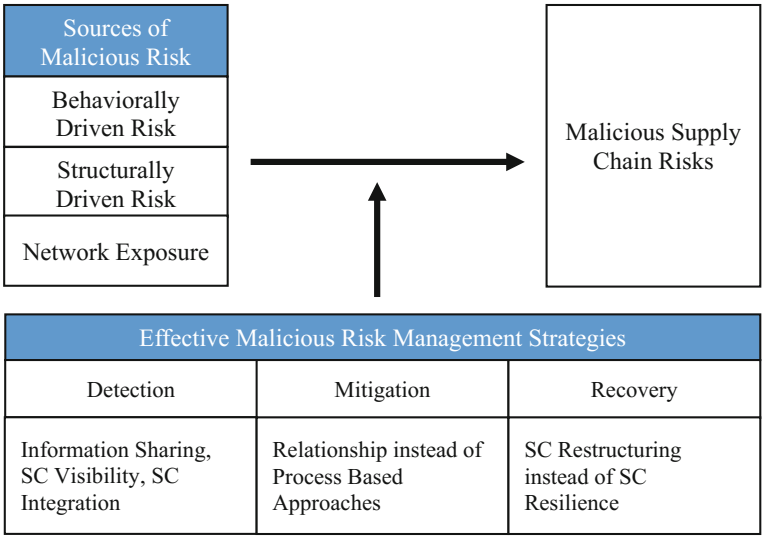

Fig. 2 Sources and mitigation strategies for malicious risks. Adapted from DuHadway et al. (2017)

(Nugent et al. 2016). Further research into the area of technology tools to enable transparency is necessary so as to provide recommendations in this area, however.

Mitigation can limit the potential impact of a disruption occurring. This is critical for minimizing the harm to a supply chain from a disruption. Some research suggests that structural approaches can help to mitigate damage, such as modularity and diversification (Kleindorfer and Saad 2005). Other more traditional approaches might include stockpiling inventory (Chopra and Sodhi 2004; Tomlin 2006). These strategies are important to recognize, because it is possible that these strategies exacerbate the risks of malicious disruptions rather than limiting them. For example, consider the impact of high levels of inventory when the disruption is due to supply chain fraud such as lead-based paint in children's toys. Higher levels of inventory would then need to be discarded in addition to the carrying costs of maintaining higher levels of inventory. Modularity has been argued to generally limit exposure to opportunism (Lippman and Rumelt 1982; Pil and Cohen 2006), but if the modular system is compromised through intellectual property theft or counterfeiting, the issue could be further exacerbated because the entire system is now compromised.

Recovery is another aspect of risk management that requires a completely different approach. One of the most common approaches for risk recovery is to develop a resilient supply chain, or one that is quickly able to return to its previous state after a disruption (Christopher and Lee 2004). However, this approach is counterintuitive when the disruption is caused by malicious risk. When the disruption is caused by malicious risk (i.e., finding out that your supplier has been selling you a counterfeit product), there is no value in returning to the previous state, so resilience-based recovery approaches are insufficient. Using an analogy of a human immune

system, we can liken resilience to being able to recover from injury. Such injuries generally occur from an external cause, and the goal of recovery is to return to full functionality from the injury. However, disruptions from malicious risks could be seen as analogous to symptoms of an infectious disease. In such a case, it might require addressing the conditions that led to the symptoms internally. Without treatment, the infection could significantly worsen and lead to other problems. The goal should not be focused only on treating the symptoms, but the core of the problem. In extreme cases, it might require removal of the infected part. The approach that should be taken when a supplier has a product quality failure due to some accidental cause should be substantially different than when a supplier intentionally deceives or lies about product quality and intentionally substitutes an inferior product to make money. Recovering from malicious risks will require a more substantive approach which will require restructuring the supply chain, for example, by excising the supplier, or more fundamental approaches to addressing the cause of the disruption. Appropriate supplier relationship management could help substantively in this area.

