Production Planning & Control
The Management of Operations

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/tppc20

Supply chain management in times of crisis: a multi-case study

Christopher M. Durugbo & Zainab Al-Balushi

To cite this article: Christopher M. Durugbo & Zainab Al-Balushi (07 Aug 2024): Supply chain management in times of crisis: a multi-case study, Production Planning & Control, DOI: 10.1080/09537287.2024.2386431

To link to this article: https://doi.org/10.1080/09537287.2024.2386431

PRODUCTION PLANNING & CONTROL
https://doi.org/10.1080/09537287.2024.2386431

Taylor & Francis
Taylor & Francis Group

Supply chain management in times of crisis: a multi-case study

Christopher M. Durugbo[a,b] and Zainab Al-Balushi[c]

[a]Department of Innovation and Technology Management, Arabian Gulf University, Manama, Bahrain; [b]Faculty of Business and Management, Muscat University, Muscat, Oman; [c]Department of Operations Management and Business Statistics, Sultan Qaboos University, Muscat, Oman

ABSTRACT

Relying on an inductive multi-case logic, this study analyses public discourse involving four supply chain crises in Europe: (i) NotPetya Cyberattack on A.P. Møller-Maersk of 2017, (ii) the Evonik industrial accident of 2012, (iii) Cadbury's Salmonella Scare of 2006 and (iv) Horsemeat Scandal of 2013. Grounded on contingency theory, the research finds three main operational vulnerabilities (an MSN of threats) surrounding the investigated cases: Market pressures, Sector dependencies and Network liabilities. The study also identifies four themes of crisis mitigation (4IR measures): (i) intelligence review for reassessments, (ii) integrated relationships for response, (iii) innovation resilience for recovery and (iv) integrity rebuilding for reassurance. Driving these mitigation measures is a customer-first mindset and close customer discussions that strive to restore normalcy, recover operations, and regulate networks. This research is original in its focus on a 'supply chain crisis' paradigm and adds to discourse on competitive and/or restorative capabilities for supply chain management (SCM) in times of crisis. Theoretically, the research advances a 'coactive' SCM strategy for improved SCM performance in times of crisis, and managerially, the value of the research lies in insights on 'best practice' for supply chain crisis management and decisiveness for confront and contain supply chain crises.

ARTICLE HISTORY
Received 14 September 2023
Accepted 15 July 2024

KEYWORDS
Supply chain crisis management; resilience; contingency theory; operations strategy; European supply chains

1. Introduction

Crises plague modern supply chains. Devastating explosions or accidents at distribution centres, healthcare supply chains in times of pandemics, food supply chains in times of food scares, insolvency of supply chain partners and mass product recalls by suppliers are instances of increasingly recurring crises within supply chains. While the Oxford Dictionary (2020) defines a crisis as 'a time of intense difficulty or danger', the Collins Dictionary (2021) defines the term as 'a time of extreme trouble or danger'. Both characterizations imply that a crisis relates to danger (e.g. loss of human life or business insolvency) and is not a conventional disruption or interruption to normal activities. Thus, a supply chain crisis is a time of intense difficulty, extreme trouble or danger for and within a supply chain. Unlike disruptions in supply chains that tend to occur from time-to-time, crises are low probability and high impact events that test the resilience of supply chains, institutions and logistics infrastructure (e.g. seaports and airports) (Notteboom, Pallis, and Rodrigue 2021; Durugbo and Al-Balushi 2023).

Reflecting on the influence of crises on supply chains gives rise to topical supply chain management (SCM) issues for further exploration. For a start, there are research problems to explain the causes and reasons for past crises to aid in supply chain preparedness for future crises (Harland 2021). Typically, the interests lie in unravelling the complexities (Sawyerr and Harrison 2019) that account for an increase in risks and for making the supply chain more operationally vulnerable (Spieske et al. 2022; Al-Balushi and Durugbo 2023). Learning lessons on operational vulnerabilities, i.e. the aspects of operations within supply chains that leave the network exposed, becomes crucial for SCM of crises. In addition, there are research challenges to analyse the range of contingencies and strategies surrounding crises and disruptions to the supply chain (Handfield, Graham, and Burns 2020; Moretto and Caniato 2021). Yet, an analysis of the SCM literature suggests there are limited studies focused on identifying a parsimonious set of contingency factors and mitigation measures from lessons learnt on the management of previous crises within supply chains. This dearth in knowledge serves as the motivation for our research study.

Grounded on contingency theory (Chandler 1962; Lawrence and Lorsch 1967; Thompson 1967; Donaldson 2001), this research aims to explore operational vulnerabilities as contingency factors of SCM in times of crisis and to identify crisis mitigation measures for SCM from comparing previous cases of crises within supply chains. The research involves a multi-case study that sheds light on four relatively recent supply chain crises in Europe: (i) NotPetya Cyberattack on A.P. Møller-Maersk (*NotPetya-M*), (ii) Evonik plant explosion (*Evonik-E*), (iii) Cadbury's Salmonella Scare (*Salmonella-C*) and (iv) Horsemeat Scandal (*Horsegate-S*).

Supply chain crises cost money and a key industrial challenge for manufacturers and suppliers is to minimize the risks of severe socioeconomic consequences from these crises. For instance, the Rana Plaza accident of 2013 in which a clothing factory building collapsed, caused the death of 1134 people in Bangladesh, with manufacturers offering millions

CONTACT Christopher M. Durugbo mcmillanod@agu.edu.bh; Zainab Al-Balushi zeinaba@squ.edu.om

of US dollars in compensation to the injured workers and families of deceased. More recently, the Suez Canal obstruction of 2021 in which the Ever Given freighter blocked the waterway for six days, cost $400 million per hour to global economy. This situation impacted 30% of global container trade, with trade volume through the Canal decreasing by as much as 42% in the aftermath of the crisis (Notteboom, Haralambides, and Cullinane 2024). Additionally, industry data suggests that recent supply chain crises and disruptions are costing firms as much as 45% in loss of profits (McKinsey Global Institute 2021) and an overall 6 to 10% loss of annual revenues (The Economist Intelligence Unit 2021). Thus, our study is important because, according to authors, such as Faruquee, Paulraj, and Irawan (2023) and Chiarini, Grando, and Belvedere (2023), it is imperative that manufacturers gain a deep understanding of the capabilities and approaches that provide answers to crises. Lessons learnt from past crises are essential to gaining this understanding that curbs the costs of crisis response and resilience. Simultaneously, our research has practical and industrial importance for suppliers who must find ways to reduce operational vulnerabilities because supply chain crises have national security implications. For instance, the joint Supply Chain Resilience Initiative by Australia, India and Japan, the Action Plan on Critical Raw Materials by the European Union, and the Endless Frontier Act (later modified as the CHIPS and Science Act) by the United States are supplier-targeted responses by various countries to the supply chain crises induced by COVID-19, digital advancement and competitiveness of countries. Informed largely by lessons learnt and insights from past crises and potential threats, these initiatives target strategic partnerships (Dubey et al. 2024), sourcing (Andaloussi 2023) and investment (Durugbo and Al-Balushi 2023) for supply chain diversification and innovation, and access to critical materials.

Using the *NotPetya-M*, *Evonik-E*, *Salmonella-C* and *Horsegate-S* cases, this research seeks to advance and contribute to existing SCM theory in two distinct ways. First, the study provides new critical insights into operational vulnerabilities as contingency factors that influence SCM in times of crisis. Second, and with close links to the first contribution, the research analyses mitigation strategies that determine efficacy of response and recovery from supply chain crises with a view to supporting future SCM in times of crisis that is contingent on various operational vulnerabilities. Overall, our contributions seek to clarify the tenuous links between supply chains and crisis, which underpin an area of sharp focus for SCM literature (Bassett et al. 2021; Fearne et al. 2021), but we also advance a contingency theory for SCM in times of crisis. Along these lines, an importance and value of our work for industrial practice is the identification of best practices learnt from previous crises (Min 2023a). Lessons learnt have emerged as potent factors for developing crisis management plans that aid suppliers and manufacturers cope with unforeseen risks, handle shocks to supply chains, and continue deliveries to customers (Fearne et al. 2021; Harland 2021; Kovács and Sigala 2021; Ye et al. 2022; Durugbo and Al-Balushi 2023; Vega, Arvidsson, and Saïah 2023; Notteboom, Haralambides, and Cullinane 2024; Zhao et al. 2024).

In line with existing literature (e.g. Heras-Saizarbitoria, Boiral, and Arana (2016), Azghandi, Griffin, and Jalali (2018) and Durugbo and Al-Balushi (2023)), our research distinguishes between two main crisis-related situations for SCM. The first is a crisis occurring outside the supply chain, which underpins, for instance, humanitarian supply chains and the SCM mandate is for response to regional and global demands and hardships – this is not the focus for our research. Rather, the interest in this research lies in the second situation, involving a crisis inside the supply chain and this situation represents the raison d'être of SCM for product contaminations, mass recalls, production interruptions and capacity crises. In so doing, this research seeks to offer better understanding of contingencies surrounding crises and disruptions within supply chains and to advance discourse on SCM in times of crisis. Motivated by the aim, focus and contributions, this study confronts the following questions:

RQ1. What operational vulnerabilities account for and impact supply chain crises?

RQ2. How do supply chain managers mitigate the effects of supply chain crises, under the operational vulnerabilities that act as contingency factors?

Mainly targeting the global community of SCM researchers and practitioners, our key message is that operational vulnerabilities (as contingency factors) aid in understanding (and moderates) how crisis mitigation contributes to SCM (performance) in times of crisis.

2. Research background

Traditionally focused on public servants, government agencies and insurance firms (Hale and Moberg 2005), research concerning times of crisis has over the years gained traction in SCM and received renewed focus due to the pervasive influences of relatively recent incidents, such as the financial crisis and COVID-19 (Durugbo and Al-Balushi 2023). Thus, the supply chain crisis paradigm connects scholarly research on SCM with the concerns of operations strategists and logistics managers, who are seeking to harness decisiveness that is proactive and reactive (Desoutter and Lavissière 2018). Measures for proactivity seek to avert a crisis while reactivity measures strive to overcome critical problems created by a crisis which is usually unpredictable but not always unexpected.

Ontologically, the life of a crisis begins when a disaster, emergency, standoff or scandal breaks out and disruptions continues during response and recovery phases that establish a new normal (Pashapour et al. 2019). The range of impacts during supply chain crisis relates to death or significant injuries, severe distrust and disruption to operations, intense negative public perception, financial strain and insolvency, major loss of staff morale and so on (Hale and Moberg 2005; Li et al. 2012; Ponis and Koronis 2012; Durugbo and Al-Balushi 2023). Much like crises, supply chain disruptions are unplanned events and situations that hinder and disturb normal flow of goods and provision of services

(Spieske et al. 2022). However, a crisis is not attributable to conventional disruptions due to poor quality or failure of delivery from supplier, rising commodity prices or other cash flow issues and internal issues (Hittle and Leonard 2011). Despite being a natural consequence of entrepreneurial activity (Wagner, Mizgier, and Papageorgiou 2017), supply chain disruptions remain substantial threats to companies due to potential drops in long-run stock price performance and negative returns on their stock prices compared to benchmark portfolios (Grötsch, Blome, and Schleper 2013). Additionally, disruptions have widespread negative effects on firms in terms of lower performance and reputational damage (Wagner, Mizgier, and Papageorgiou 2017; Pashapour et al. 2019).

2.1. Supply chains and crisis

According to Natarajarathinam, Capar, and Narayanan (2009), a supply chain crisis occurs due to an interruption in the activities of supply chain actor(s) and this interruption results in a major disruption to the normal flow of goods or services. These interruptions incur direct and indirect costs of response to the crisis, e.g. recall costs for consumer products amount to $700 billion yearly in the United States (Memon, Lee, and Mari 2015). Interruptions stem from problems, such as reduced capital stock (Pashapour et al. 2019) and rapid surges in logistic activities (Narasimha, Jena, and Majhi 2021). However, a crisis could stem from perceptions, for instance, in the case of fuel panics (i.e. panic buying of fuel by drivers) in the United Kingdom during September 2000 and March 2012 where direct-action protests and political warnings of a possible future supply chain disruption created public anxiety and spikes in fuel demands (Upton and Nuttall 2014). Similarly, crises may stem from corporate scandals (Kassahun et al. 2014) or deep tensions with potential standoffs between supply chain partners (e.g. farmers, food companies and retailers) (Arcidiacono 2018) without immediate interruptions to the normal flow of goods or services. Due to the nature of firm-to-firm trade that characterizes supply chains (Chacha, Kirui, and Wiedemann 2024), there is a high likelihood that a crisis will transmit and amplify socioeconomic shocks to supply chain partners *via* cumulative, combinative, complicating and cascading effects, as suggested in Durugbo and Al-Balushi (2023).

In the literature, approaches to compartmentalize supply chain crisis, from an organizational perspective, entail analysing *internal* or *external* causes and the far-reaching consequences for focal organizations, supply networks and external environments (Hermann 1963; Natarajarathinam, Capar, and Narayanan 2009; Pfohl, Köhler, and Thomas 2010; Withers, Corley, and Hillman 2012; Heras-Saizarbitoria, Boiral, and Arana 2016; Azghandi, Griffin, and Jalali 2018). For instance, socioeconomic shocks due to major external events, such as the COVID-19 pandemic (Craighead, Ketchen, and Darby 2020; Ivanov 2022) and the financial crisis (Blome and Schoenherr 2011; Leeuw et al. 2015), trigger crisis in the supply chain resulting in extensive disruptions and additional country- and industry-level spill-over effects and extreme demand and supply shifts. These events create severe uncertainties in global demand and disruptions to global supply chains with imperatives for mitigation steps that involve supply chain optimization for safety stock, on-time delivery and digitalization for end-to-end transparency (Ye et al. 2022). However, for crisis due to internal causes and occurring inside the supply chain, managers contend with strategic decisions, such as workforce management, destruction of supply chain produce, reduction in production capacity and intensification of containment and sanitary conditions (Barton 1991; Vo and Thiel 2011; Wojtczuk-Turek, Turek, and Mitręga 2022). For instance, the 1990 detection of abnormal traces of benzene in the French-based Perrier's bottled water led to a recall of 70 million water products, and the 2003 avian influenza (bird flu) crisis in Netherlands resulted in the putting down of 30 million birds. Another commonly made distinction in the literature is between *natural crises* due to natural disasters like earthquakes or flooding, and *man-made crises* due to human actions like terrorist attacks or human trafficking (Natarajarathinam, Capar, and Narayanan 2009; Baldini et al. 2012) that pose conundrums for crisis management. One approach distinguishes between crisis as befalling an organization, being manufactured or being escalations from accidents or disruptions (Curtin, Hayman and Husein 2005). Geographical foci on supply chain crisis suggest a classification according to single stage (or company), supply chain and regional scales (Natarajarathinam, Capar, and Narayanan 2009). There are also risk-based perspectives that classify supply chain crises according to crisis event predictability, severity and cascading effects (Baldini et al. 2012).

Due to the complex characteristics of systems (e.g. healthcare and food systems) supported by supply chains, crises often pose complex, wicked and ill-defined problems (Do et al. 2021). In non-normal situations induced by crises, performance effectiveness is no longer merely a function of capability, rather the effective deployment of capabilities warrant creativity, flexibility and pragmatism to navigate the of inherent tensions of the crises (Harland 2021). Despite negative implications of crisis, an analysis of literature suggests the occurrence of a crisis hastens the re-examination of ineffective business models by firms (Panwar, Vlosky, and Hansen 2012) and prompts waves of organizational and supply chain upgrades, rebranding, reconfigurations and restructuring for more agile and resilient production networks (Sass and Szalavetz 2013; Vega, Arvidsson, and Saïah 2023; Notteboom, Haralambides, and Cullinane 2024). Crises also create windows of opportunity for non-distressed firms to outperform their distressed counterparts (Liu 2013), for internationalization ventures by non-distressed domestic firms (Domański et al. 2013), and for growth opportunity of non-distressed firms to solve crisis-induced problems, such as telecommunications services for stay-at-home workers (Overby et al. 2004).

2.2. Supply chain management in times of crisis

Operational vulnerabilities circumscribe SCM in times of crisis, and have been long considered a major problem for the

management of production systems (Asbjornslett 1999). Vulnerability, for a supply chain, means 'an exposure to serious disturbance, arising from risks within the supply chain as well as risks external to the supply chain' (Christopher and Peck 2004; p. 3), and at least two important phenomena account for vulnerability and susceptibility to crises in modern supply chains. First, globalization that connects different sectors to global markets is a megatrend with 'tele-connected vulnerability', i.e. vulnerability of sectors to processes occurring at multiple spatial and temporal scales (Bassett et al. 2021). Due to global connections, there is a lengthening and stretching of supply chains that quickly turns faults and disruptions into a crisis (Blome and Schoenherr 2011; Hittle and Leonard 2011). Longer supply chains render supply chain partners more vulnerable (Levine 2012) and exposed to risks particularly in regard to critical materials (Sprecher et al. 2017) and potential problems in production capacity, product quality or supply variability (Poberschnigg, Pimenta, and Hilletofth 2020). There are also greater potentials for volatility and complexity that increase the fragility of supply chains (Johnson, Elliott, and Drake 2013). Thus, globalization is often cited by SCM scholars as accounting for operational vulnerabilities that magnify the severities and shocks of disease outbreaks (Overby et al. 2004; Tan and Enderwick 2006), financial crisis (Panwar, Vlosky, and Hansen 2012; Wang et al. 2018), food safety crisis (Manning 2007, Leeuw et al. 2015) and capacity crisis (Dibben et al. 2020).

Second, digitalization produces contradictory effects on supply chains because on the one hand digital inclusion improves agility (Dubey et al. 2024) and reduces the operational vulnerability of supply chain actors, such as smallholder farmers (Quayson, Bai, and Osei 2020), but on the other hand, digitalization especially through increasing internet use in society also fuels illegal international supply chains, procurement and counterfeit practices (Mackey and Liang 2011; Fischbacher-Smith and Smith 2015). Due to these effects, SCM scholars note unique challenges of public organizations as laggards in information technology (IT) use (Li et al. 2017) potentially creating integration challenges in times of crisis. On the whole, vulnerabilities due to both globalization and digitalization magnifies the effects of a crisis or disruption through snowballing (Sprecher et al. 2017) and weakest link (Levine 2012) effects that cascade the interruption or break from a 'troubled' more fragile origin and unravels the whole network.

Viewed from a digitalization and globalization perspective, some of the most critical problems of SCM in times of crisis relate to technology, trust, transactions and transportation. Technology problems stem from the pervasive impact of digitalization and IT use in business operations and the emergence of cyber supply chains that link supply chains *via* virtual networks (Boyson 2014), heightening prospects for cyberattacks (Boyes 2015) and requiring careful considerations and caution when applying high-risk technologies (Boin, Kofman-Bos, and Overdijk 2004). Trust problems are relational and reputational in nature with origins that lie in imbalanced relationships between producers and distributors (Arcidiacono 2018; Chammem et al. 2018), product safety incidents that trigger loss of confidence in brands and corrode trust in supply chains (Gao et al. 2012), and partner incompetence to fulfil contracts and collaborate with other partners (Li et al. 2012). Transaction problems concern understanding various network structures, embedded actors and agents and echelons for direct and indirect trade connections (Pinior et al. 2012). This understanding ensures better distribution of liability among agents (Banterle and Stranieri 2008) and supports the complexity of interactions that create vulnerabilities (Barnes and Oloruntoba 2005). Transportation problems relate to optimal movement mechanisms to facilitate resource flow and demand fulfilment, particularly international shipment (e.g. containers containing materials and products to consignees) from warehouses by rail or road, and port-to-port via ships or air transport (Meyer-Larsen et al. 2012). Here, the concern is for transportation disruption due to a range of issues concerning the well-being of truck drivers (Boyce 2016), vehicle fuel distribution (Upton and Nuttall 2014) and global logistics systems that integrate transport, handling, and storage (Mazzarino 2012; von der Gracht and Darkow 2013). Other issues entail the transport capacity planning, safety stocks, cargo volumes and security demands due to sea piracy (Urciuoli et al. 2014), shipping conditions (Benson 2011), maritime trading systems (Barnes and Oloruntoba 2005) and shipyard activity within maritime cluster (Koilo and Grytten 2019). In relation to these problems, SCM researchers note that the cross-border and tight interdependencies between actors of domestic and international networks (Merz, Hiete, and Bertsch 2009; Pinior et al. 2012; Burns and Marx 2014) increase the susceptibility and vulnerabilities of supply chains to transmit, cascade or ripple the impact of crisis events and situations to far-off supply chain links.

Typical SCM responses to problems and risks of disruptions and crises include reactive (damage reduction for speedy recovery) and proactive (preventative approaches) (Kleindorfer et al. 2003; Elluru et al. 2019; Al-Balushi and Durugbo 2023) with researchers arguing for more proactiveness at organizational, inter-organizational and managerial levels (Buttermann, Germain, and Iyer 2008; Grötsch, Blome, and Schleper 2013). Here, the interest is in preparedness and prevention (Roshan, Tavakkoli-Moghaddam, and Rahimi 2019) that entail cultivating proactive management attitudes (Desoutter and Lavissière 2018) and averting potential paralysis in decision making (Rosenthal, Boin, and Comfort 2001). Contemporary research further emphasizes relationship dynamics for SCM in times of crisis with spotlights on shock-induced trading relationships typified by craftmanship-induced buyer dependence and market-position-induced supplier dependence (Karaosman, Marshall, and Villena 2023; Chacha, Kirui, and Wiedemann 2024). There are also SCM measures that shift supply chains *via* re-shoring, near-shoring, shipping alliance arrangements and chassis legacy contracts (Kent and Haralambides 2022). In this context, crisis simulations offer mechanisms for educating and bridging gaps between theory and practice (Boin, Kofman-Bos, and Overdijk 2004) and for studying disparities in management strategies (Chong et al. 2014). For instance, the development

of slack capacity that provides resiliency (Kent and Haralambides 2022) needs to be balanced with optimized capacity that guarantees safety stock levels and on-time delivery (Ye et al. 2022).

Importantly, suppliers are aware that that there is no one-size-fits-all supply chain strategy, accentuating the role of trade-offs for achieving operational objectives and such trade-offs may change in times of crisis (von Falkenhausen, Fleischmann, and Bode 2019; Siebert, Brandenburg, and Siebert 2020; AlMalki and Durugbo 2023). For instance, there are SCM challenges for trade-offs in the amount of product and process traceability that aids securitization, regionalization and centralization of supply chain structures during crises like disease outbreaks, food scares or product contaminations (Lu et al. 2019; Durugbo et al. 2022; Razak, Hendry, and Stevenson 2023; Vega, Arvidsson, and Saïah 2023). Additionally, global crises shed the spotlight on the status of supply chains because these crises make material dependencies more apparent and raise political and societal debate on dealing with the crises (Dewick, Hofstetter, and Schroeder 2021). Efficacy of supply chains becomes paramount as firms consider evolutions or revolutions in practice by industry sectors and institutions. Accordingly, SCM literature suggests growing interests in 'best practice' (Li et al. 2017) studies of supply chain crisis with attention varying according to foresight-based procurement (Allal-Chérif and Maira 2011), holistic risk management (Blome and Schoenherr 2011), resource and partner reconfiguration (Chang and Lin 2019; Vega, Arvidsson, and Saïah 2023) and compatibility of human resources (Dibben et al. 2020). These studies represent efforts to consolidate the competitive and/or restorative capabilities of SCM in times of crisis (Durugbo et al. 2022). In support of these efforts, this research advances current discourse with specific insights on contingencies from recent cases of supply chain crises.

2.3. Industrial challenges and relevance of supply chain crises

Industrial systems are increasingly complex due to varied work-life activities (Bai, Sarkis, and Xue 2024) and the fragilities and vulnerabilities of modern supply networks (Durugbo and Al-Balushi 2023). From earlier spotlights on the efficacy, i.e. efficiency and effectiveness, of production systems that create industrial products (Asbjornslett 1999), the frontiers of industrial systems have expanded to encompass collaborative networks and intelligence for global outsourcing, digital transformation, smart manufacturing, innovativeness and environmental friendliness (Durugbo 2016; Karaosman, Marshall, and Villena 2023; Min 2023a, 2023b; Andaloussi 2023; Dubey et al. 2024).

During times of supply chain crises, the resilience of industrial systems is particularly crucial because the economic distress of a major manufacturing firm could cascade to suppliers with significant loss in revenue and supplier insolvencies (Karaosman, Marshall, and Villena 2023) as well as trigger severe shortages of consumer products, essential resources and skilled labour (Durugbo and Al-Balushi 2023). For these times, there is an urgent manufacturing need to deliver immediate short-term solutions for response and relief to those affected by the crisis or dealing with the crisis effects (Primo et al. 2021; Durugbo and Al-Balushi 2023). Crucially, industrial strategists require knowledge of operational vulnerabilities surrounding the crises to devise additional health and safety measures for industrial workers and to understand the incurred costs and time for safeguarding resources (Zhao et al. 2024). Furthermore, as the crisis evolves, suppliers and other industry experts must ponder and decide on the sustained use of short-term 'fire-fighting' adaptive steps or the implementation of long-term 'problem solving' structural adjustments (Notteboom, Haralambides, and Cullinane 2024).

Ensuring industrial systems and supply chains return to normalcy when perturbed by crises or disruptions remains a major industrial concern. In this regard, past research encourages supply chain managers to employ situational understanding for decisiveness during crisis response and recovery with emphasis on cultural value orientations (Zhao et al. 2024). Unlike more mature generative cultures for crisis management that perform periodic drills based on simulated crisis situations, a proactive culture documents and maintains current policies and plans for managing crises based on lessons learnt from previous crises (Min 2023a). Previous studies also serve as a warning for managers of lower-tier suppliers on the need for crisis mitigation approaches because some firms in times of crisis tend to be exploitative and driven by self-interests, leaving suppliers vulnerable and/or in significant financial distress (Karaosman, Marshall, and Villena 2023). Insights from lessons learnt may warrant fundamental rethinks of SCM premised on the management of emergent or underlying industrial risks (Durugbo et al. 2020; Dubey et al. 2024). In the quest for agility, visibility and resilience, lessons learnt from past crises enrich current debates concerning top-down *vs.* bottom-up (Primo et al. 2021), proactive vs reactive, globalization *vs.* localization (or regionalization) and inshoring *vs.* offshoring SCM strategies (Elluru et al. 2019; Dewick, Hofstetter, and Schroeder 2021; Kent and Haralambides 2022).

2.4. Conceptual framework: a contingency perspective

Contingency theory (Chandler 1962; Lawrence and Lorsch 1967; Thompson 1967; Donaldson 2001) informs this study due to our fact-finding interest in the contingency (i.e. situational and contextual) factors that influence the link between crisis mitigation and the performance of SCM in times of crisis. In literature, SCM repertoires for crisis mitigation vary with interests in insurance, inventory, sourcing, rerouting, demand management and contingency stocks as tactics for mitigating disruptions (Tomlin 2006; VanVactor 2011; Karaosman, Marshall, and Villena 2023; Andaloussi 2023). Multidisciplinary teams and taskforces deliver timely responses that mitigate the situation (Fearne et al. 2021), and there are examinations of crisis mitigations in the form of buffering and bridging (Al-Balushi and Durugbo 2020; Spieske et al. 2022; Min 2023b), and borrowing/lending

materials from organizations within the same sector (Kovács and Sigala 2021).

Contingency theory postulates that 'organizational effectiveness results from fitting characteristics of the organization, such as its structure, to contingencies that reflect the situation of the organization' (Donaldson 2001; p. 1). Thus, the premise of the theory is that there is no transcendent way of functioning because different environments offer different antecedents. Instead, the performance of organizational functions and activities depends on organizational-related contextual factors, such as individuals, processes, time and strategies. Another core argument of contingency approaches is that 'the effect of one variable on another depends upon some third variable' (Donaldson 2001; p. 6) with multiple pathways for explaining organizational viewpoints (Csaszar and Ostler 2020). This third variable in essentially a moderator with varied focus in research studies, and in the case of this study, operational vulnerabilities.

Based on contingency theory, the expectation is that crisis mitigation 'fits' with operational vulnerability, as shown by Figure 1. According to Wagner and Bode (2006), this vulnerability grows and spreads in a supply chain with increased customer and supplier dependence, supplier concentration, single and global sourcing. Literature notes vulnerabilities of supply chains in terms of lack of infrastructure development of developing economies (Harpring et al. 2021), past supplier insolvencies (Grötsch, Blome, and Schleper 2013) and lack of inventory visibility (Harland et al. 2021). Broadly, there are suggestions that recent emphasis on Just-In-Time (JIT) philosophy magnifies the vulnerability of supply chains because JIT processes under normal situations leave minimal room for error (Farahani, Shavandi, and Rahmani 2017) and there have been spotlights on how some companies exert their dominance, i.e. dependence and power, within the supply chain, focusing on self-interest and rendering lower-tier suppliers financially vulnerable (Karaosman, Marshall, and Villena 2023). Similarly, heavy reliance on low-cost countries for sourcing needs (Min and Kim 2011) and risk dependencies within supply networks (Al-Balushi and Durugbo 2020, 2023), add to the vulnerability of supply chains.

Although previously limited in SCM literature (Buttermann, Germain, and Iyer 2008), contingency theory continues to garner interest and acceptance among SCM researchers (e.g. Cao et al. (2015); von Falkenhausen, Fleischmann, and Bode (2019) and Romero-Silva, Santos, and Hurtado-Hernández (2024) as an avenue for connecting SCM strategies to performance with particular interest in internal and external fit between SCM strategies, environment and practices (Prajogo, Mena, and Nair 2018). Related SCM studies posit on contingencies such as past supplier insolvencies that explain supply chain risk management proactiveness (Grötsch, Blome, and Schleper 2013), environmental uncertainties and unpredictability that account for integration (Buttermann, Germain, and Iyer 2008; Wong, Boon-Itt, and Wong 2011) and supply chain finance on social and environmental performance during crisis (Moretto and Caniato 2021). In these contexts, there are distinctions made between the effects of internal and external groups of contingency outcomes and variables, where operational factors mainly account for the internal contingencies, while environmental factors predominantly constitute the external contingencies . Using novel arguments on management-performance links, SCM researchers examine the strengthening of these links under high internal and external contingencies.

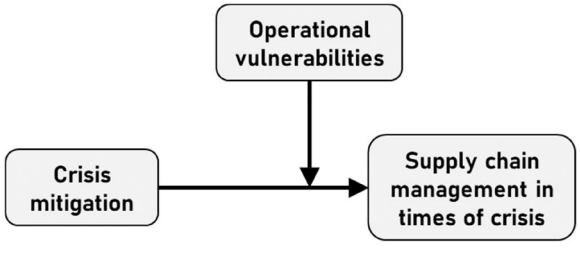

Figure 1. Preliminary contingency-based framing for case study.

In line with Wagner and Bode (2006), this study posits that vulnerability is a contingency factor for certain supply chain characteristics (i.e. SCM in times of crisis) and that crisis mitigation (as well as incurred losses) by supply chain partners stem from this vulnerability to a particular supply chain crisis. Specific focus for this study is on the operational vulnerability, arising within the supply chain (Christopher and Peck 2004) and the crisis, also within the supply chain (Natarajarathinam, Capar, and Narayanan 2009; Hittle and Leonard 2011). The next section outlines the methodology for the research regarding the rationale for the case study, adopted methods and research philosophy.

3. Research methodology

Grounded on contingency theory (Chandler 1962; Lawrence and Lorsch 1967; Thompson 1967; Donaldson 2001), this research applies an inductive, qualitative multi-case approach to explore operational vulnerabilities and crisis mitigation within European supply chains. The multi-case logic serves as the focus because it enables in-depth understanding of an examined phenomenon and how it has evolved (Eisenhardt and Graebner 2007; Yin 2013, 2017). Compared to quantitative approaches, such as surveys and experiments, interviews aid in garnering data from information-rich cases and uniquely confront the 'how' and 'what' of SCM in times of crisis posed by **RQ1** and **RQ2**. Furthermore, the inductive stance (Denzin 2007) supports the use of observations for contexts (i.e. operational vulnerabilities and crisis mitigation) and initial framings for research (i.e. Figure 1) as starting points for alternating between collecting data and building theory.

Additionally, the research follows an interpretivist epistemology (Walsham 1993), which sheds light on the languages used and meanings within investigated case. Focus on interpretivism is pivotal to this research study due to use and analysis of qualitative data. Considering the overall approach, we defined our unit of reference as operational vulnerabilities and crisis mitigation for supply chains, and our unit of analysis as European supply chains. The next subsections describe the case study domain and how data were captured and analysed.

3.1. Case selection and rationale

Four crises within European supply chains provide the case studies: the *NotPetya* cyberattack (2017) on the Danish shipping firm Maersk, the *Evonik* industrial accident (2012) in Germany, Cadbury's *Salmonella* Scare (2006) in the United Kingdom and the *Horsemeat* Scandal (2013) in most of Europe with original detection in Ireland. The selected number of cases is amidst the accepted case study range that falls between two and fifteen (Perry 1998). The rationale for these cases is 2-fold.

First, all cases, in line with the aim and focus of this research, are instances of crisis inside the supply chain. The cases relate to danger and damages specific to the supply chain and exclude multi-faceted crises, such as pandemics, political turmoil or financial crises where the origins tend to be outside the supply chain and the impacts are varied. Additionally, the selection of cases seeks varied contexts to shed light on commonalities in operational vulnerabilities for supply chains and to offer extensive and deep insights on crises within supply chains as part of conducting case study research (Yin 2017). Two cases (*Salmonella-C* and *Horsemeat*) relate to a food scare and scandal associated with widespread product contamination while the other two cases (*NotPetya-M* and *Evonik-E*) pertain to an industrial accident and cyberattack that created severe production interruptions. Generally, the cases are due to two main sources:

i. bad actors – internal (*Horsegate*) and external (*NotPetya*) to the supply chain and
ii. industrial incidents – due to a major fire from a plant explosion (*Evonik-E*) and a leaking pipe (*Salmonella*) which accounted for severe disruptions to the supply chain.

The cases also offer samples of business-to-business (B2B) (*NotPetya-M* and *Evonik-E*) and business-to-consumer (B2C) (*Salmonella-C,* and *Horsegate*) supply networks, where the B2B instances provide services that facilitate logistics and the B2C instances deliver consumer food products. Although varied in context, duration, and setting, a unifying theme for the cases is that the crisis occurred within and affected the supply chain.

Second, the cases are relatively recent and high-profile European cases with influences and implications on global value chains, which increases the prospect of public discourse, but more importantly, these crises, are now over. European supply chains evolve depending on the contextual and situational factors of their industries and this evolution characteristically depends on digitalization (Pessot et al. 2021). Involvement in global networks remains a hallmark of European supply chains, as evident by the operations of the firms of the selected cases. Cadbury operates in 60 countries, Maersk operates worldwide, Evonik has operations in 100 countries, while the major European retailers, impacted by Horsegate, such as Aldi, Dunnes Stores, Iceland, Lidl and Tesco, own stores, and facilities, across the globe. Rather than drawing inferences about some larger population, this study seeks analytic generalization wherein the extracted ideas from case studies' findings can be applied to newer situations other than the cases in the original study (Yin 2013).

3.2. Case data and sourcing

Data for this research study originates from *public discourse* and intends to capture web available information on the selected cases and to transform the information into knowledge with practical lessons that advance SCM scholarship. Recent SCM studies present prospects of public discourse for investigating crisis in supply chains (e.g. Bapuji and Beamish (2019) and Mammadova, Behagel, and Masiero (2020)), and this study adds to SCM scholarship through focusing on SCM in times of crisis, from a contingency perspective. As secondary sources of data (Stewart and Kamins 1993), public discourse are speeches, publications and other statements made in pursuit of the public good (Sellers 2003).

Similar to Thompson and Anderson (2021), this research uses data from contemporaneous newspaper, professional and technical reports. Using the search engines of Google, Bing and Yahoo!, the process of identifying web sources involved searches using the cases, with Boolean operators where appropriate, as search strings, i.e.: (i) 'Cadbury' AND 'Salmonella', (ii) 'Evonik' AND ('fire' OR 'explosion' OR 'accident'), (iii) Horsegate and (iv) 'NotPetya' AND 'Maersk'.

For the sourcing, we input the search strings in the search bars of each search engine, observing significant duplication of sources in the returned results across the different search engines. The searches were conducted initially between April and July 2020 during the initial stages of this research to establish timelines and strengthen motivation. A subsequent search during April, June and December 2022 aids in identifying and gathering sources. Initial results from the search engines are as follows:

i. 'Cadbury' AND 'Salmonella' – Google (58,300 results), Bing (80,700 results) and Yahoo! (495,000 results),
ii. 'Evonik' AND ('fire' OR 'explosion' OR 'accident') – Google (324,000 results), Bing (35,800 results) and Yahoo! (12,900 results),
iii. 'Horsegate' – Google (134,000 results), Bing (21,900 results) and Yahoo! (21,700 results) and
iv. 'NotPetya' AND 'Maersk' – Google (91,100 results), Bing (75,000 results) and Yahoo! (193,000 results).

Focusing on the top 100 results, from each search engine, we then skimmed and scanned successive links for relevance and data saturation. Using main and news web sources from these search engines, this study collected a range of policy statements, annual reports, magazines, newspaper reports, press releases/reports and web pages. Due to the need for a balance in the cross-case analysis and data saturation, we decided to identify and include 20–25 sources from the overall search for each case. Appendix I presents the range of sources that provide the public discourse for this study.

3.3. Data analysis, reliability and validity

For the analysis, the study relies on the thematic analysis approach, which guides researchers in 'identifying, analysing, and reporting patterns (themes) within data' (Braun and

Clarke 2006; p. 79). This is consistent with Miles and Huberman (1994) framework that has three consecutive tasks: data reduction, data display and conclusion drawing. Incorporating thematic analysis offers advantages, such as (i) allowing condensed data into a concise description; (ii) underlining similarities and differences among datasets; (iii) generating unpredicted acumens and unanticipated penetrations (Braun and Clarke 2006); and (iv) delivering a simple method that does not need theoretical details and technical knowledge (Javadi and Zarea 2016). ATLAS.ti software for qualitative data analysis (Friese 2014) offers support for managing the transcription process of generating thematic grouping and coding functionalities. The research also adopts the widely-accepted six-stage thematic analysis process (Braun and Clarke 2006) involving data familiarization, initial code generations, identification of potential themes, review of theme, definition of themes and report production.