4 Drivers of Malicious Risks

The above discussion makes clear that dealing with malicious risk through the prism of traditional supply chain risk management can be insufficient for preventing disruptions due to such risks. The reason is that the causes for the manifestation of such risks are different, and so too are the impacts that they have on the network in which the firm is embedded. Although the research on malicious risks is relatively limited, we propose that the drivers (i.e. antecedents) of such malicious risks can arise from three core areas: (1) the microlevel: behavioral drivers; (2) the mesolevel: structural drivers; and (3) the macrolevel: network exposure as a driver. Below, we briefly explore the implications of each of these drivers and propose a research question motivating each area's future work.

4.1 Micro-Drivers: Behaviorally Driven Risk

Take the example of the fraudulent beef lasagna example above, where at one point someone made the choice to swap horse for beef and include it in the supply chain. This is a microlevel decision with cascading impacts on the rest of the supply chain. Concepts such as dependence asymmetry, trust and relational governance, transitive trust, cultural norms and values, business ethics can provide interesting insight into terms of how we can limit malicious supply chain risks. At this level, a core research question is: *What relational mechanisms engender the development of malicious supply chain risks?*

4.2 Meso-Drivers: Structurally Driven Risk

The structural drivers of malicious risk can include risks associated with the general trends to the changing environmental conditions surrounding supply chain management in a modern era. These include the increasing reliance on digital manufacturing, high levels of modularity, data security processes, the world becoming increasingly connected, and emergent cultural differences through a more connected world. Take, for example, the recent ascendency of blockchain technology into various supply chain processes. On the one hand, it promises increased transparency and visibility (Nugent et al. 2016), yet in order for the supply chain to benefit from transparency firms must be candid and share all of their information on the blockchain. What happens if an actor is less than honest? Hence, a core research question motivating these structural drivers of malicious risk is: *What are the exogenous, structural mechanisms engendering the development of malicious supply chain risk?*

4.3 Macro-Drivers: Network Exposure

Research examining a firm's network exposure as a driver of malicious risk should seek to understand how different network structures in which firms are embedded can change their exposure to malicious risks. For example, highly central firms or firms with a high degree of connectivity to various firms might experience more exposure to malicious behavior. In addition, the influence of opportunistic behavior on a network could exhibit transitive properties such that malicious risks can spread throughout a network. Take, for example, the increasing role of Internet of things (IoT) and the connectivity across many different systems in a typical supply chain. What if, for example, an autonomous trailer is hacked by a malicious actor? The truck interacts with the firm via the cloud, and now, the hacker has the ability to steal data, corrupt systems, and so on. Thus, with increased connectivity comes increased risk, particularly as it is related to the firm's network. Thus, a motivating research question at this level is: *What role does the structure of the network in which a firm is embedded have on its susceptibility to/from malicious supply chain risk?*

5 Conclusion

Human beings hedging against risk can be seen as far back as the ancient Egyptians stockpiling grain as a mitigation tool against poor harvests (Levinson and Levinson 1985). Furthermore, while tools, techniques, and methods for dealing with risk have evolved into advanced systems, much of the research advocating prescriptive methodologies for managing risk focuses predominantly on inadvertent risk. The

core thesis of this chapter is to shift the thinking, to focus on *malicious* risks, or those that are intentionally caused in the supply chain.

The reason for this need to examine, theorize against, and prescribe mechanisms for dealing with such risks is simple: Malicious risk can circumvent traditional supply chain risk management approaches. Effectively, the reason why malicious risks can be so pervasive is that their causes are quite different. Thus, in this vein we suggest that there are three core areas which drive malicious supply chain risk: behavioral-, structural-, and network-related engendering mechanisms. Further, research in this area is quite nascent with little, if any, work explicitly focused on these causes. Thus, as we enter the brave new world of supply chain risk management in the twenty-first century, our thinking needs to evolve with it. Traditional (inadvertent) risks and disruptions, though ever present, are also compounded by those intentional threats to normal operating conditions. Supply chain management needs to adjust its thinking to also consider how to thwart and minimize such risks. Moving forward, we are wise to remember the advice of Warren Buffet, "Risk comes from not knowing what you're doing."