Following Thomas (2006), analysis started with careful reading of the collected public data as part of data screening and synthesis, followed by summarizing raw textual data to derive concepts, categories and common themes for developing a framework through elucidations and commentaries that emerge from the raw data during the coding process. In line with the initial framing of Figure 1, and motivated by contingency theory, the investigation involved case-by-case (or within-case) analysis of operational vulnerabilities, as contingency factors, as well as crisis mitigation measures that account for SCM of the crisis. This phase allowed fair treatment of the evidence to produce inductive analytic conclusions (Yin 2017). Converting html files into pdf files aids in importing the web sources into a created ATLAS.ti project (.atlproj22 file). Overall, the collected data for the case study involves 90 documents (21 for *NotPetya-M*, 24 for *Evonik-E*, 22 for *Salmonella-C* and 23 for *Horsegate-S*), as detailed in Appendix I, which contain 89,007 words. Importing the documents paved the way for subsequent steps: (i) to tag quotes and associate each highlighted quote with a concept of interest/importance – termed 'codes' in ATLAS.ti, and (ii) to create code and document groups for generating themes as key findings. The 'memos' feature of ATLAS.ti additionally aids in keeping track of changes while network diagrams provide visualizations of the relationships between 'nodes', i.e. codes, quotations and documents. Implementing the stages of the thematic analysis produced 91 initial codes: 29 on operational vulnerabilities and 62 on crisis mitigation, as shown by the network diagrams of Figures 2 and 3.

Intercoder-reliability using percentage agreement is 96.8% (91/94), and results in dropping three codes beforehand because these codes relate to situations or events in the cases (i.e. (i) Lagos power cut as a source of fortune, (ii) damaging impact of the crisis, and (iii) more 'unknowns' than 'knows'). Aggregating the related codes to identify potential themes generated 16 subthemes (7 sources of vulnerabilities and 9 focuses for mitigation), and further review and refinement produced **7** main themes (3 on operational vulnerabilities and 4 on crisis mitigation) for the reporting stage.

Given that validity in qualitative study is related to the interpretation of themes that arise from the data (Tharenou, Donohue, and Cooper 2007), both researchers for this study independently reviewed the documents comprising the developed themes, and five independent researchers assessed the developed themes. Similar to Thompson and Anderson (2021), this study achieves internal validity through gathering data from multiple sources (e.g. audit committee leadership summit viewpoints, BBC news webpages and Maersk newsletters) and multiple data types (e.g. text, transcripts from interviews in the newspapers and charts in reports). Additionally, the varied perspectives and accounts from varied geographical regions, i.e. different European countries, aid triangulation of information. Furthermore, the use of different globally available main and news web sources seeks to improve the external validity of the research.

4. Research findings

This section presents two sets of findings. First, we describe the findings on the operational vulnerabilities associated with the crisis. These vulnerabilities pose SCM challenges in the lead up to crises and during the response and recovery phases. Second, we outline the results from analysing themes on crisis mitigation measures for SCM performance within the investigated cases. Table 1 offers a within-case analysis on the profiles, triggers and impacts of the case crises, while the next subsections detail the findings on operational vulnerabilities and crisis mitigation, based on the cross-case analysis.

4.1. Operational vulnerabilities for a supply chain crisis

Initial analysis of operational vulnerabilities surrounding the crisis in the investigated cases, identifies three main themes (i.e. an MSN of threats): **M**arket pressures, **S**ector dependencies and **N**etwork liabilities. Table 2 summaries the main sources, challenges for SCM and related cases associated with the different vulnerabilities. The next subsections elaborate on each theme.

4.1.1. Market pressures

From the analysis, market pressures provide the first theme on operational vulnerabilities. Triggered by market forces, these susceptibilities originate from chronic demands to cut operating costs and from persistent price wars. Such pressures place existing supply chain partners in on-going and precarious decision-making situations that affect the sustained competitiveness and continued survival of these partners (independently and as part of the value chain). For instance, commenting on the causes of *Horsegate-S,* Professor ManMohin Sodhi, of the University of London, observes that:

> '**First is the focus on low cost,** leaving very little 'meat on the bones' for any supplier. The supermarket competing on price looks for low-cost suppliers if it has to make money, which in turn look for even lower cost suppliers if they are to make money and so on'.

Similarly, Professor Chris Elliott, of Queen's University, who led the independent inquiry into *Horsegate-S,* noted that:

> 'Recent reports in the media show the emergence of a **new price war** between some major retailers, and suppliers are already under pressure to further reduce prices'.

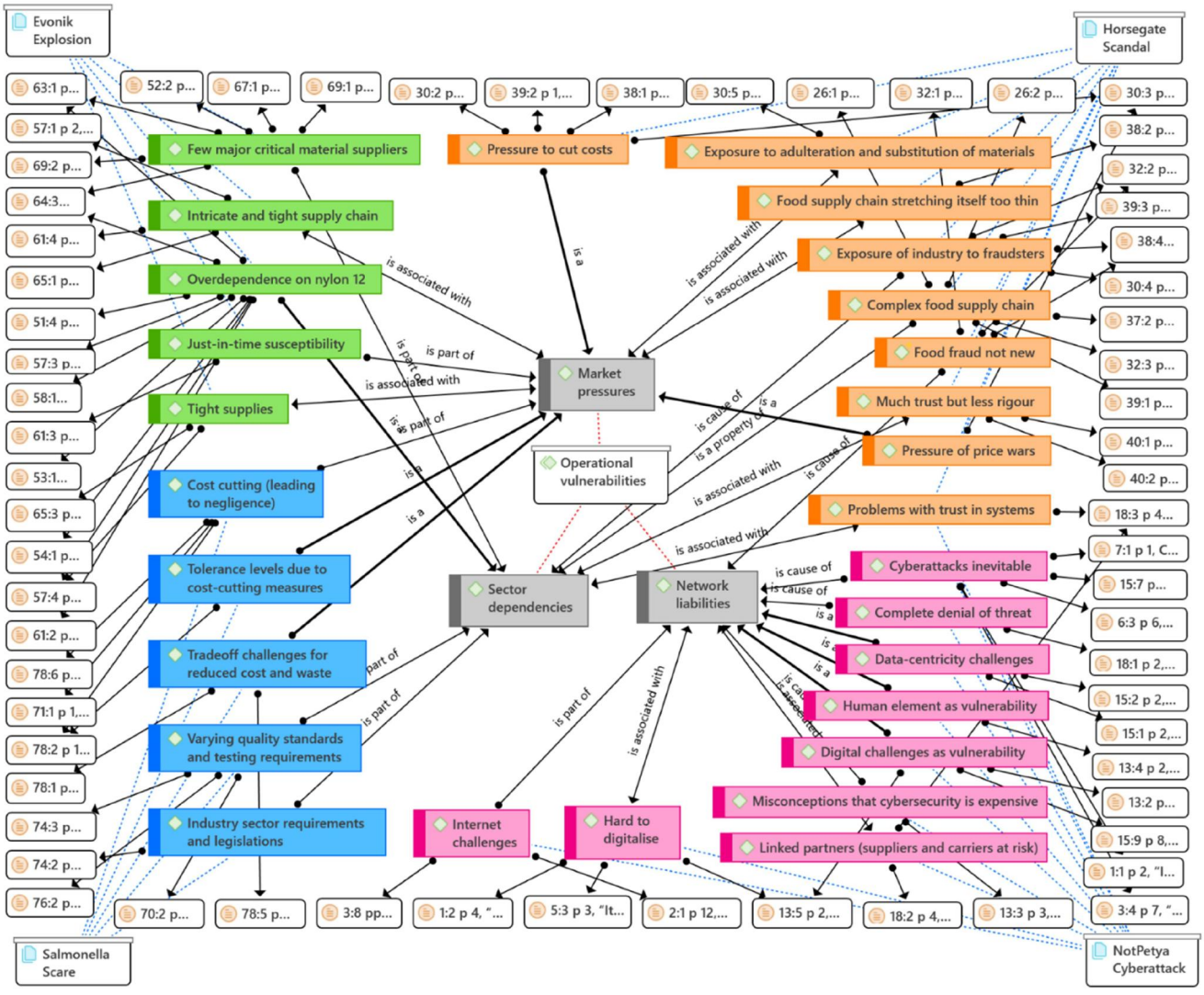

Figure 2. Network diagram on operational vulnerabilities (grey boxes show main themes, other coloured boxes show derived codes/subthemes based on interview excerpts, arrows show the linkages and clear boxes with numbering are some illustrative quotes).

Regarding the *Salmonella-C* case, Recorder James Guthrie QC, presiding in the Birmingham Crown Court during the Cadbury trial for the food scare, stated that:

> 'They then changed it to (allow) what they believed to be an allowable tolerance level. They (Cadbury) sought to save money from wastage by allowing a tolerance for salmonella in their food … The avoidance of wastage and the accompanying benefit of **reducing costs** which accompanied the new system was no doubt welcome and contributed to the lack of scrutiny (which resulted in contamination), which the change ought to have received'.

Market pressures cause firms to create tight supply chains and to run on JIT schedules, which ensure cleanness and leanness of production plants, but as evident by excerpts on the *Evonik-E* case,

> 'All it takes is for one **of those parts to be missing** and an **entire production line** can be shut down … (this tightness) Makes production **susceptible to disruption** when something goes awry' (Huffington Post).

> 'So **tight** is the global car industry's **supply chain** that one break in a small link threatens the lot' (BBC news).

4.1.2. Sector dependencies

Sector dependencies offer the next theme on operational vulnerability. The analysis identifies two main sectoral dependences that expose the supply chain to major loses in times of crisis: partner interdependence and resource overdependence.

Partner interdependence, the first source of dependence exposure, means the complex network of interdependent partners that enables a supply chain to deliver goods and services. For the *Evonik-E* case, which relates to the global automotive supply chain, the Huffington Post observes that:

> 'This incident (i.e., the *Evonik* industrial accident) exposes vulnerabilities in the **world's most complex supply chain, whereby 3,000 individual parts go into each car or truck made**. Each component contains hundreds of other pieces supplied by multiple other companies – such as the rubberized portion of a windshield wiper, the hard metal parts of that wiper or the electronics used for a wiper to move'.

Related interdependencies exist for the regional food supply chain surrounding the *Horsegate-S* cases, as reported by National Geographic, i.e.

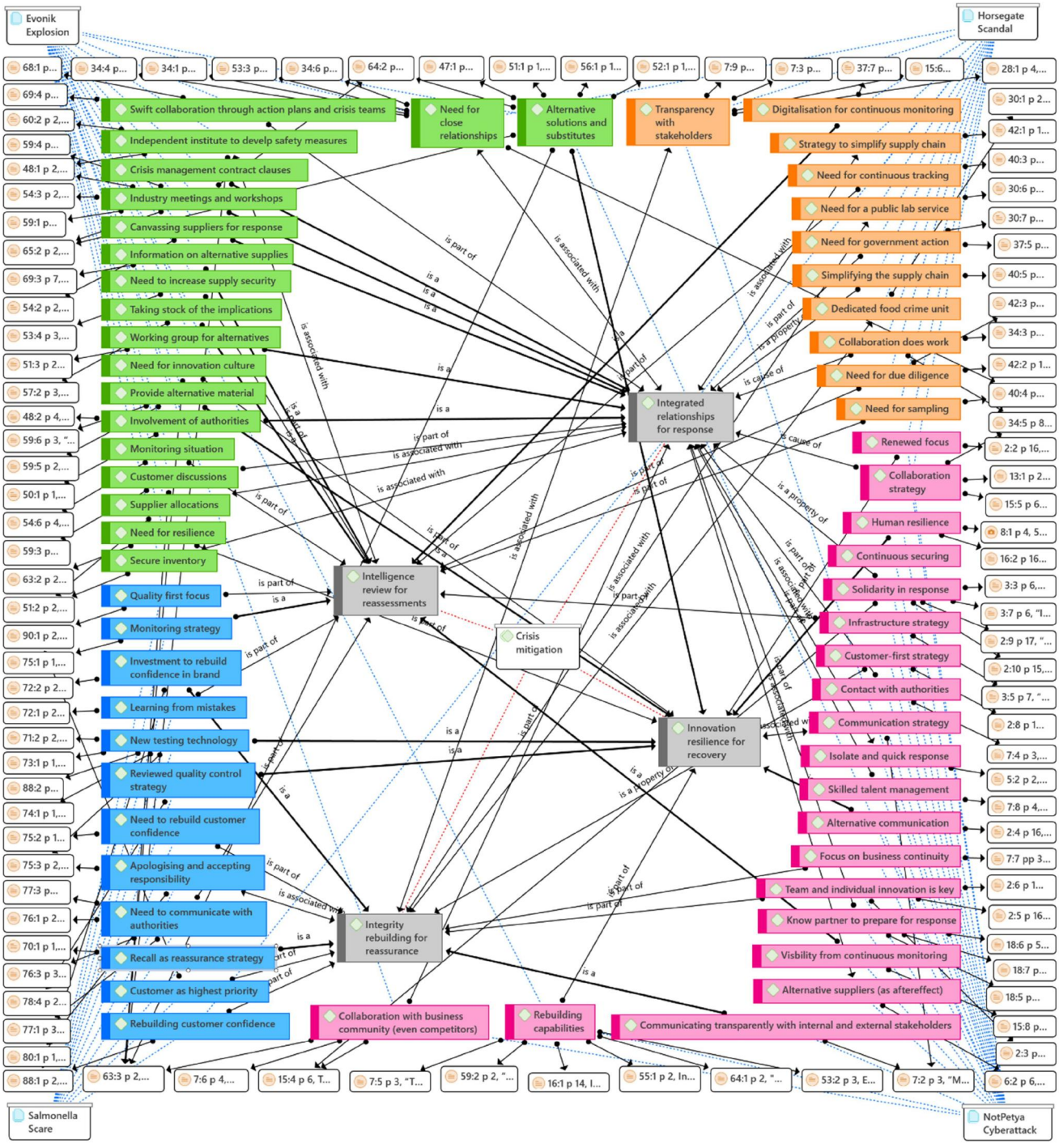

Figure 3. Network diagram on crisis mitigation (grey boxes show main themes, other coloured boxes show derived codes/subthemes based on interview excerpts, arrows show the linkages and clear boxes with numbering are some illustrative quotes).

> 'There are around 450 points at which the integrity of the [**supply**] **chain can break down'.**

> 'Despite the growing farm-to-table trend and ascendant "locavore" mentality, the fact is that much of the way we get our food these days remains **woefully convoluted'.**

Distinctively, within the food industry, there are different sectoral requirements due to varying characteristics of food products. Prof Hugh Pennington at the University of Aberdeen University, in a BBC interview, on the causes of the *Salmonella* outbreak, observed that

> 'The fat in chocolate actually preserves the salmonella from the normal intestinal defences, so you don't have to **eat very many salmonellas to get infected** … It's about a thousand times less than if you're eating it from traditional sources like meats'.

Consequently, quality control measures vary, as suggested by Nick Lowe, team leader of the Birmingham City Council, investigating the outbreak:

> 'They (Cadbury) were using a statistical method that relies on an even spread of the contaminant but that's **not the way it works**. Chocolate is not homogeneous. You could have salmonella in three bars and none in several thousand. You can't measure the risk by averaging out the infection across all the bars'.

Table 1. Overview and within-case analysis of the supply chain crisis cases.

Case	Overview	Synopsis of the crisis	Trigger	Impact
NotPetya cyberattack on Maersk (2017)	Maersk is a Danish-based global shipping and logistics company responsible for 76 ports worldwide, and manages around 900 ships, 4 million containers, 1000 warehouses and a seaborne freight that transports about 15% of global trade by containers. NotPetya is a file-scrambling software targeting Microsoft Windows PCs, impacted businesses in Ukraine and spread to 60 countries	Severe suspension of production affecting suppliers and customers. Nature of crisis: Abruptly – malicious cyberattack Industry sector: Logistics/ transport industry	*Main triggering incident* was the NotPetya Malware infecting parts of the organisation and disabling systems in Maersk's container business. Stimulating and exaggerating factors were: • Complex logistics supply chain • Interdependent and interconnected industry • Data centric and technology dependent • Over-trusting partners' security practices and confidence in technologies' securities	Disruption mainly impacted global logistics On Maersk – Direct revenue losses of about $300 million and additional IT restoration and operational costs in total potential losses amounting to about $20 billion. On upstream relationships – Container terminals shut down, delays in freight upload, long waiting times for ships and trucks, and trucks turned away from terminals. On downstream relationships – Customers unable to place or track orders, overpriced air freight delivery, expired inventory, reputational losses, brand losses and falling stock prices.
Horsemeat scandal across Europe (2013)	The Irish Food Safety Authority found horse DNA in 1/3 of frozen beef burgers sold by Irish and British retailers. Subsequent investigations reveal beef contamination in 13 other European countries with traces of horse DNA in meat imported from outside the EU. Although considered a global issue, response called for EU-wide solutions that started with widespread recalls.	Widespread product-related contamination caused by upstream suppliers Nature of crisis: Gradually – detected equine-contaminated beef burgers Industry sector: Food industry	*Main triggering incident* was deliberate act of beef product contamination with horsemeat. Stimulating and exaggerating factors were: • Complex supply chains, lack of upstream visibility • Over-trusting suppliers, and over-reliant on paperwork • Lack of retailers' direct influence over suppliersEU single market accelerated the spread	Disruption mainly impacted regional (within Europe) consumers Consumers- Trust in food industry and food labels dropped by 24% and 65%, respectively, questions industry's ability to regulate itself, and changes shopping habits. Retailers – Sales of frozen burger and frozen-ready meals dropped by 43% and 13%, respectively, reputational, and financial loss and oblivious brand equity
Evonik industrial accident in Germany (2012)	Evonik is German based company known as a leader in specialty chemicals and is active in more than 100 countries. It's one of the leading suppliers that covers 50% of cyclododecatriene – CDT – chemical's supply particularly for automotive industry worldwide to produce PA12 for brakes and fuel system in cars. The fire caused a shortage in the supply of CDT that had global impact and slow-down in the production of cars. As a solution, car producers had to save the material in inventory until alternative solutions were found.	Severe process-related shortages due to accidental explosion at plant Nature of crisis: Abruptly – Fire caused closure of the chemical plant Industry sector: Transport industry	*Main triggering incident* was the sudden fire in the Marl, Germany plant that led to drop in supply of cyclododecatriene and production of PA12. Stimulating and exaggerating factors were: • Limited number of suppliers for the chemical • Automotive industry was already affected by Tsunami in Japan • Just-in-time approach was applied for the PA12 material that led to lack of safety stockNo alternatives were available in the market	Disruption mainly impacted global car manufacturers Customers (PA12 producers): there were only two suppliers of CDT, the manufacturers had to place orders last minute to the Arkema Customers (car producers): the production of cars was slowed down and companies tried to save the PA12 in inventory. Arkema: pressure of last-minute demand spike was on the company as it was only left as supplier It took 9 months at least for Evonik to re-operate the plant

(*continued*)

Table 1. Continued.

Case	Overview	Synopsis of the crisis	Trigger	Impact
Salmonella Scare at Cadbury (2006)	The Health Protection Agency reported an unusual rise in human cases of salmonella attributed to contaminated Cadbury chocolates. Cadbury is a UK based confectionery brand that produces different kinds of chocolates, gums and candies. An outbreak in the Cadbury plant caused contamination of Salmonella Montevideo – a bacteria that caused poisoning in the chocolate – in Europe. 37 people were poisoned within two months. As a solution Cadbury recalled all the contaminated chocolates from the market and invested further on safety modifications.	Widespread compromised production due to a leaking factory pipe Nature of crisis: Gradually – Contamination of the chocolate (toxicity) Industry sector: Food industry	*Main triggering incident* was the contamination of salmonella Montevideo in various products of Cadbury leading to poisoning of children and adults in the EU region. Stimulating and exaggerating factors were: • Cadbury's failure to inform the authorities about the possibility of contamination although it knew about it 5 months earlier (since January) • The same problem occurred in 2002 but kept hidden from authorities and no corrective actions were taken Old quality control and inspection system	Disruption mainly impacted regional (within Europe) consumers Customers: around 37 people had food poisoning out of 56 cases due to the contamination, this included children. The trust level of the customers dropped. Company: Cadbury lost around £40 million in paying fines, recalling the products, and updating the quality system. Moreover, drop in sales was noticed as its chocolate market shares fell by 2.7%.

Table 2. Operational vulnerabilities within cases.

Themes	Main sources	Supply chain management challenges	Related cases
Market pressures	• Demands to cut operating costs • Persistent price wars	• Maintaining tight and resilient supply chains	• Evonik-E • Salmonella-C • Horsegate
Sector dependencies	• Partner interdependence • Resource overdependence • Excessive trust and dependence on sectoral systems	• Ensuring integrity and integration of supply chain partners • Effective planning and contingencies in anticipation of potential severe shortages	• Evonik-E • Salmonella-C • Horsegate • NotPetya
Network liabilities	• Negligent and bad human actors • Pace and complexity of digitalization	• Coping with changing digital business and security landscape	• Salmonella-C • Horsegate-S • NotPetya-M

Complex interdependence within supply networks also occurs in the shipping and logistics industries, which offers the *NotPetya-M* case, but the focus for this sector is on B2B systems-based connectivity and data-centricity that drive seamless integration of operations, i.e.

> 'This (Maersk) is a **data-centric business …** If you think about the way data is used in this sort of business, unlike financial services, you can lock it up, you can't create a centralized data pool and put every form of defence around it'.

> 'Shippers, forwarders and carriers are **often connected via integrated APIs and ERP systems …** One attack on somebody can boomerang and impact others as well'.

Resource overdependence is the second source of sector-based dependency exposure and is an upstream problem that exists because within some industries, such as the steel and automobile industries, there are limited or no alternative sources of raw and critical material. In these cases, effective planning and contingencies are required, in anticipation of potential severe shortages. For instance, overdependence on the polyamide 12 (PA-12) resin for the automotive sector is suggested by the *Evonik-E* case, and the vulnerability is an upstream problem that relates to the company's large market of PA-12 supply. The following excerpts describe the overdependence vulnerability for supply chains associated with the *Evonik-E* case:

> 'At the time of the incident, Evonik covered about **50**% **of the global production capacity** for CTD, making it a significant point of failure' (Prof Paolo Trucco of Politecnico di Milano and Prof. Alessandra Negri of Università Politecnica delle Marche)'.

> 'Evonik Industries' plant in Germany was responsible for a **good chunk of the world's supply** - one estimate put it between a quarter and a half' (BBC news).

According to Sheryl Toby, co-chair of Dykema's bankruptcy department, the *Evonik-E* case sheds the spotlight on how for supply chains,

> 'In general, it's much harder to get a real handle on **raw-material impact and availability**'.

Similarly, the Detroit Bureau observes that,

> 'The Evonik crisis worsens an already serious problem. **Demand for PA-12 resin** has threatened to outstrip supply for several years as the auto industry began rebounding from its 2009 global crash'.

Subsequent PA-12 shortage due to the explosion and fire at the Evonik factory, underlines the need for on-going sectoral scrutiny of supply chain parts, components and raw materials originating from few (or even a single) suppliers.

The need for scrutiny extends to the systems for innovation and value within different sectors. Due to the closeknit nature and routinization of these systems, certain sectors with time develop trustworthiness and the *Horsegate-S* case offers a context for questioning excessive trust and dependence on these systems. For instance, Professor Chris Elliott, charged with investigating the scandal, speaking at an Environment, Food and Rural Affairs (EFRA) Select Committee meeting in parliament, notes that:

> 'I was surprised at how the supermarkets **very much took on trust**. There was very little rigour, very little verification that people were meeting specifications'.

Similarly, Mr Owen Paterson, the Secretary of State for EFRA from 2010 to 2012, reflecting on sector practices at the time, remarked that he had

> 'a gut feeling and a very clear belief … that **too much is taken on trust** within the current system … at the moment it is very much a paper-based system, too much taken on trust'.

4.1.3. Network liabilities

The next theme on operational vulnerabilities entails the **network liabilities** due to human element and digital demand concerns. Analysis of the various cases identifies the initial network liability as negligent or bad human actors within the network. Human and organizational negligence in the study involves misconceptions and denial of quality and security management practices, and mainly originates from the *NotPetya-M* and *Salmonella-C* cases. For the *NotPetya-M* case, there were initial denials and misconceptions related to the cost of cybersecurity, as suggested by the following excerpts:

> 'Before NotPetya, the maritime industry's **approach to cybersecurity was "complete denial"**'.

> 'Many shipping companies **wrongfully believe** that cyber security has to be expensive. The reality is that often simple, inexpensive, actions will raise security significantly both on the landside and on the vessels'.

For the *Salmonella-C* case, negligence mainly related to human and management failings in assessing threat levels and communicating these levels to relevant authorities, i.e.

> 'Mistakenly, we **did not believe that** (for the Salmonella-C cases) there was a threat to health and thus any requirement to report the incident to the authorities … We accept that this approach was incorrect. Quality has always been at the heart of our business, but the process we followed in the UK in this instance was unacceptable. We have apologised for this and do so again today'

> 'We were told on Monday that there was a problem occurring in January and that problem has gone on for a number of weeks before being corrected. We would have **expected them to tell us'.**

The analysis also identifies bad human actors within the supply network as threats and direct sources of crisis, as suggested by the following excerpts on the *Horsegate-S,* and *NotPetya-M* cases

> 'There has **always been food fraud**. Once upon a time it might have been watered down beer or bread adulterated with sawdust' (BBC).

> 'But the global food supply chain is vast and complex, with ingredients for simple ready meals sourced from multiple countries. The scale of the business means that supermarkets cannot monitor every step of the chain, which could **allow rogue operators** to strike' (Chris Elliott, lead of the UK government's independent review of food supply chains following *Horsegate*).

> '**Cyber-attacks are not going to go away,** and technology is becoming a more strategic asset in the future of our business' (Adam Banks, Chief Information Officer at A.P. Moller – Maersk).

The impact of human actors as potential network liabilities is such that experts consider the human element within the supply chain as the most vulnerable link. According to Phil Tinsley, the Maritime Security Manager at Bimco (a major non-governmental organization for shipping companies), while commenting on the *NotPetya-M* case,

> 'It is **the human element which we believe is the gravest concern**. Why? There is unfortunately still a lack of awareness of the potential severity of a malicious cyber security attack'.

Next, the analysis identifies increased digital liabilities for supply chain partners due to industry and market demand to digitalize supply networks. According to Maersk's CEO, Soren Skou, the challenges for B2B networks are one of complexity, i.e.

> 'It's easy to talk about **digitalising things**; it's quite difficult to do in a B2B environment. It's hard to digitalise that complexity'.

Another perspective on digital liabilities identified by Jens Monrad, senior intel analyst, at FireEye iSight, in relation to the NotPetya-M, centres on the need to keep pace with changing digital business and security needs in tandem with industry threats, i.e

> 'One of the **biggest challenges I see in the shipping and maritime sector** is the **pace of digitalisation in the industry versus the ever-changing threat landscape**. Today a lot of critical functions, commercial and business operations must meet the digitalisation demand, and this has forced industries, including the shipping and maritime sector into meeting demands, which potentially changes the way security was built and designed to secure infrastructure, protect data, customers, and employees'.

4.2. Crisis mitigation for supply chain management in times of crisis

Appendix II provides timelines of the cases. Analysing these timelines indicates that the trigger for a crisis is when authorities detect an emergency at a focal firm along the supply network (*Horsegate*) or from clients of the focal firm (*Salmonella-C*), or a focal firm detects an emergency and contacts the authorities (*Evonik-E* and *NotPetya*), as summarized by Figure 4.

Notification of authorities (and those impacted) is a requirement of organizations, with failures resulting in potentially significant consequences for supply chain partners. For instance, the General Data Protection Regulation (GDPR) that safeguards the data of European citizens enforces a 72-h

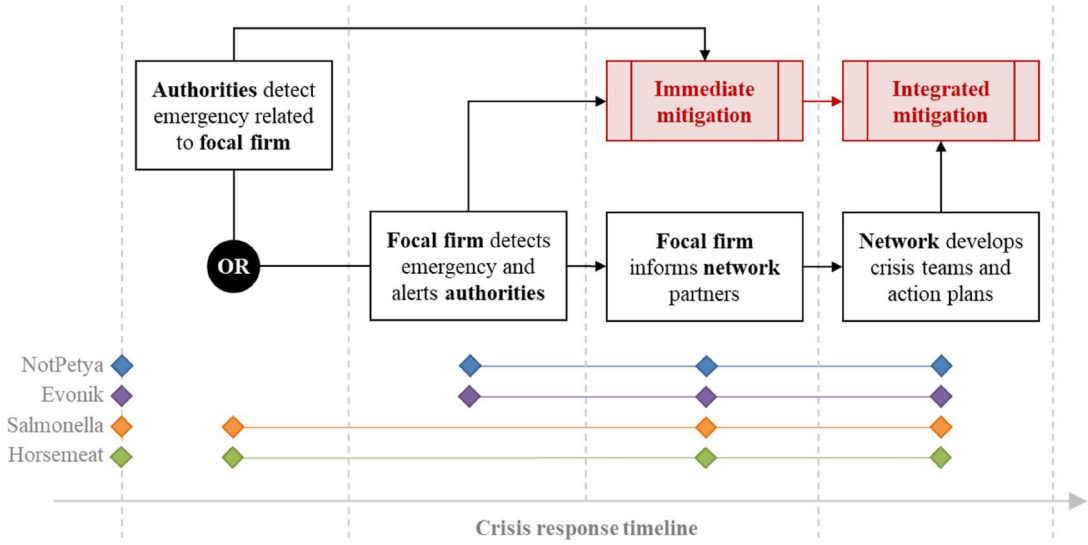

Figure 4. Overview of crisis response timeline for cases.

mandatory breach-notification period with financial penalties that could amount to 4% of the firm's annual global revenue or €20 million. Following (or in consonance with) notification of relevant authorities, the focal firm informs network partners as disruptions escalate (*NotPetya-M, Salmonella-C* and *Horsegate*) or breaks occur (*Evonik*) within the supply chain. Analysis of the cases suggests that the modus operandi for mitigation measures seems to involve customer-first mindsets, and close discussions with customer, as suggested by these excerpts from the *NotPetya-M, Salmonella-C* and *Evonik-E* cases

> 'If I were to boil it down to the very basics, what our colleagues did is quite simple but powerful: **Put customers first**, then A.P. Moller - Maersk, then team and then self' (Navneet Kapoort, Head of the Global Service Centres, Maersk).

> 'Our **customers are our highest priority'** (Simon Baldry, Managing Director of Cadbury).

> 'We are in **close discussions with our customers** (on) how to solve this situation' (Spokesperson for Evonik).

Further analysis of the cases indicates that in response to the crises, supply chain managers adopt a repertoire of mitigation measures, as summarized by the themes of Table 3, which strive to restore normalcy amid the crisis, to recover from the effects of the crisis or to regulate efforts within the network. The next subsections elaborate on these themes.

4.2.1. Intelligence review for reassessments

Intelligence review is a cluster of mitigation measures for scrutinising and auditing the existing knowledge on the crisis (and domain in relation to the crisis), comprehensively and continuously, under **sector dependencies** and **network liabilities**. Due to the technological nature of the *NotPetya* attack on IT systems, intelligence-based mitigation measures for the case mainly entail control policies for tightening and securing systems in two main areas. Building more secure and reliable infrastructure is the first measure, and according to Adam Banks, CIO at Maersk:

> 'That means we (Maersk) need to continue what we've started and finish building a more **secure and reliable infrastructure** that can support the growth strategy of this company. We will have more to share about what this will look like and what it will mean for employees and the company when we announce the new IT strategy'.

Similarly, Lars Jensen, CEO, and partner, at SeaIntelligence Consulting, commenting on updates to systems as mitigation measures associated with the *NotPetya-M* case, argued that:

> 'Often it is a matter of ensuring that **systems get updated** in a timely fashion, business processes are changed slightly, networks are properly configured, security features are tested, and users properly trained'.

Conducting ongoing risk assessments is the second measure, with internal and external demands on the focal firm. Internally, these assessments contribute to the contingency plans that deliver immediate responses in the event of emergencies, while externally, assessments offer knowledge on the preparedness of network partners. Thus,

> 'When something bad happens, you're not in information gathering mode, not in scramble mode … "How much do you know about that partner that you're doing business with? How much do you trust their security practices?" are questions to ask **when assessing risk'** (Joe McMann, strategy lead for Capgemini Cyber North America).

> '**Dealing with a company** that thinks the password "X" is perfectly secure, that in itself does not prove that their back-end systems aren't secure—but it's a sign. That would leave me worried' (Lars Jensen, maritime security advisor at Improsec).

Such knowledge aids in delivering both immediate and integrated responses to disruptions from emergencies.

For the *Horsegate-S* case, regular testing and ongoing risk assessments are at the heart of the audit programme and due diligence system that responds to previous shortcomings of the European food supply chain, as suggested by Steve Mclean, Head of Agriculture, Marks and Spencer

Table 3. Crisis mitigation themes within cases.

Themes	Main focuses	Management repertoires for crisis mitigation	Supply chain management objectives of mitigation	Operational vulnerabilities as contingency factors	Related cases
Intelligence review for reassessments	• Building more secure and reliable infrastructure • Ongoing risk assessments and testing	• Continuous monitoring • Comprehensive audits	• Restore normalcy • Recovery operations • Regulate network	• Sector dependencies • Network liabilities	*Evonik-E, Salmonella-C, Horsegate-S* and *NotPetya*
Integrated relationships for response	• Cross-functional and swift organizational collaboration • Inter-organizational assistance • Institutional support	• Controlling and securing inventory • Close contact and canvasing supply chains • Crisis teams and meetings • Capacity rebuilding	• Restore normalcy • Recovery operations	• Market pressures • Sector dependencies • Network liabilities	*Evonik-E, Horsegate-S* and *NotPetya*
Innovation resilience for recovery	• Individual and team creativity • Technology development	• Communication and solution alternatives	• Recovery operations • Regulate network	• Market pressures • Sector dependencies • Network liabilities	*Evonik-E, Salmonella-C* and *NotPetya*
Integrity rebuilding for reassurance	• Management of communications • Restoring customer confidence	• Clarity and transparency in communications • Cooperation and co-opting independent commissions	• Restore normalcy • Regulate network	• Market pressures • Network liabilities	*Salmonella-C, Horsegate-S* and *NotPetya*

> 'We need to make sure that we have got an **audit and due diligence system** that ensures we do not get caught out and never let our customers down … So, I know it is a burden for the supply base and we are looking at how we can carry out the **audit programme and deliver** what we require in the most cost-effective way. But we are never going to lump in our requirements with everybody else'.

Professor Chris Elliott additionally observes that:

> 'The industry is doing a **huge amount of testing** at the moment. They don't need to be told to do testing'.

In the *Salmonella* case, the focus is on learning lessons from a review of the outbreak and response. Top officials associated with the focal firm demanded that

> 'Employees **learn lessons from the affair**, speaking of a "deep concern to ensure that we do not let consumers and ourselves down"' (John Sunderland, chairman of Cadbury Schweppes).

> 'We **learned a lot** about ourselves in 2006 and we're profiting from that learning' (Todd Stitzer, CEO of Cadbury Schweppes).

The analysis also identifies continuous monitoring as an additional intelligence-based measure for the post-crisis recovery, as reflected by the following excerpts from spokespersons of auto supplier linked to the *Evonik-E* case, related to

> 'Our plants are operating normally, and we **continue to monitor the situation**' (Mike Goss, spokesperson for Toyota).

> '(The company is) **monitoring the situation** … At this time, we do not anticipate any production impacts' (Katie Hepler, spokesperson for Chrysler).

Similar monitoring is suggested by Todd Stitzer, CEO of Cadbury Schweppes, in connection with the *Salmonella-C* case, as follows,

> 'We … are **still monitoring** the trading impact of the UK product recall'.

4.2.2. Integrated relationships for response

Integrated response is a cluster of mitigation measures based on organizational collaboration within the focal firm, inter-organizational assistance from partners and firms within the same sector, and institutional support from government authorities and industry associations. These measures are the purview of response plans and crisis teams that offer immediate response to a crisis, under **market pressures**, **sector dependencies** and **network liabilities**. For the *NotPetya-M* case, two main orientations helped Maersk's crisis team deal with the outage due to the cyberattack: (i) the solidarity from a cross-functional response by Maersk employees that was driven by a customer-first mindset, and (ii) the support from Maersk IT partners and global cyber security agencies for system recovery. The following excerpts capture these orientations:

> 'I saw how **all colleagues across all functions were pulling together**, working hard and doing their very best for the company to recover and get us out of the situation as quickly as possible. It was a great experience to see the immense efforts and amazing teamwork' (Søren Toft, COO at Maersk Line).

> 'This was the worst crisis I think any of us have experienced. **And we were never alone, so many hands helped in this recovery**. From the very first days, we got phone calls from all over the organisation from people who wanted to fly in and help, but also from technology partners and other companies' (Adam Banks, CIO at Maersk).

Data from the *Evonik-E* case indicate two core orientations assisted in the response to the industrial accident. First, is the immediate response from the North Rhine Westphalia authorities through a loudspeaker campaign, radio messages and handing out flyers to inform and warn the immediate neighbourhood of the accident. The authorities and an independent

expert commissioned by Evonik also independently investigated the cause of the explosion. Second, is the coordinated sectoral support from the working group (i.e. the Automotive Industry Action Group [AIAG]), industry meetings and workshops involving over 200 executives held at secret locations to offer an industry-wide strategy. For instance, an AIAG meeting held in Michigan assembled Original Equipment Manufacturers (OEMs) (e.g. Honda, Chrysler, Ford and Volkswagen) and suppliers (e.g. BASF, Delphi, DuPont Automotive and Martinrea International) to assess the impact of the shortage and to seek alternatives to Nylon-12. In all, the group created six technical committees and the response highlighted the need for strengthened supply chain relationships, i.e.

> 'It is serious but the action of an **awful lot of people** working together is starting to look like we are getting results. We are working very, very hard with the vehicle manufacturers and suppliers to get a handle on the situation' (Neil De Koker, president and CEO of Original Equipment Suppliers Association (OESA)).

> 'So, there's plenty of work to be done. Some of it needs to occur at the very **start of a relationship between manufacturer and supplier**. It's smart to spell out the basic steps that each might take with regard to allocating product in case of a sudden shortage' (Robert Bowman, Editor-in-Chief of SupplyChainBrain).

Following the recall associated with the *Horsegate-S* case, there are calls for greater collaboration and close working relationships with partners within the food supply chain, i.e.:

> 'The horsemeat scandal took supermarkets by surprise because they took a complex supply chain too much "on trust" and were over-reliant on paperwork, rather than sampling and **close trade relationships'** (Rod Addy, News Editor of Food Manufacture).

> 'The buzzword now is "collaboration" … **Closer working** like this can lead to closer bonds, product innovation, investment opportunities, improved risk for the buyers as well as lower costs. Some collaboration evangelists among SCM aficionados could well be feeling that the horsemeat debacle means that their time has come' (Gavin Hinks, Editor-in-Chief of Financial Director)

Premised on close working and supply chain collaboration, the food fraud of the *Horsegate-S* case also challenged managers to simplify the food supply chain. For instance, citing examples of best practice by McDonald's and Morrisons, Professor Chris Elliott argued that

> 'Manufacturers should look at **simplifying their supply chains**, as greater complexity multiplied the number of weak points in the system'.

Similarly, Dalton Philips, CEO of Morrisons, argued that

> 'There **need only be four parts** (for the meat supply chain) - farmer, abattoir, meat manufacturing plant and retailer'.