References

Agrawal, A., & Muthulingam, S. (2015). Does organizational forgetting affect vendor quality performance? An empirical investigation. *Manufacturing & Service Operations Management, 17*(3), 350–367.

Ambulkar, S., Blackhurst, J., & Grawe, S. (2015). Firm's resilience to supply chain disruptions: Scale development and empirical examination. *Journal of Operations Management, 33,* 111–122.

Arnold, U., Neubauer, J., & Schoenherr, T. (2012). Explicating factors for companies' inclination towards corruption in Operations and supply chain management: An exploratory study in Germany. *International Journal of Production Economics, 138*(1), 136–147.

Babich, V., & Tang, C. S. (2012). Managing opportunistic supplier product adulteration: Deferred payments, inspection, and combined mechanisms. *Manufacturing & Service Operations Management, 14*(2), 301–314.

Barrett, S. R., Speth, R. L., Eastham, S. D., Dedoussi, I. C., Ashok, A., Malina, R., et al. (2015). Impact of the Volkswagen emissions control defeat device on US public health. *Environmental Research Letters, 10*(11), 114005.

Bhide, C. S. (2012). A study of the importance of forensic accounting in the modern business world. *DYPIMS's International Journal of Management and Research, 1*(1), 12–17.

Bonin, F., Devaux, B., & Dupré, A. (2006). *Turtles of the World*. Baltimore: JHU Press.

Brown, B. (2013). *Findus beef lasagne contained up to 100% horsemeat*. BBC News: FSA says.

Cheng, J.-H., & Chen, M.-C. (2016). Influence of institutional and moral orientations on relational risk management in supply chains. *Journal of Purchasing and Supply Management, 22*(2), 110–119.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review, 46*(1), 53.

Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management, 34*(5), 388–396.

Daimler. (2017). Tracking down the product pirates. *Brand Protection.* Retrieved from https://www.daimler.com/sustainability/product/claim/brand-protection.html.

Doney, P. M., & Cannon, J. P. (1997). An examination of the nature of trust in buyer-seller relationships. *The Journal of Marketing*, 35–51.

DuHadway, S., Carnovale, S., & Hazen, B. (2017). Understanding risk management for intentional supply chain disruptions: Risk detection, risk mitigation, and risk recovery. *Annals of Operations Research*, 1–20.

Dwyer, F. R., Schurr, P. H., & Oh, S. (1987). Developing buyer-seller relationships. *The Journal of Marketing*, 11–27.

Finch, P. (2004). Supply chain risk management. *Supply Chain Management: An International Journal, 9*(2), 183–196.

Fisk, M. C., Mehrotra, K., Katz, A., & Plungis, J. (2016). Volkswagen agrees to $15 billion diesel-cheating settlement. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2016-06-28/volkswagen-to-pay-14-7-billion-to-settle-u-s-emissions-claims.

Ganesan, S., & Hess, R. (1997). Dimensions and levels of trust: Implications for commitment to a relationship. *Marketing Letters, 8*(4), 439–448.

Garvey, M. D., Carnovale, S., & Yeniyurt, S. (2015). An analytical framework for supply network risk propagation: A Bayesian network approach. *European Journal of Operational Research, 242*(2), 618–627.

Giunipero, L. C., & Aly Eltantawy, R. (2004). Securing the upstream supply chain: A risk management approach. *International Journal of Physical Distribution & Logistics Management, 34*(9), 698–713.

Huang, X., Gattiker, T. F., & Schwarz, J. L. (2008). Interpersonal trust formation during the supplier selection process: The role of the communication channel. *Journal of Supply Chain Management, 44*(3), 53–75.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management, 14*(1), 53–68.

Lee, H. L., & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics, 96*(3), 289–300.

Levinson, H. Z., & Levinson, A. R. (1985). Storage and insect species of stored grain and tombs in ancient Egypt. *Zeitschrift für Angewandte Entomologie, 100*(1–5), 321–339.