Analysis indicates that controlling and securing inventory, canvassing supply chains and capacity rebuilding, e.g. repairing facilitating and ramped production following recalls, are the key practical and immediate integrated response measures pursuant to a disaster, emergency, standoff or scandal. For instance, due to the uncertainty of PA-12 shortages in the *Evonik-E* case,

> 'Carmakers are faced with the problem of **securing inventory to maintain production'** (Automotive Logistics).

> 'OEMs are **canvassing their supply chains to identify risks, available inventories**, etc.' (Paul Blanchard, North American director of engineering resins for the consulting group IHS Chemical (now part of S&P Global Inc.)).

> 'An extensive work to **repair the damage** caused by the fire allowed Evonik to start operating again after less than ten months and gradually return to full production' (About Resilience).

For the *NotPetya* cyberattack, capacity rebuilding as the immediate response, involved using a full, unencrypted copy of Active Directory from a local office in Lagos Nigeria that was offline at the time of the attack and canvassing supply chains for Azure cloud engineers to rebuild the system, as observed by Adam Banks, the CIO of Maersk:

> 'The 23- year-old local IT support guy (from the Maersk office in Lagos, Nigeria) got a free trip on a Gulfstream G450, physically carrying the hard drive that we used as the yeast that **built the rest of the network'.**

> 'If you (i.e., Maersk partner) haven't been hit by this and you have some Azure cloud engineers, can we **borrow them** for a week?'.

Primarily, restoring normalcy is the target of this rebuilding exercise, as opposed to more strategic and profound system changes. According to Lewis Woodstock, Maersk's Head of Cybersecurity compliance:

> 'We went about **rebuilding our infrastructure** over a period of about 10 days, during which time we were doing all we could to maintain normal business operations'.

4.2.3. Innovation resilience for recovery

Innovation resilience for recovery is a cluster of mitigation measures based on individual and team creativity and technology development to create alternative solutions for scarce supplies and to develop alternative means of communication. Under **market pressures**, **sector dependencies** and **network liabilities,** innovation within the supply chain delivers ideas to restore normalcy and recover operations.

For the *NotPetya* case, innovation in response to severe disruptions of the cyberattack stems from individual and team creativity that sought alternative means for communication and solutions to restore normalcy, as suggested by the following quotes from Manjini Balanarayanan, an Operations Team Manager at Maersk's Global Service Centre:

> 'Initially, we didn't even have good Wi-Fi to get connected with additional resources, so **we had to be creative** while management in Maersk Line Asia Pacific and MCC provided good **support with innovative ideas**. We tried using lots of alternative ways to communicate with one another, using WhatsApp and Google Drive in sending the data information'.

> 'However, everyone was in the same situation, and with the terminal, MCC and Maersk Line working together, we found alternative ways to solve the problem. Over the two weeks we reduced the number of containers with unknown destination from 7,500 to 400. By **working innovatively** and as one team we came back strong and really worked well'.

The excerpts reflect an extension of the integrated approach to addressing the problems of the cyberattack but with emphasis on human resilience, as suggested by the following:

'We overcame the problem with **human resilience'** (Jim Hagemann Snabe, Chairman, Maersk).

'That recovery operation really relied heavily on **human resilience'** (Lewis Woodstock, Head of Cybersecurity compliance, Maersk).

For the *Evonik-E* case, the quest and search for alternative solutions was challenge for technology development. Here, the main mitigation involved deriving and testing substitutes for PA-12 for immediate and long-term use to improve supply security, i.e.

'At the moment we still do not have any indication as to the full extent of the damage. While we do expect there to be substantial constraints with respect to our ability to provide supplies of CDT-based products, we are nonetheless confident that we will be able to **provide alternative solutions** in the form of substitutes such as VESTAMID® Terra. It is possible to modify these biobased polymers as required for many of the relevant applications to achieve much the same material attributes as PA12. We are already making every effort to ensure the facility is repaired and running and that we will be able to re-establish full supply capability as soon as possible' (Evonik press release).

'Ever since the German plant was damaged in the blast, automakers and suppliers have been rushing **to find substitutes for PA-12**. The plant, owned by Evonik Industries, made at least a quarter of the world's PA-12, and up to 70 percent of CDT, a key ingredient used by other companies to make the resin' (Tom Krisher, Auto Industry Journalist, Associated Press).

Technology development also characterizes the innovation for the *Salmonella-C* case, along with apologies that offer accountability for the crisis. With £15 million spent on recall cost, Cadbury additionally spent £20 million making changes to address the quality problems due to the crisis. According to Cadbury's financial report and press release around the time of the food scare, the company explained that:

'We have apologised to our consumers, customers and colleagues for any concerns caused and are **implementing changes** to our UK manufacturing and quality assurance processes so that this cannot happen again' (Todd Stitzer, CEO of Cadbury).

'We have spent over £20 m in **changing our procedures** to prevent this ever happening again' (spokesperson for Cadbury).

These changes or innovations seek to improve the quality of processes for monitoring and testing. For instance, Cadbury adopted the Pathatrix pathogen testing system to improve its microbiological surveillance, in an effort to improve response to market pressures on its supply chain while maintaining compatibility with Cadbury's existing technology systems, as observed by Jeff Banks, Group Director of Food Safety and Quality for Cadbury:

'The (Pathatrix) system integrates well with other technologies and provides a high quality and practical asset for our laboratories … with a validated, **science-based solution** to the rigorous demands of a highly interdependent and time-critical supply chain'.

4.2.4. Integrity rebuilding for reassurance

Integrity rebuilding for reassurance is a cluster of mitigation measures that seek to reassure and restore customer confidence in brands and offerings by the sector. Under **market pressures** and **network liabilities**, this reassurance is pivotal at the time of the crisis (i.e. intra-crisis) and post-crisis. Additional requirements for integrity building stem from prompted 'confidence crisis' (i.e. widespread loss of consumer confidence) due to failings associated with the *Salmonella-C* and *Horsegate-S* cases.

For the *NotPetya-M* case, there was a deliberate focus of Maersk on transparency at the outset, with management of communications within the organization via reporting groups and with 12-h video updates to clients and customers, as commented on by Adam Banks, CIO at Maersk, as follows:

'We decided to be **transparent from the get-go**. In hindsight, we didn't have a choice. That was transparency with both customers and internal stakeholders. It was a wise choice by the CEO'.

'Management formed a group and then created cascading **reporting groups across the organization**, enabling teams to communicate'

This transparency-based approach to communications and maintaining firm integrity, according to Adam Banks, avoided employee distractions and potential confusions due to excessive updates, leading to praise for the response and renewed focus, as observed below:

'**Transparency** was also a key part of Maersk's response, and something it has been praised for in the aftermath. That also helped generate enough goodwill to get others to aid with its recovery efforts' (Dan Swinhoe Editor, CSO).

'The silver lining, if any, to the crisis, is that we have a **renewed sense of purpose** and a pointer to a different way of working' (Navneet Kapoort, Head of the Global Service Centres, Maersk).

Restoring customer confidence is also a feature of the *Salmonella-C* case, with Cadbury spending a further £5 million on advertising seeking to

'**Rebuild confidence** and momentum, and to reunite customers with the Cadbury brand' (Todd Stitzer, CEO of Cadbury).

Broadly, the impacts of *Salmonella-C* food scare triggered a massive recall, which Cadbury undertook to reassure customers, as suggested by the following quote:

'We decided to conduct a **precautionary recall to** reassure our consumers and the public at large to minimise any confusion as to the quality of our products' (Matthew Shattock, European president of Cadbury)

Similarly, in the *Horsegate-S* case, there were integrity rebuilding measures by the Food Safety Authority (FSA), such as an independent inquiry into the food fraud which recommended the creation of a new food crime unit and funding for the public laboratory service. According to Elizabeth Truss, the Environment Secretary during the food scandal:

'We're taking action to make sure that families can have absolute **confidence in the food** that they buy … When a shopper picks something up from a supermarket shelf, it should be exactly what it says on the label, and we'll crack down on food fraudsters trying to con British consumers'.

5. Discussion

Although some firms harness demand outlooks in times of crisis (e.g. private-jet travel during the SARS outbreak (Overby et al.

2004)), crisis has a negative connotation due damages, destruction or disruptions caused by crisis events, triggering insecurity and unpredictability. Crises expose system weaknesses (Notteboom, Pallis, and Rodrigue 2021) and pose challenges for SCM to understand *vulnerabilities* that explain or exacerbate what went wrong (Harland 2021) and to reflect on the *mitigation* that acts as interventions for the survivability and continuity of supply chain partners (Sheng and Saide 2021). Insights on these vulnerabilities and mitigation measures remain central to developing agility and resilience of supply chains. SCM contingencies aid in explaining the efficacy of firms within supply chains (Prajogo, Mena, and Nair 2018) and managers face difficulties identifying relevant variables for formulating well-suited SCM strategies (von Falkenhausen, Fleischmann, and Bode 2019).

Premised on contingency theory's assertion that efficacy in managerial actions stem for relevant organizational contexts (Chandler 1962; Lawrence and Lorsch 1967; Thompson 1967; Donaldson 2001), this study analyses the SCM context for crisis mitigation with respect to the contingency factor of pre-existing operational vulnerabilities. Using Maersk's *NotPetya* cyberattack, *Evonik's* industrial accident, Cadbury's *Salmonella* Scare and *Horsemeat* Scandal, the study concentrates and developes insights from supply chains in times of crisis. Figure 5 summarizes the findings detailed in the previous section in a revised model of SCM in times of crisis, showing amendments regarding:

- the industrial response, which contributes to management performance, and
- the industrial constraints and management repertoires which contribute to operational vulnerabilities and crisis mitigation, respectively.

The next subsections discuss the theoretical, managerial, and industrial implications of the study findings.

5.1. Theoretical implications

The theoretical implications of this research's findings are threefold. First, the findings from analysing the *Evonik-E, Salmonella-C, Horsegate-S* and *NotPetya-M* cases suggest that market pressures, sector dependencies and network liabilities (i.e. the MSN) are the three main themes of operational vulnerabilities that explain supply chain crises, as summarized by Table 2. Although these crises occurred inside the supply chain, in accordance with perspectives on vulnerabilities (Christopher and Peck 2004), the MSN are related to risks internal (network liabilities) and external (market pressures

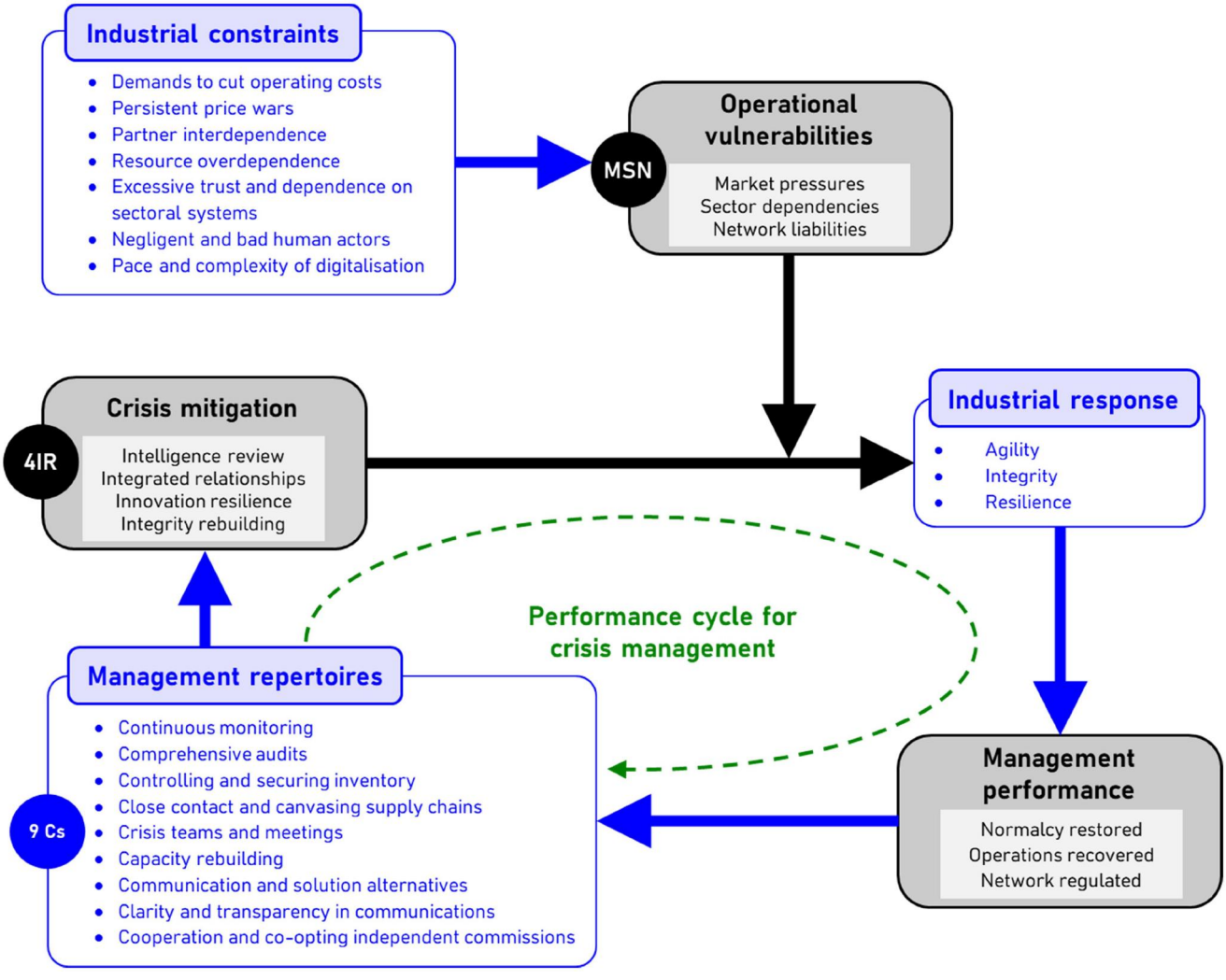

Figure 5. Summary of case study findings and revised model of supply chain crisis management.

and sector dependencies) to the supply chain. The MSN also relate to globalization that creates market pressures for tighter supply chains running on JIT schedules (as indicated by the *Evonik-E, Salmonella-C* and *Horsegate*) and to digitalization that establishes digital demands and liabilities in view of pressures to keep step with evolving digital business and security needs (as suggested by the *NotPetya*). This insight adds to SCM conversations on digitalization and globalization as motives for tele-connected vulnerability of supply chain partners (Bassett et al. 2021) and for lengthened and stretched supply chains that increase exposure to a crisis (Blome and Schoenherr 2011; Hittle and Leonard 2011). As shown by Table 3, due to MSN vulnerabilities, SCM confronts challenges of maintaining tight and resilient supply chains, ensuring integrity and integration of supply chain partners, effective planning and contingencies in anticipation of potential severe shortages, and coping with changing digital business and security landscape. Along these lines, this research contributes to a *contingency theory* of SCM in times of crisis. Related studies (e.g. Wagner and Bode (2006), Harland et al. (2021), Harpring et al. (2021) and Karaosman, Marshall, and Villena (2023)) identify operational vulnerabilities in the form of increased customer and supplier dependence, supplier concentration and self-interests, as well as single and global sourcing. However, this research specifically draws insights from cases of supply chain crises surrounding widespread product contamination and severe production interruption. While a crisis chronologically begins when a disaster, emergency, standoff or scandal breaks out (Pashapour *et al*. 2019; Durugbo and Al-Balushi 2023), insights from the *Evonik-E, Salmonella-C, Horsegate-S* and *NotPetya-M* cases indicate that SCM in times of crisis begins with alerting the relevant authorities, as shown by Figure 4, and this active involvement of authorities offers an additional and clear distinction between a crisis and routine disruptions in supply chains. For instance, in Europe, the GDFR requires firms to notify relevant authorities (and those affected) of breaches, but this notification triggers the active involvement and investigations by these authorities. Here, the spotlights of investigation for crises could be on the focal firm (*Salmonella-C*), the supply chain (*Evonik-E*) or the wider industry sector and ecosystem (*Horsegate-S*). There are similar breach notification rules in other regions (such as the Personal Information Protection Law of Mainland China) and sectors (such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR §§ 164.400–414) of healthcare in the USA).

Second, the research finds four themes on crisis mitigation (i.e. the 4IR measures) that serve as immediate, independent and integrated responses during supply chain crises: (i) intelligence review for reassessments, (ii) integrated relationships for response, (iii) innovation resilience for recovery and (iv) integrity rebuilding for reassurance. As summarized by Table 3, these mitigation measures stem from analysing the *Evonik-E, Salmonella-C, Horsegate-S* and *NotPetya-M* cases and these interventions strive to restore normalcy, recovery operations and regulate networks as partners grapple with exigencies for SCM decisiveness. Although literature notes that there is no one-size-fits-all supply chain strategy (von Falkenhausen, Fleischmann, and Bode 2019; Siebert, Brandenburg, and Siebert 2020), researchers stress the need for studies that ascertain variables for developing context-dependent SCM strategies (von Falkenhausen, Fleischmann, and Bode 2019). Accordingly, this research adds to the discourse on chain mitigation variables for SCM in times of crisis but with spotlight on the intense difficulty, extreme trouble, or danger for and within a supply chain. Table 3 additionally indicates that underpinning crisis mitigation in the analysed cases is a set of '9Cs' crisis response repertories involving continuous monitoring, comprehensive audits, controlling and securing inventory, close contact and canvassing supply chains, crisis teams and meetings, capacity rebuilding, communication and solution alternatives, clarity and transparency in communications, and cooperation and co-opting independent commissions. Related SCM studies posit on mitigation measures for supply chain disruptions such as insurance, inventory, sourcing, rerouting, demand management, contingency stocks, buffering or bridging and borrowing or lending materials from organizations within the same sector (Al-Balushi and Durugbo 2020, 2023; Kovács and Sigala 2021; Spieske et al. 2022).

Third, the findings from the case study indicate that underpinning immediate SCM responses to crises are customer-first mindsets and close discussions with customers, as suggested by the excerpts from the *NotPetya-M, Salmonella-C* and *Evonik-E* cases. This priority is a recurring focus of the different 4IR mitigation measures as highlighted by the need for intelligence review that 'never lets customer (or consumers) down' (*Horsegate-S* and *Salmonella-C* cases) and transparency in customer discussions for integrity rebuilding (*NotPetya-M* and *Salmonella-C* cases). Related studies argue for a centralization thesis of SCM in times of crisis for delivering leadership and solidarity in strategies, such as the establishment of 'war rooms' as operational command (Durugbo et al. 2022). However, a customer-first mindset adds a layer to SCM philosophy that complements centralization for solidarity from a cross-functional response, as suggested by the *NotPetya-M* case. Additionally, the customer-first mindset offers a unifying theme for decisiveness required in times of clarity (Desoutter and Lavissière 2018). In advancement of *crisis management framing of SCM*, customer-first mindsets challenge existing proactive *vs*. reactive SCM strategies in times of crisis (Elluru et al. 2019; Dewick, Hofstetter, and Schroeder 2021) and call for a fundamental rethinking of such dichotomy for framing strategies. Here, the close contact and discussions with customers imply a 'coactive' SCM strategy that co-opts and involves customers and key stakeholders in strategy analysis, formulation, and implementation for improved performance in times of crisis. Thus, the findings offer more clarity on the tenuous links between supply chain crisis, mitigation strategies and operational vulnerabilities (Bassett et al. 2021; Fearne et al. 2021), by expanding the options for SCM to a trichotomy of proactive-reactive-coactive SCM strategies.

5.2. Managerial implications

From a managerial perspective, the findings of the case study, as summarized by Figure 5, offer a framing with strategy implications for supply chains agility, integrity and resilience.

Agility and resilience are characteristics demanded of responses to the various crises and disruptions that threaten supply chain survivability (Sheng and Saide 2021). Similarly, integrity ensures adherence to principles of ethical conduct, efficacy and completeness of industrial systems (Durugbo and Al-Balushi 2023). In this study, and in line with contingency theory (Chandler 1962; Donaldson 2001), the analysis suggests that the ability of partners to restore normalcy, recovery operations and regulate networks explains the performance of SCM in times of crisis. This triad of objectives is crucial to focusing SCM efforts for minimizing the escalation and propagation of incidents across the value chain as well as decreasing the probability and impact of adverse and prolonged effects. The case study findings suggest that these different objectives relate to different capabilities, such as secure and reliable infrastructure, risk assessments and testing, institutional support and team creativity.

Driven by imperatives to learn lessons from past cases of crisis, this study also encourages SCM practitioners to stress perceptiveness and innovativeness for the decisiveness that confronts and contains supply chain crises. Perceptiveness views of interventions pre- and post-crisis, challenge managers to harness and prioritize supply chain relationships and intelligence capabilities during prevention and preparation steps, as underscored by the *Evonik-E, Salmonella-C, Horsegate-S* and *NotPetya-M* cases. In this context, it is worth noting that preparations based on technology, trust, transaction and transport (Banterle and Stranieri 2008; Gao et al. 2012; Meyer-Larsen et al. 2012; Boyson 2014) need careful consideration because these aspects could become sources of problems during crisis, spread, multiply and amplify the crisis or create different crises *in situ*. Therefore, during SCM strategy formulation, this study recommends that practitioners extend their risk assessment proclivity to include management systems for these technology, trust, transaction and transport considerations during crises.

Similarly, the study implies innovativeness for coping measures that lead to preventive, pragmatic, promotion and progressive moves intra-crisis, as suggested in Gulati, Nohria, and Wohlgezogen (2010). Here, the charge is for supply chain managers to cultivate cultures for human resilience and creativity that played a key role in recovering operations of supply chains associated with the *Evonik-E* and *NotPetya-M* cases. SCM could also benefit from silos with crisis-oriented redundant resources within the ecosystem for mitigating potential ripple effects of crises to other supply chains, sectors, or regions. These silos aid in isolating functioning systems from the affected ones during crisis (curbing and dampening ripple effects) and thus enabling quicker detection of the source as well as prompt response.

5.3. Industrial implications

Finally, the research findings have industrial implications for manufacturers and suppliers. For manufacturers, the findings suggest a need for industry system benchmarks regarding crisis management. Benchmarks for crisis management contain mitigation points of reference and emerge from identifying and integrating best practices and optimal/critical solutions for industrial systems during crisis. In this regard, the findings from the cases offer lessons on industrial best practice (Li et al. 2017; Min 2023a) regarding foci on the MSN vulnerabilities, the 4 IRs of crisis mitigation and the '9Cs' crisis management repertories. Crisis management insurance stemming from network liabilities, industry intelligence plans for coping with market pressures, and supply chain crisis management standards and legislation (e.g. the Supply Chain Resilience Initiative, the Action Plan on Critical Raw Materials and the CHIPS and Science Act) for curbing resource and partner dependence issues are some specific benchmarking points of reference implied by the study.

Regarding suppliers, the findings imply a culture of crisis management, in line with recent studies (Zhao et al. 2024), but based on enhanced management performance through continuous learning, as shown by Figure 5. The need for performance cycles, premised on continuous 'learning cycles' and 'marketing loops' for profitable industrial relationships between firms and clients, is well established in previous industrial studies (Durugbo 2020). The lessons learnt by manufacturers and suppliers from these loops contribute to virtuous cycles and best practices for industrial systems along modern service–recovery and production–distribution chains. For the performance cycle of crisis management, as shown by Figure 5, lessons learnt by suppliers from management performance inform transformations and tweaks to management repertoires. For instance, with lessons primarily from the *Horsemeat* and *Salmonella-C* cases, suppliers could establish channels and norms for interacting with authorities and maintain due diligence for industrial systems. These norms derive support from intelligence reviews (of the 4IRs) that foster visualization and sharing of data. Intelligence capabilities also support reliability through allowing proactive management of fluctuations as these variations occur – permitting regular individual audits, enabling mutual accountability, and stimulating intelligent opportunities across the ecosystems of supply chains.

6. Conclusions

Characterized by times of intense difficulty, extreme trouble or danger and imperatives to involve regional authorities, crises within supply chains, i.e. supply chain crises, cause major disruptions or interruptions that impact the normal flow of goods and provision of services. Thus, SCM, contends with scope, spill-over and shift effects that usually extend beyond interrupting optimal flow of resources and demand fulfilment to threating long-standing relational and reputational values. The effects could also cause an unequal distribution of liabilities among exchange partners, resulting in loss of confidence in the exchange environment. Additionally, due to increasing digitalization and globalization of supply chains, crises are becoming cybernetic and transboundary, corrupting and disconnecting systems and paralysing supply chain operations.

Motivated by contingency theory, this research explores operational vulnerabilities as contingency factors for supply chains crises and identifies crisis mitigation practices of supply

chains, using four European cases of supply chain crises: (i) the NotPetya Cyberattack on A.P. Møller-Maersk (*NotPetya-M*), (ii) the *Evonik* plant explosion (*Evonik-E*), (iii) Cadbury's Salmonella Scare (*Salmonella-C*) and (iv) the Horsemeat Scandal (*Horsegate-S*). The study contributes to the SCM body of knowledge by advancing theoretical understanding of crisis mitigation in supply chains and providing practical lessons on SCM strategies in time of crisis.

This study confronts two research questions. First, this study considers "What operational vulnerabilities account for and impact supply chain crises?" **(RQ1)**. Insights from analysing the case studies suggest that three main themes of operational vulnerabilities (i.e. 'the MSN of threats') explain supply chain crises: (i) market pressures, (ii) sector dependencies, and (iii) network liabilities. At the heart of these vulnerabilities are SCM challenges for tighter and resilient supply chains, integrity and integration supply chain partner, effective planning and contingencies in anticipation of potential severe shortages, and measures to cope with the persistently changing digital business and security landscape. Second, this study ponders 'How do supply chain managers mitigate the effects of supply chain crises, under the operational vulnerabilities that act as contingency factors?' **(RQ2)**. Similarly, the analysis of the case studies indicates that four main themes of crisis mitigation measures (i.e. the 4IR) account for the immediate, independent and integrated SCM responses during supply chain crises: (i) intelligence review for reassessments, (ii) integrated relationships for response, (iii) innovation resilience for recovery and (iv) integrity rebuilding for reassurance. Driving the 4IR is a set of '9Cs' crisis response repertories consisting of continuous monitoring, comprehensive audits, controlling and securing inventory, close contact and canvassing supply chains, crisis teams and meetings, capacity rebuilding, communication and solution alternatives, clarity and transparency in communications and cooperation and co-opting independent commissions. Hinged on customer-first mindsets and close discussions with customers, these measures and repertoires contribute to SCM performance in times of crisis through restoring normalcy, recovering operations and regulating networks. *Theoretically*, this research implies a contingency theory of SCM for crisis, a set of chain mitigation variables for supply chain crisis, and a 'coactive' SCM strategy for improved performance in times of crisis. *Managerially*, the research has implications for the agility and resilience of supply chains, best practice for SCM in times of crisis, and argues for perceptiveness and innovativeness in the decisiveness of supply chain managers in response to a supply chain crisis. *Industrially*, the research has implications for benchmarking of industrial systems to support crisis management by manufacturers and for cultivating cultures of crisis management by suppliers premised on continuous learning.

This study has four main limitations. First, the scope of the study is limited to crises affecting the European region. Second, the case research has limitations concerning generalizability of the findings to a larger population. Yet, this study seeks analytic generalization wherein the extracted ideas from case studies' findings could apply to different situations other than the cases in the original study. The other limitations of the study are the exploratory nature of the study and the sole focus of the case study analysis on secondary data. These limitations could serve as the foundation for future research to expand analytical, topical and methodological focus by including other crises, industries, and region/country contexts.

To conclude, our analysis from this study enables us to capture and put forward a better perspective on operational vulnerabilities of supply chains and how crisis mitigation aids organizations in enhancing SCM for crises. The expectation is that management concepts from this study could serve as the foundation and support for further studies that produce more conceptual and empirical insights on trends, topics, and theories for a 'supply chain crisis' paradigm. Our message to manufacturer and suppliers is that due to the critical nature and costs of operational vulnerabilities associated with a crisis, companies within supply chains require crisis mitigation benchmarks and cultures informed by lessons learned from past crises.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Dr. Christopher M. Durugbo is Director for the Faculty of Business and Management at Muscat University in the Sultanate of Oman. He is a supply chain and services innovation expert with an interest in system thinking for innovative services and policies, network analysis for supply chain innovation, and managing collaboration for innovation through analytics, informatics and ergonomics. Dr Durugbo has published findings from his research in several journals such as *International Journal of Operations and Production Management, European Journal of Operational Research, Supply Chain Management: An International Journal, International Journal of Production Research, Production Planning and Control, Annals of Operations Research, Technological Forecasting and Social Change, Expert Systems with Applications, Ergonomics,* and *Information Sciences.*

Dr Zainab Al-Balushi is Assistant Professor of Operations Management at the College of Economics and Political Science, Sultan Qaboos University in the Sultanate of Oman. She is a founding member of Oman Logistics Association and a member in formulating the Sultanate of Oman Logistics Strategy 2040. She is a reviewer for various journals and has published in international journals such as *Supply Chain Management: An International Journal and International Journal of Physical Distribution & Logistics Management,* and *Computers & Industrial Engineering*. Her research interests include Inter-Firm Relationships, Supply Chain Uncertainty and Risk Management, CSR & Sustainability, Logistics Digitalization, and Logistics Education.

References

Al-Balushi, Z., and C. M. Durugbo. 2020. "Management Strategies for Supply Risk Dependencies: Empirical Evidence from the Gulf Region." *International Journal of Physical Distribution & Logistics Management* 50 (4): 457–481. https://doi.org/10.1108/IJPDLM-06-2019-0201.

Al-Balushi, Z., and C. M. Durugbo. 2023. "A Unified Model of Supply Risk Mitigation." *Computers & Industrial Engineering* 177: 109019. https://doi.org/10.1016/j.cie.2023.109019.

Allal-Chérif, O., and S. Maira. 2011. "Collaboration as an anti-Crisis Solution: The Role of the Procurement Function." *International Journal of Physical Distribution & Logistics Management* 41 (9): 860–877. https://doi.org/10.1108/09600031111175825.

AlMalki, H. A., and C. M. Durugbo. 2023. "Institutionalising Industry 4.0: A Delphi Study of Institutional Change Readiness for the Fourth Industrial Revolution in an Emerging Economy." *Production Planning & Control* 0 (0): 1–19. https://doi.org/10.1080/09537287.2023.2217414.

Andaloussi, M. B. 2023. "Logistics Outsourcing to Provide Supply Chain Agility in Crisis Time: An Action Research." *Journal of Global Operations and Strategic Sourcing* 17 (1): 88–103. https://doi.org/10.1108/JGOSS-06-2023-0050.

Arcidiacono, D. 2018. "Promises and Failures of the Cooperative Food Retail System in Italy." *Social Sciences* 7 (11): 232. https://doi.org/10.3390/socsci7110232.

Asbjornslett, B. E. 1999. "Assess the Vulnerability of Your Production System." *Production Planning & Control* 10 (3): 219–229. https://doi.org/10.1080/095372899233181.

Azghandi, R., J. Griffin, and M. S. Jalali. 2018. "Minimization of Drug Shortages in Pharmaceutical Supply Chains: A Simulation-Based Analysis of Drug Recall Patterns and Inventory Policies." *Complexity* 2018: 1–14. https://doi.org/10.1155/2018/6348413.

Bai, C. A., J. Sarkis, and W. Xue. 2024. "Improving Operational Efficiency and Effectiveness through Blockchain Technology." *Production Planning & Control* 35 (9): 857–865. https://doi.org/10.1080/09537287.2024.2329182.

Baldini, G., F. Oliveri, M. Braun, H. Seuschek, and E. Hess. 2012. "Securing Disaster Supply Chains with Cryptography Enhanced RFID." *Disaster Prevention and Management: An International Journal* 21 (1): 51–70. https://doi.org/10.1108/09653561211202700.

Banterle, A., and S. Stranieri. 2008. "Information, Labelling, and Vertical Coordination: An Analysis of the Italian Meat Supply Networks." *Agribusiness* 24 (3): 320–331. https://doi.org/10.1002/agr.20169.

Bapuji, H., and P. W. Beamish. 2019. "Impacting Practice through IB Scholarship: Toy Recalls and the Product Safety Crisis." *Journal of International Business Studies* 50 (9): 1636–1643. https://doi.org/10.1057/s41267-019-00247-3.

Barnes, P., and R. Oloruntoba. 2005. "Assurance of Security in Maritime Supply Chains: Conceptual Issues of Vulnerability and Crisis Management." *Journal of International Management* 11 (4): 519–540. https://doi.org/10.1016/j.intman.2005.09.008.

Barton, L. 1991. "A Case Study in Crisis Management: The Perrier Recall." *Industrial Management & Data Systems* 91 (7): 6–8. https://doi.org/10.1108/02635579110007077.

Bassett, H. R., J. Lau, C. Giordano, S. K. Suri, S. Advani, and S. Sharan. 2021. "Preliminary Lessons from COVID-19 Disruptions of Small-Scale Fishery Supply Chains." *World Development* 143: 105473. https://doi.org/10.1016/j.worlddev.2021.105473.

Benson, A. P. 2011. "Communicating Risk to Consumers in Domestic and Internationally Traded Products." *Food Control*. 22 (9): 1529–1534. https://doi.org/10.1016/j.foodcont.2010.07.015.

Blome, C., and T. Schoenherr. 2011. "Supply Chain Risk Management in Financial Crises - A Multiple Case-Study Approach." *International Journal of Production Economics* 134 (1): 43–57. https://doi.org/10.1016/j.ijpe.2011.01.002.

Boin, A., C. Kofman-Bos, and W. Overdijk. 2004. "Crisis Simulations: Exploring Tomorrow's Vulnerabilities and Threats." *Simulation & Gaming* 35 (3): 378–393. https://doi.org/10.1177/1046878104266220.

Boyce, W. S. 2016. "Does Truck Driver Health and Wellness Deserve More Attention?" *Journal of Transport & Health* 3 (1): 124–128. https://doi.org/10.1016/j.jth.2016.02.001.

Boyes, H. 2015. "Cybersecurity and Cyber-Resilient Supply Chains." *Technology Innovation Management Review* 5 (4): 28–34. https://doi.org/10.22215/timreview/888.

Boyson, S. 2014. "Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems." *Technovation* 34 (7): 342–353. https://doi.org/10.1016/j.technovation.2014.02.001.

Braun, V., and V. Clarke. 2006. "Using Thematic Analysis in Psychology." *Qualitative Research in Psychology* 3 (2): 77–101. https://doi.org/10.1191/1478088706qp063oa.

Burns, K. F., and T. G. Marx. 2014. "Crisis Management Planning among Tier 2 Automobile Suppliers: Why Suppliers Fail to Plan." *Journal of Contingencies and Crisis Management* 22 (2): 108–112. https://doi.org/10.1111/1468-5973.12046.

Buttermann, G., R. Germain, and K. N. S. Iyer. 2008. "Contingency Theory 'Fit' as Gestalt: An Application to Supply Chain Management." *Transportation Research Part E: Logistics and Transportation Review* 44 (6): 955–969. https://doi.org/10.1016/j.tre.2007.05.012.

Cao, Z., B. Huo, Y. Li, and X. Zhao. 2015. "The Impact of Organizational Culture on Supply Chain Integration: A Contingency and Configuration Approach." *Supply Chain Management: An International Journal* 20 (1): 24–41. https://doi.org/10.1108/SCM-11-2013-0426.

Chacha, P. W., B. K. Kirui, and V. Wiedemann. 2024. "Supply Chains in Times of Crisis: Evidence from Kenya's Production Network." *World Development* 173: 106363. https://doi.org/10.1016/j.worlddev.2023.106363.

Chammem, N., M. Issaoui, A. I. D De Almeida, and A. M. Delgado 2018. "Food Crises and Food Safety Incidents in European Union, United States, and Maghreb Area: Current Risk Communication Strategies and New Approaches." *Journal of AOAC International* 101 (4): 923–938. https://doi.org/10.5740/jaoacint.17-0446.

Chandler, A. D. J. 1962. *Strategy and Structure: Chapters in the History of the American Industrial Enterprise*. Cambridge, MA: Harvard University Press.

Chang, W., and Y. Lin. 2019. "The Effect of Lead-Time on Supply Chain Resilience Performance." *Asia Pacific Management Review* 24 (4): 298–309. https://doi.org/10.1016/j.apmrv.2018.10.004.

Chiarini, A., A. Grando, and V. Belvedere. 2023. "Disruptive Social Manufacturing Models: Lessons Learned from Ferrari Cars and Isinnova Networks for a Post-Pandemic Value Creation Path." *Production Planning & Control* 34 (12): 1135–1148. https://doi.org/10.1080/09537287.2021.1986865.

Chong, Y. Q., B. Wang, G. L. Yue Tan, and S. A. Cheong. 2014. "Diversified Firms on Dynamical Supply Chain Cope with Financial Crisis Better." *International Journal of Production Economics* 150: 239–245. https://doi.org/10.1016/j.ijpe.2013.12.030.

Christopher, M., and H. Peck. 2004. "Building the Resilient Supply Chain." *The International Journal of Logistics Management* 15 (2): 1–14. https://doi.org/10.1108/09574090410700275.

Craighead, C. W., D. J. Ketchen, and J. L. Darby. 2020. "Pandemics and Supply Chain Management Research: Toward a Theoretical Toolbox." *Decision Sciences: Journal of Innovative Education* 51 (4): 838–866. https://doi.org/10.1111/deci.12468.

Csaszar, F. A., and J. Ostler. 2020. "A Contingency Theory of Representational Complexity in Organizations." *Organization Science* 31 (5): 1198–1219. https://doi.org/10.1287/orsc.2019.1346.

Curtin, T., Hayman, D., and Husein, N. 2005. *Managing a Crisis*. London: Palgrave Macmillan.

Denzin, N. K. 2007. "Analytic induction." In *The Blackwell Encyclopedia of Sociology*, edited by G. Ritzer. Oxford: Wiley.

Desoutter, M., and A. Lavissière. 2018. "Handling Supply Chain Crises When Everything has been Done to Avoid Them." *Supply Chain Forum: An International Journal* 19 (3): 219–232. https://doi.org/10.1080/16258312.2018.1484250.

Dewick, P., J. S. Hofstetter, and P. Schroeder. 2021. "From Panic to Dispassionate Rationality - Organizational Responses in Procurement after the Initial COVID-19 Pandemic Peak." *IEEE Engineering Management Review* 49 (2): 45–56. https://doi.org/10.1109/EMR.2021.3079630.

Dibben, P., J. Meira, C. Linhares, R. Bruce, P. Dibben, J. Meira, C. Linhares, and R. Bruce. 2020. "Vanishing Value Chains, Industrial Districts and HRM in the Brazilian Automotive Industry." *The International Journal of Human Resource Management* 5192: 1–18. https://doi.org/10.1080/09585192.2016.1233446.

Do, Q. N., N. Mishra, N. B. I. Wulandhari, A. Ramudhin, U Sivarajah, and G. Milligan 2021. "Supply Chain Agility Responding to Unprecedented Changes: Empirical Evidence from the UK Food Supply Chain during

COVID-19 Crisis." *Supply Chain Management: An International Journal* 26 (6): 737–752. https://doi.org/10.1108/SCM-09-2020-0470.