Lippman, S. A., & Rumelt, R. P. (1982). Uncertain imitability: An analysis of interfirm differences in efficiency under competition. *The Bell Journal of Economics*, 418–438.

Liu, Y., Shankar, V., & Yun, W. (2017). Crisis management strategies and the long-term effects of product recalls on firm value. *Journal of Marketing, 81*(5), 30–48.

Madichie, N. O., & Yamoah, F. A. (2017). Revisiting the European horsemeat scandal: The role of power asymmetry in the food supply chain crisis. *Thunderbird International Business Review, 59*(6), 663–675.

McGreevy, C., & Harrop, W. (2015). Intentional cargo disruption by nefarious means: Examining threats, systemic vulnerabilities and securitisation measures in complex global supply chains. *Journal of business continuity & emergency planning, 8*(4), 326–345.

Morgan, R. M., & Hunt, S. D. (1994). The commitment-trust theory of relationship marketing. *The Journal of Marketing*, 20–38.

Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research, 5*.

Parajuli, A., Kuzgunkaya, O., & Vidyarthi, N. (2017). Responsive contingency planning of capacitated supply networks under disruption risks. *Transportation Research Part E: Logistics and Transportation Review, 102,* 13–37.

Pettit, T. J., Simpson, N. C., Hancock, P. G., Clark, H., Haydel, T., & Pierce, J. (2016). Exploring operational resilience in the context of military aviation: Finding the right mode at the right time. *Journal of Business and Behavior Sciences, 28*(2), 24.

Pil, F. K., & Cohen, S. K. (2006). Modularity: Implications for imitation, innovation, and sustained advantage. *Academy of Management Review, 31*(4), 995–1011.

Rubel, O. (2018). Profiting from product-harm crises in competitive markets. *European Journal of Operational Research, 265*(1), 219–227.

Sapuric, S., & Kokkinaki, A. (2014). Bitcoin Is Volatile! Isn't that Right? In *Paper presented at the International Conference on Business Information Systems*.

Shah, R., Ball, G. P. & Netessine, S. (2017). Plant operations and product recalls in the automotive industry: An empirical investigation. *Management Science, 63*(8).

Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management, 12*(2), 1–11.

Suh, T., & Houston, M. B. (2010). Distinguishing supplier reputation from trust in buyer–supplier relationships. *Industrial Marketing Management, 39*(5), 744–751.

Tomlin, B. (2006). On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science, 52*(5), 639–657.

Trudell, C., & Fisk, M. C. (2016). Honda audit finds Takata engineers manipulated air-bag test data. *Bloomberg*. Retrieved July 18, 2016, from https://www.bloomberg.com/news/articles/2016-07-18/honda-audit-finds-takata-engineers-manipulated-air-bag-test-data.

Trudell, C., Hagiwara, Y., & Jie, M. (2014). Air-bag maker in global crisis used unusual explosive. *Bloomberg*. Retrieved October 26, 2014, from http://www.bloomberg.com/news/articles/2014-10-27/air-bag-maker-in-global-crisis-used-unusual-explosive.

Villena, V. H., & Craighead, C. W. (2017). On the same page? how asymmetric buyer-supplier relationships affect opportunism and performance. *Production and Operations Management, 26*(3), 491–508.

Vollmer, S. (2015). Monitoring fraud risks in the supply chain. *Journal of Accountancy, 219*(4), 26.

Warner, K., Timme, W., Lowell, B., & Hirshfield, M. (2013). Oceana study reveals seafood fraud nationwide. *Oceana, 11,* 1–69.

Williamson, O. E. (1985). *The economic intstitutions of capitalism*. New York: Simon and Schuster.

Woo, C. (2008). Mattels recalls (2007): Communication implications for quality control, outsourcing and consumer relations. *Arthur. W. Page Society, 2008 Case Study Competition*.

Wowak, K. D., & Boone, C. A. (2015). So many recalls, so little research: a review of the literature and road map for future research. *Journal of Supply Chain Management, 51*(4), 54–72.