Domański, B., R. Guzik, K. Gwosdz, and M. Dej. 2013. "The Crisis and beyond: The Dynamics and Restructuring of Automotive Industry in Poland." *International Journal of Automotive Technology and Management* 13 (2): 151–166. https://doi.org/10.1504/IJATM.2013.052998.

Donaldson, L. 2001. *The Contingency Theory of Organizations*. Thousand Oaks, CA: SAGE Publications Inc.

Dubey, R., D. J. Bryde, C. Blome, Y. K. Dwivedi, S. J. Childe, and C. Foropon. 2024. "Alliances and Digital Transformation are Crucial for Benefiting from Dynamic Supply Chain Capabilities during Times of Crisis: A Multi-Method Study." *International Journal of Production Economics* 269: 109166. https://doi.org/10.1016/j.ijpe.2024.109166.

Durugbo, C. 2016. "Collaborative Networks: A Systematic Review and Multi-Level Framework." *International Journal of Production Research* 54 (12): 3749–3776. https://doi.org/10.1080/00207543.2015.1122249.

Durugbo, C. M. 2020. "After-Sales Services and Aftermarket Support: A Systematic Review, Theory and Future Research Directions." *International Journal of Production Research* 58 (6): 1857–1892. https://doi.org/10.1080/00207543.2019.1693655.

Durugbo, C. M., and Z. Al-Balushi. 2023. "Supply Chain Management in Times of Crisis: A Systematic Review." *Management Review Quarterly* 73 (3): 1179–1235. https://doi.org/10.1007/s11301-022-00272-x.

Durugbo, C. M., S. M. Almahamid, L. H. Budalamah, O. R. Al-Jayyousi, and B. BendiMerad. 2022. "Managing Regional Logistics in Times of Crisis: A COVID-19 Case Study." *Journal of Humanitarian Logistics and Supply Chain Management* 12 (1): 54–77. https://doi.org/10.1108/JHLSCM-01-2021-0001.

Durugbo, C. M., O. Amoudi, Z. Al-Balushi, and A. L. Anouze. 2020. "Wisdom from Arabian Networks: A Review and Theory of Regional Supply Chain Management." *Production Planning & Control* 32 (15): 1265–1281. https://doi.org/10.1080/09537287.2020.1796144.

Eisenhardt, K. M., and M. E. Graebner. 2007. "Theory Building from Cases: Opportunities and Challenges." *Academy of Management Journal* 50 (1): 25–32. https://doi.org/10.5465/amj.2007.24160888.

Elluru, S., H. Gupta, H. Kaur, and S. P. Singh. 2019. "Proactive and Reactive Models for Disaster Resilient Supply Chain." *Annals of Operations Research* 283 (1–2): 199–224. https://doi.org/10.1007/s10479-017-2681-2.

von Falkenhausen, C., M. Fleischmann, and C. Bode. 2019. "How to Find the Right Supply Chain Strategy? An Analysis of Contingency Variables." *Decision Sciences* 50 (4): 726–755. https://doi.org/10.1111/deci.12355.

Farahani, M., H. Shavandi, and D. Rahmani. 2017. "A Location-Inventory Model Considering a Strategy to Mitigate Disruption Risk in Supply Chain by Substitutable Products." *Computers & Industrial Engineering* 108: 213–224. https://doi.org/10.1016/j.cie.2017.04.032.

Faruquee, M., A. Paulraj, and C. A. Irawan. 2023. "A Typology of Supply Chain Resilience: Recognising the Multi-Capability Nature of Proactive and Reactive Contexts." *Production Planning & Control* 1–21. https://doi.org/10.1080/09537287.2023.2202151.

Fearne, A., B. Wagner, N. McDougall, and D. Loseby. 2021. "The Power of Purpose – Lessons in Agility from the Ventilator Challenge." *Supply Chain Management* 26 (6): 753–766. https://doi.org/10.1108/SCM-09-2020-0468.

Fischbacher-Smith, D., and L. Smith. 2015. "Navigating the 'Dark Waters of Globalisation': Global Markets, Inequalities and the Spatial Dynamics of Risk." *Risk Management* 17 (3): 179–203. https://doi.org/10.1057/rm.2015.12.

Friese, S. 2014. *Qualitative Data Analysis with ATLAS.ti*. London: SAGE.

Gao, H., J. G. Knight, H. Zhang, D. Mather, and L. P. Tan. 2012. "Consumer Scapegoating during a Systemic Product-Harm Crisis." *Journal of Marketing Management* 28 (11–12): 1270–1290. https://doi.org/10.1080/0267257X.2011.645859.

von der Gracht, H. A., and I. L. I. Darkow. 2013. "The Future Role of Logistics for Global Wealth - Scenarios and Discontinuities Until 2025." *Foresight* 15 (5): 405–419. https://doi.org/10.1108/FS-05-2012-0031.

Grötsch, V. M., C. Blome, and M. C. Schleper. 2013. "Antecedents of Proactive Supply Chain Risk Management – a Contingency Theory Perspective." *International Journal of Production Research* 51 (10): 2842–2867. https://doi.org/10.1080/00207543.2012.746796.

Gulati, R., N. Nohria, and F. Wohlgezogen. 2010. "Roaring out of Recession." *Harvard Business Review* 88 (3): 62–69. https://hbr.org/2010/03/roaring-out-of-recession.

Hale, T., and C. R. Moberg. 2005. "Improving Supply Chain Disaster Preparedness: A Decision Process for Secure Site Location." *International Journal of Physical Distribution & Logistics Management* 35 (3): 195–207. https://doi.org/10.1108/09600030510594576.

Handfield, R. B., G. Graham, and L. Burns. 2020. "Corona Virus, Tariffs, Trade Wars and Supply Chain Evolutionary Design." *International Journal of Operations & Production Management* 40 (10): 1649–1660. https://doi.org/10.1108/IJOPM-03-2020-0171.

Harland, C. 2021. "Discontinuous Wefts: Weaving a More Interconnected Supply Chain Management Tapestry." *Journal of Supply Chain Management* 57 (1): 27–40. https://doi.org/10.1111/jscm.12249.

Harland, C. M., L. Knight, A. S. Patrucco, J. Lynch, J. Telgen, E. Peters, T. Tátrai, and P. Ferk. 2021. "Practitioners' Learning about Healthcare Supply Chain Management in the COVID-19 Pandemic: A Public Procurement Perspective." *International Journal of Operations & Production Management* 41 (13): 178–189. https://doi.org/10.1108/IJOPM-05-2021-0348.

Harpring, R., A. Maghsoudi, C. Fikar, W. D. Piotrowicz, and G. Heaslip. 2021. "An Analysis of Compounding Factors of Epidemics in Complex Emergencies: A System Dynamics Approach." *Journal of Humanitarian Logistics and Supply Chain Management* 11 (2): 198–226. https://doi.org/10.1108/JHLSCM-07-2020-0063.

Heras-Saizarbitoria, I., O. Boiral, and G. Arana. 2016. "Renewing Environmental Certification in Times of Crisis." *Journal of Cleaner Production* 115: 214–223. https://doi.org/10.1016/j.jclepro.2015.09.043.

Hermann, C. F. 1963. "Some Consequences of Crisis Which Limit the Viability of Organizations." *Administrative Science Quarterly* 8 (1): 61. https://doi.org/10.2307/2390887.

Hittle, B., and K. M. Leonard. 2011. "Decision Making in Advance of a Supply Chain Crisis." *Management Decision* 49 (7): 1182–1193. https://doi.org/10.1108/00251741111151208.

Ivanov, D. 2022. "Viable Supply Chain Model: Integrating Agility, Resilience and Sustainability Perspectives—Lessons from and Thinking beyond the COVID-19 Pandemic." *Annals of Operations Research* 319 (1): 1411–1431. https://doi.org/10.1007/s10479-020-03640-6.

Javadi, M., and K. Zarea. 2016. "Understanding Thematic Analysis and its Pitfall." *Journal of Client Care* 1 (1): 33–39. https://doi.org/10.15412/J.JCC.02010107.

Johnson, N., D. Elliott, and P. Drake. 2013. "Exploring the Role of Social Capital in Facilitating Supply Chain Resilience." *Supply Chain Management: An International Journal* 18 (3): 324–336. https://doi.org/10.1108/SCM-06-2012-0203.

Karaosman, H., D. Marshall, and V. H. Villena. 2023. "Chrysalis of Crisis: Covid-19 as a Catalyst for Awakening Power and Justice in a Luxury Fashion Supply Chain." *International Journal of Operations & Production Management* 43 (10): 1634–1666. https://doi.org/10.1108/IJOPM-05-2022-0320.

Kassahun, A., R. J. M. M. Hartog, T. Sadowski, H. Scholten, T. Bartram, S. Wolfert, and A. J. M. M. Beulens. 2014. "Enabling Chain-Wide Transparency in Meat Supply Chains Based on the EPCIS Global Standard and Cloud-Based Services." *Computers and Electronics in Agriculture* 109: 179–190. https://doi.org/10.1016/j.compag.2014.10.002.

Kent, P., and H. Haralambides. 2022. "A Perfect Storm or an Imperfect Supply Chain? The US Supply Chain Crisis." *Maritime Economics & Logistics* 24 (1): 1–8. https://doi.org/10.1057/s41278-022-00221-1.

Kleindorfer, P. R., J. C. Belke, M. R. Elliott, K. Lee, R. A. Lowe, and H. I. Feldman. 2003. "Accident Epidemiology and the US Chemical Industry: Accident History and Worst-Case Data from RMP*Info." *Risk Analysis* 23 (5): 865–881. https://doi.org/10.1111/1539-6924.00365.

Koilo, V., and O. H. Grytten. 2019. "Maritime Financial Instability and Supply Chain Management Effects." *Problems and Perspectives in*

Management 17 (4): 62–79. https://doi.org/10.21511/ppm.17(4).2019.06.

Kovács, G., and I. F. Sigala. 2021. "Lessons Learned from Humanitarian Logistics to Manage Supply Chain Disruptions." *Journal of Supply Chain Management* 57 (1): 41–49. https://doi.org/10.1111/jscm.12253.

Lawrence, P. R., and J. W. Lorsch. 1967. *Organization and Environment: Managing Differentiation and Integration*. Homewood, IL: R. D. Irwin.

Leeuw, S., V. C. S. de, S. Wiers, V. C. De Leeuw, and S. Wiers. 2015. "Warehouse Manpower Planning Strategies in Times of Financial Crisis: Evidence from Logistics Service Providers and Retailers in the Netherlands." *Production Planning and Control* 26 (4): 328–337. https://doi.org/10.1080/09537287.2014.904531.

Levine, D. K. 2012. "Production Chains." *Review of Economic Dynamics* 15 (3): 271–282. https://doi.org/10.1016/j.red.2012.01.003.

Li, H., J. Sun, J. Wu, and X. J. Wu. 2012. "Supply Chain Trust Diagnosis (SCTD) Using Inductive Case-Based Reasoning Ensemble (ICBRE): The Case of General Competence Trust Diagnosis." *Applied Soft Computing* 12 (8): 2312–2321. https://doi.org/10.1016/j.asoc.2012.03.029.

Li, L., K. Du, S. Xin, and W. Zhang. 2017. "Creating Value through IT-Enabled Integration in Public Organizations: A Case Study of a Prefectural Chinese Center for Disease Control and Prevention." *International Journal of Information Management* 37 (1): 1575–1580. https://doi.org/10.1016/j.ijinfomgt.2016.07.002.

Liu, Z. 2013. "The co-Evolution of Integrated Corporate Financial Networks and Supply Chain Networks with Insolvency Risk." *Computational Management Science* 10 (2–3): 253–275. https://doi.org/10.1007/s10287-013-0161-y.

Lu, X., A. L. Horn, J. Su, and J. Jiang. 2019. "A Universal Measure for Network Traceability." *Omega* 87: 191–204. https://doi.org/10.1016/j.omega.2018.09.004.

Mackey, T. K., and B. A. Liang. 2011. "The Global Counterfeit Drug Trade: Patient Safety and Public Health Risks." *Journal of Pharmaceutical Sciences* 100 (11): 4571–4579. https://doi.org/10.1002/jps.22679.

Mammadova, A., J. Behagel, and M. Masiero. 2020. "Making Deforestation Risk Visible. Discourses on Bovine Leather Supply Chain in Brazil." *Geoforum* 112: 85–95. https://doi.org/10.1016/j.geoforum.2020.03.008.

Manning, L. 2007. "Food Safety and Brand Equity." *British Food Journal* 109 (7): 496–510. https://doi.org/10.1108/00070700710761491.

Mazzarino, M. 2012. "Strategic Scenarios of Global Logistics: What Lies Ahead for Europe?" *European Transport Research Review* 4 (1): 1–18. https://doi.org/10.1007/s12544-011-0069-y.

McKinsey Global Institute. 2021. "Building National Supply Chain Resilience." McKinsey Insights. https://www.mckinsey.com/mgi/overview/in-the-news/building-national-supply-chain-resilience (accessed 01 April, 2024)

Memon, M. S., Y. H. Lee, and S. I. Mari. 2015. "Analysis of Traceability Optimization and Shareholder's Profit for Efficient Supply Chain Operation under Product Recall Crisis." *Mathematical Problems in Engineering* 2015: 1–8. https://doi.org/10.1155/2015/896239.

Merz, M., M. Hiete, and V. Bertsch. 2009. "Multicriteria Decision Support for Business Continuity Planning in the Event of Critical Infrastructure Disruptions." *International Journal of Critical Infrastructures* 5 (1–2): 156–174. https://doi.org/10.1504/IJCIS.2009.022854.

Meyer-Larsen, N., D. Lyridis, R. Müller, and P. Zacharioudakis. 2012. "Improving Intermodal Container Logistics and Security by RFID." *International Journal of RF Technologies* 3 (1): 15–38. https://doi.org/10.3233/RFT-2011-015.

Miles, M. B., and A. M. Huberman. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. London: Sage Publications, Inc.

Min, H. 2023a. "Supply Chain Crisis Management in the Wake of the COVID-19 Pandemic." *International Journal of Logistics Systems and Management* 44 (1): 1. https://doi.org/10.1504/IJLSM.2023.128555.

Min, H. 2023b. "Assessing the Impact of a COVID-19 Pandemic on Supply Chain Transformation: An Exploratory Analysis." *Benchmarking: An International Journal* 30 (6): 1765–1781. https://doi.org/10.1108/BIJ-04-2022-0260.

Min, H., and I. Kim. 2011. "Measuring the Risk of Sourcing from Low Cost Countries: A Macro Perspective." *International Journal of Services and Operations Management* 9 (3): 308–329. https://doi.org/10.1504/IJSOM.2011.041102.

Moretto, A., and F. Caniato. 2021. "Can Supply Chain Finance Help Mitigate the Financial Disruption Brought by Covid-19?" *Journal of Purchasing and Supply Management* 27 (4): 100713. https://doi.org/10.1016/j.pursup.2021.100713.

Narasimha, P. T., P. R. Jena, and R. Majhi. 2021. "Impact of COVID-19 on the Indian Seaport Transportation and Maritime Supply Chain." *Transport Policy* 110: 191–203. https://doi.org/10.1016/j.tranpol.2021.05.011.

Natarajarathinam, M., I. Capar, and A. Narayanan. 2009. "Managing Supply Chains in Times of Crisis: A Review of Literature and Insights." *International Journal of Physical Distribution & Logistics Management* 39 (7): 535–573. https://doi.org/10.1108/09600030910996251.

Notteboom, T., H. Haralambides, and K. Cullinane. 2024. "The Red Sea Crisis: Ramifications for Vessel Operations, Shipping Networks, and Maritime Supply Chains." *Maritime Economics & Logistics* 26 (1): 1–20. https://doi.org/10.1057/s41278-024-00287-z.

Notteboom, T., T. Pallis, and J.-P. Rodrigue. 2021. "Disruptions and Resilience in Global Container Shipping and Ports: The COVID-19 Pandemic versus the 2008–2009 Financial Crisis." *Maritime Economics & Logistics* 23 (2): 179–210. https://doi.org/10.1057/s41278-020-00180-5.

Overby, J., M. Rayburn, K. Hammond, and D. C. Wyld. 2004. "The China Syndrome: The Impact of the SARS Epidemic in Southeast Asia." *Asia Pacific Journal of Marketing and Logistics* 16 (1): 69–94. https://doi.org/10.1108/13555850410765131.

Oxford Dictionary. 2020. *Oxford Dictionary of English*. Oxford: Oxford University Press.

Oxford Dictionary. 2021. *Collins English Dictionary*. Glasgow: HarperCollins.

Panwar, R., R. Vlosky, and E. Hansen. 2012. "Gaining Competitive Advantage in the New Normal." *Forest Products Journal* 62 (6): 420–428. https://doi.org/10.13073/FPJ-D-12-00104.1.

Pashapour, S., A. Bozorgi-Amiri, A. Azadeh, S. F. Ghaderi, and A. Keramati. 2019. "Performance Optimization of Organizations Considering Economic Resilience Factors under Uncertainty: A Case Study of a Petrochemical Plant." *Journal of Cleaner Production* 231: 1526–1541. https://doi.org/10.1016/j.jclepro.2019.05.171.

Perry, C. 1998. "Processes of a Case Study Methodology for Postgraduate Research in Marketing." *European Journal of Marketing* 32 (9–10): 785–802. https://doi.org/10.1108/03090569810232237.

Pessot, E., I. Marchiori, A. Zangiacomi, and R. Fornasiero. 2021. "A Journey into the European Supply Chains: Key Industries and Best Practices." In *Next Generation Supply Chains. Lecture Notes in Management and Industrial Engineering*, edited by R. Fornasiero, S. Sardesai, A.C. Barros, and A. Matopoulos, 235–264. Cham, Switzerland: Springer.

Pfohl, H. C., H. Köhler, and D. Thomas. 2010. "State of the Art in Supply Chain Risk Management Research: Empirical and Conceptual Findings and a Roadmap for the Implementation in Practice." *Logistics Research* 2 (1): 33–44. https://doi.org/10.1007/s12159-010-0023-8.

Pinior, B., U. Platz, U. Ahrens, B. Petersen, F. Conraths, and T. Selhorst. 2012. "The German Milky Way: Trade Structure of the Milk Industry and Possible Consequences of a Food Crisis." *Journal on Chain and Network Science* 12 (1): 25–39. https://doi.org/10.3920/JCNS2012.x001.

Poberschnigg, T. F. da S., M. L. Pimenta, and P. Hilletofth. 2020. "How Can Cross-Functional Integration Support the Development of Resilience Capabilities? The Case of Collaboration in the Automotive Industry." *Supply Chain Management: An International Journal* 25 (6): 789–801. https://doi.org/10.1108/SCM-10-2019-0390.

Ponis, S. T., and E. Koronis. 2012. "A Knowledge Management Process-Based Approach to Support Corporate Crisis Management." *Knowledge and Process Management* 19 (3): 148–159. https://doi.org/10.1002/kpm.1390.

Prajogo, D., C. Mena, and A. Nair. 2018. "The Fit Between Supply Chain Strategies and Practices: A Contingency Approach and Comparative Analysis." *IEEE Transactions on Engineering Management* 65 (1): 168–180. https://doi.org/10.1109/TEM.2017.2756982.

Primo, M. A. M., F. L. DuBois, M. de L. M. C. de Oliveira, E. S. D. de M. Amaro, and D. D. N. Moser. 2021. "Lean Manufacturing

Implementation in Time of Crisis: The Case of Estaleiro Atlântico Sul." *Production Planning & Control* 32 (8): 623–640. https://doi.org/10.1080/09537287.2020.1747655.

Quayson, M., C. Bai, and V. Osei. 2020. "Digital Inclusion for Resilient Post-COVID-19 Supply Chains: Smallholder Farmer Perspectives." *IEEE Engineering Management Review* 48 (3): 104–110. https://doi.org/10.1109/EMR.2020.3006259.

Razak, G. M., L. C. Hendry, and M. Stevenson. 2023. "Supply Chain Traceability: A Review of the Benefits and Its Relationship with Supply Chain Resilience." *Production Planning & Control* 34 (11): 1114–1134. https://doi.org/10.1080/09537287.2021.1983661.

Romero-Silva, R., J. Santos, and M. Hurtado-Hernández. 2024. "A Conceptual Framework of the Applicability of Production Scheduling from a Contingency Theory Approach: Addressing the Theory-Practice Gap." *Production Planning & Control* 35 (3): 262–282. https://doi.org/10.1080/09537287.2022.2076627.

Rosenthal, U., R. A. Boin, and L. K. Comfort. 2001. *Managing Crises: Threats, Dilemmas, Opportunities*. Springfield: Charles C Thomas Pub Ltd.

Roshan, M., R. Tavakkoli-Moghaddam, and Y. Rahimi. 2019. "A Two-Stage Approach to Agile Pharmaceutical Supply Chain Management with Product Substitutability in Crises." *Computers & Chemical Engineering* 127: 200–217. https://doi.org/10.1016/j.compchemeng.2019.05.014.

Sass, M., and A. Szalavetz. 2013. "Crisis and Upgrading: The Case of the Hungarian Automotive and Electronics Sectors." *Europe-Asia Studies* 65 (3): 489–507. https://doi.org/10.1080/09668136.2013.779463.

Sawyerr, E., and C. Harrison. 2019. "Developing Resilient Supply Chains: Lessons from High-Reliability Organisations." *Supply Chain Management: An International Journal* 25 (1): 77–100. https://doi.org/10.1108/SCM-09-2018-0329.

Sellers, M. N. S. 2003. "Ideals of Public Discourse." In *Republican Legal Theory*, 62–70. London: Palgrave Macmillan UK.

Sheng, M. L., and S. Saide. 2021. "Supply Chain Survivability in Crisis Times through a Viable System Perspective: Big Data, Knowledge Ambidexterity, and the Mediating Role of Virtual Enterprise." *Journal of Business Research* 137: 567–578. https://doi.org/10.1016/j.jbusres.2021.08.041.

Siebert, J. U., M. Brandenburg, and J. Siebert. 2020. "Defining and Aligning Supply Chain Objectives Before, During, and after the COVID-19 Pandemic." *IEEE Engineering Management Review* 48 (4): 72–85. https://doi.org/10.1109/EMR.2020.3032369.

Spieske, A., M. Gebhardt, M. Kopyto, and H. Birkel. 2022. "Improving Resilience of the Healthcare Supply Chain in a Pandemic: Evidence from Europe during the COVID-19 Crisis." *Journal of Purchasing and Supply Management* 28 (5): 100748. https://doi.org/10.1016/j.pursup.2022.100748.

Sprecher, B., I. Daigo, W. Spekkink, M. Vos, R. Kleijn, S. Murakami, and G. J. Kramer. 2017. "Novel Indicators for the Quantification of Resilience in Critical Material Supply Chains, with a 2010 Rare Earth Crisis Case Study." *Environmental Science & Technology* 51 (7): 3860–3870. https://doi.org/10.1021/acs.est.6b05751.

Stewart, D., and M. A. Kamins. 1993. *Secondary Research: Information Sources and Methods*. London: SAGE Publications Ltd.

Tan, W.-J., and P. Enderwick. 2006. "Managing Threats in the Global Era: The Impact and Response to SARS." *Thunderbird International Business Review* 48 (4): 515–536. https://doi.org/10.1002/tie.20107.

Tharenou, P., R. Donohue, and B. Cooper. 2007. *Management Research Methods*. Cambridge: Cambridge University Press.

Thomas, D. R. 2006. "A General Inductive Approach for Analyzing Qualitative Evaluation Data." *American Journal of Evaluation* 27 (2): 237–246. https://doi.org/10.1177/1098214005283748.

Thompson, D. D. P., and R. Anderson. 2021. "The COVID-19 Response: Considerations for Future Humanitarian Supply Chain and Logistics Management Research." *Journal of Humanitarian Logistics and Supply Chain Management* 11 (2): 157–175. https://doi.org/10.1108/JHLSCM-01-2021-0006.

Thompson, J. D. 1967. *Organizations in Action: Social Science Bases of Administrative Theory*. New York, NY: McGraw-Hill.

Tomlin, B. 2006. "On the Value of Mitigation and Contingency Strategies for Managing Supply Chain Disruption Risks." *Management Science* 52 (5): 639–657. https://doi.org/10.1287/mnsc.1060.0515.

The Economist Intelligence Unit. 2021. "The Business Costs of Supply-Chain Disruption." *Economist Impact*. https://impact.economist.com/perspectives/sites/default/files/the_business_costs_of_supply_chain_disruption_gep_1.pdf (accessed 01 April, 2024)

Upton, E., and W. J. Nuttall. 2014. "Fuel Panics: Insights from Spatial Agent-Based Simulation." *IEEE Transactions on Intelligent Transportation Systems* 15 (4): 1499–1509. https://doi.org/10.1109/TITS.2014.2302358.

Urciuoli, L., S. Mohanty, J. Hintsa, and E. G. Boekesteijn. 2014. "The Resilience of Energy Supply Chains: A Multiple Case Study Approach on Oil and Gas Supply Chains to Europe." *Supply Chain Management: An International Journal* 19 (1): 46–63. https://doi.org/10.1108/SCM-09-2012-0307.

VanVactor, J. D. 2011. "Cognizant Healthcare Logistics Management: Ensuring Resilience during Crisis." *International Journal of Disaster Resilience in the Built Environment* 2 (3): 245–255. https://doi.org/10.1108/17595901111167114.

Vega, D., A. Arvidsson, and F. Saïah. 2023. "Resilient Supply Management Systems in Times of Crisis." *International Journal of Operations & Production Management* 43 (1): 70–98. https://doi.org/10.1108/IJOPM-03-2022-0192.

Vo, T. L. H., and D. Thiel. 2011. "Economic Simulation of a Poultry Supply Chain Facing a Sanitary Crisis." *British Food Journal* 113 (8): 1011–1030. https://doi.org/10.1108/00070701111153760.

Wagner, S. M., and C. Bode. 2006. "An Empirical Investigation into Supply Chain Vulnerability." *Journal of Purchasing and Supply Management* 12 (6): 301–312. https://doi.org/10.1016/j.pursup.2007.01.004.

Wagner, S. M., K. J. Mizgier, and S. Papageorgiou. 2017. "Operational Disruptions and Business Cycles." *International Journal of Production Economics* 183: 66–78. https://doi.org/10.1016/j.ijpe.2016.10.002.

Walsham, G. 1993. *Interpreting Information Systems in Organizations*. Chichester, West Sussex: Wiley.

Wang, J., R. Dou, R. R. Muddada, and W. Zhang. 2018. "Management of a Holistic Supply Chain Network for Proactive Resilience: Theory and Case Study." *Computers & Industrial Engineering* 125: 668–677. https://doi.org/10.1016/j.cie.2017.12.021.

Withers, M. C., K. G. Corley, and A. J. Hillman. 2012. "Stay or Leave: Director Identities and Voluntary Exit from the Board during Organizational Crisis." *Organization Science* 23 (3): 835–850. https://doi.org/10.1287/orsc.1110.0660.

Wojtczuk-Turek, A., D. Turek, and M. Mitręga. 2022. "Pandemics Related-Demands upon Managers and Job Crafting in the Production Sector in Poland." *Production Planning & Control*, 1–18. https://doi.org/10.1080/09537287.2022.2066016.

Wong, C. Y., S. Boon-Itt, and C. W. Y. Wong. 2011. "The Contingency Effects of Environmental Uncertainty on the Relationship between Supply Chain Integration and Operational Performance." *Journal of Operations Management* 29 (6): 604–615. https://doi.org/10.1016/j.jom.2011.01.003.

Ye, F., K. Liu, L. Li, K. H. Lai, Y. Zhan, and A. Kumar. 2022. "Digital Supply Chain Management in the COVID-19 Crisis: An Asset Orchestration Perspective." *International Journal of Production Economics* 245: 108396. https://doi.org/10.1016/j.ijpe.2021.108396.

Yin, R. K. 2013. "Validity and Generalization in Future Case Study Evaluations." *Evaluation* 19 (3): 321–332. https://doi.org/10.1177/1356389013497081.

Yin, R. K. 2017. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks, CA: Sage Publications, Inc.

Zhao, G., M. Vazquez-Noguerol, S. Liu, and J. C. Prado-Prado. 2024. "Agri-Food Supply Chain Resilience Strategies for Preparing, Responding, Recovering, and Adapting in Relation to Unexpected Crisis: A Cross-Country Comparative Analysis from the COVID-19 Pandemic." *Journal of Business Logistics* 45 (1): e12361. https://doi.org/10.1111/jbl.12361.

Appendix I: Public discourse sources for case study

NotPetya Cyberattack on Maersk case sources

1. ACLS, Audit Committee Leadership Submit (2018) Lessons from cyber-breach responses, Tapestry Networks, May 2018, access at https://www.tapestrynetworks.com/sites/default/files/publication_pdf/ACLS%20View Points%20-%20Cyber-breach%20response%20-%20April%202018%20-%20FINAL_0.pdf (accessed on April 7, 2022)
2. Boccio, D. (2019) Insights into Supply Chain Cyberattacks: From Ports to Production, DHL Resilience360, January 15, 2019 https://spendmatters.com/2019/01/15/insights-into-supply-chain-cyberattacks-from-ports-to-production/ (accessed on April 7, 2022)
3. Churchill, J. (2017), "When the Screens Went Black," Maersk Post, September 14, 2017, p 12-14 https://www.maersk.com/press/publications (accessed on April 7, 2022)
4. Crosignani, M., F. Silva, A., & Macchiavelli, M. (2022). Cyberattacks and supply chain disruptions. Liberty Street Economics. Retrieved from https://libertystreeteconomics.newyorkfed.org/2021/06/cyberattacks-and-supply-chain-disruptions/ (accessed on April 7, 2022)
5. Forrest, C. (2017). Notpetya ransomware outbreak cost Merck more than $300 m per quarter. TechRepublic. Retrieved from https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/#:~:text=Pharmaceutical%20giant%20Merck%20lost%20roughly,said%20on%20an%20earnings%20call (accessed on April 7, 2022)
6. Greenberg, A. (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, 22 August https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed on 7 July 2020)
7. Greig, J. (2020) Nearly 300 cybersecurity incidents impacted supply chain entities in 2019, TechRepublich; March 12 2020, https://www.techrepublic.com/article/nearly-300-cybersecurity-incidents-impacted-supply-chain-entities-in-2019/
8. ISTR (2019) Internet Security Threat Report, Symantec, Volume 24, February 2019 (https://docs.broadcom.com/doc/istr-24-2019-en) (accessed on April 7, 2022)
9. Kapadia, S. (2020) 3 years, 3 cyberattacks on major ocean carriers. How can shippers protect themselves?, Supply Chain Dive, https://www.supplychaindive.com/news/ocean-carrier-cybersecurity-maersk-msc-cosco/576754/(accessed on April 7, 2022)
10. Milne, R. (2017) Maersk CEO Soren Skou on surviving a cyber-attack, Financial Times, August 13, 2017, https://www.ft.com/content/785711bc-7c1b-11e7-9108-edda0bcbc928
11. Morgan, S. (2019), 2019 Official Annual Cybercrime Report, Cybersecurity Ventures https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/
12. Nash, K. S., Castellanos, S. & Janofsky, A. (2018) One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs, The Wall Street Journal, June 27, 2018, source https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906 (accessed on 25 July 2020)
13. Palmer, D. (2019) Ransomware: The key lesson Maersk learned from battling the NotPetya attack, ZD NET, April 29, from https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/ (accessed on 7 July 2020)
14. Rosendahl, A. (2017), Siblings Bury the Hatchet, Maersk Post, Page 20-23 | September-November 2017 https://www.maersk.com/press/publications
15. Saul, J. (2017) Global shipping feels fallout from Maersk cyber-attack, Technology News, JUNE 29, retrieved from https://www.reuters.com/article/us-cyber-attack-maersk/global-shipping-feels-fallout-from-maersk-cyber-attack-idUSKBN19K2LE (accessed on 7 July 2020)
16. Sharkov, D. (2018). Russia accused of massive $1.2 billion cyberattack. Newsweek. Retrieved from https://www.newsweek.com/russia-accused-massive-12-billion-cyber-attack-807867 (accessed on April 7, 2022)
17. Stone, I. (2019) The Future of the Supply Chain Managing: the impact of climate change, political uncertainty and digitalisation, Vuealta, https://www.vuealta.com/blog/the-future-of-the-supply-chain/ (accessed on April 7, 2022)
18. Tracy, P. (2016) Big data helps Paramount and Maersk Line adapt to changing times, RCR wireless news, September 15, 2016 https://www.rcrwireless.com/20160915/big-data-analytics/paramount-maersk-big-data-tag31-tag99 (accessed on April 7, 2022)
19. Valour Consultancy (2017) Maersk Cyber-Attack: A Lesson Learned? 04 AUG 17 https://valourconsultancy.com/maersk-cyber-attack-lesson-learned/ (accessed on April 7, 2022)
20. PTI (2017) New malware hits JNPT operations as APM Terminals hacked globally, http://indianexpress.com/article/india/cyber-attack-new-malware-hits-jnpt-ops-as-apm-terminals-hacked-globally-4725102/ (accessed on April 7, 2022)
21. Swinhoe, D. (2019) Rebuilding after NotPetya: How Maersk moved forward, CSO | OCT 9, 2019 https://www.csoonline.com/article/3444620/rebuilding-after-notpetya-how-maersk-moved-forward.html (accessed on April 7, 2022)

Evonik plant explosion case sources

1. Belgium: CLEPA, Japia Quiet on Evonik blast as fire details emerge. Just Auto. (2012). Retrieved from https://www.just-auto.com/news/belgium-clepa-japia-quiet-on-evonik-blast-as-fire-details-emerge/ (accessed on June 10, 2022)
2. Bowman, R. J. (2012). Are You Ready for the Next Supply-Chain Disaster? Think tank RSS. SupplyChainBrain RSS. Retrieved from https://www.supplychainbrain.com/blogs/1-think-tank/post/13562-are-you-ready-for-the-next-supply-chain-disaster (accessed on June 10, 2022)
3. Bryant, C., & Wilson, J. (n.d.). Evonik IPO to underscore its key role. Subscribe to read | Financial Times. Retrieved from https://www.ft.com/content/e58f57a4-a0ce-11e1-851f-00144feabdc0 (accessed on June 10, 2022)
4. Carty, S. S. (2012). Obscure chemical shortage threatens to disrupt U.S. auto industry. HuffPost. Retrieved from https://www.huffpost.com/entry/pa-12-resin-shortages-evonik-industries_n_1432386 (accessed on June 10, 2022)
5. Dow Jones & Company. (2012). Resin alert: Nylon-12 shortage could hurt car makers. The Wall Street Journal. Retrieved June 10, 2022, from https://www.wsj.com/articles/BL-DSB-8739 (accessed on June 10, 2022)
6. Eisenstein, P. A. (2012). Resin plant fire latest disaster to threaten Global Auto Industry. The Detroit Bureau. Retrieved from https://www.thedetroitbureau.com/2012/04/resin-plant-fire-latest-disaster-to-threaten-global-auto-industry/ (accessed on June 10, 2022)
7. Els, P. (2018). The recent evolution of Fuel System Materials. Automotive IQ. Retrieved from https://www.automotive-iq.com/lubricants-and-fuels/articles/the-recent-evolution-of-fuel-system-materials (accessed on June 10, 2022)
8. Esposito, F. (2012). Nylon 12 shortage ending, Evonik ready to resume CDT production. Plastics News. Retrieved from https://www.plasticsnews.com/article/20121204/NEWS/312049980/nylon-12-shortage-ending-evonik-ready-to-resume-cdt-production (accessed on June 10, 2022)
9. Esposito, F. (2013). Evonik recovers after nylon 12 shortage. Plastics News. Retrieved from https://www.plasticsnews.com/article/20131017/NEWS/131019931/evonik-recovers-after-nylon-12-shortage (accessed on June 10, 2022)
10. Evans, S. (2012). Fire in small German town could curb World Car production. BBC News. Retrieved from https://www.bbc.com/news/business-17769466 (accessed June 10, 2022)
11. Explosion at Evonik Factory May Have Serious Knock-On Effect for Global Car Production. S&P Global Market Intelligence. (2012). Retrieved from https://www.spglobal.com/marketintelligence/en/mi/country-industry-forecasting.html?id=1065966710 (accessed on June 10, 2022)
12. Express-News. (2012). Plant Blast Hits automakers. mySA. Retrieved from https://www.mysanantonio.com/business/article/Plant-blast-hits-automakers-3489369.php (accessed on June 10, 2022)
13. Fire at the CDT plant on the grounds of the marl chemicals park. Evonik Industries. (2019). Retrieved from https://corporate.evonik.

com/en/media/press-releases/corporate/fire-at-the-cdt-plant-on-the-grounds-of-the-marl-chemicals-park-106518.html (accessed June 10, 2022)
14. German factory explosion causes global car part shortage. IFSEC Global. (2012). Retrieved from https://www.ifsecglobal.com/uncategorized/german-factory-explosion-causes-global-car-part-shortage/ (accessed on June 10, 2022)
15. Germany: Fatal Evonik fire to disrupt resin supply until at least July. Just Auto. (2012). Retrieved from https://www.just-auto.com/news/germany-fatal-evonik-fire-to-disrupt-resin-supply-until-at-least-july/ (accessed on June 10, 2022)
16. Krisher, T. (2012). Resin shortage not likely to hurt production, Ford says. Arkansas Online. Retrieved from https://www.nwaonline.com/news/2012/apr/28/resin-shortage-not-likely-hurt-production-20120428/ (accessed on June 10, 2022)
17. Krisher, T. (2020). Automakers dodged parts shortage, but virus poses new threat. Yahoo! News. Retrieved from https://news.yahoo.com/automakers-dodged-parts-shortage-virus-164617472.html (accessed on June 10, 2022)
18. Logistics, A. (2012). Evonik explosion threatens severe parts shortage. Automotive Logistics. Retrieved from https://www.automotivelogistics.media/evonik-explosion-threatens-severe-parts-shortage/7709.article (accessed on June 10, 2022)
19. Nicholls, R. (2012). Evonik explosion severely affects SLS powder production. Rapid Prototyping, 3D Printing, Low Volume Production Company. Retrieved from https://mnl.co.uk/evonik-explosion-severely-affects-sls-powder-production/ (accessed on June 10, 2022)
20. PCI Magazine. (2012). Fatal fire at Evonik plant will likely disrupt CDT supply. PCI Magazine RSS. Retrieved from https://www.pcimag.com/articles/96307-fatal-fire-at-evonik-plant-will-likely-disrupt-cdt-supply (accessed on June 10, 2022)
21. Resilience strategies for complex supply chains: Evonik Industries - about resilience. About Resilience. (2021). Retrieved from https://www.aboutresilience.com/resilience-strategies-for-complex-supply-chains-evonik-industries/ (accessed on June 10, 2022)
22. Tullo, A. H. (2012). Cen.acs.org. Retrieved from https://cen.acs.org/articles/90/i17/Nylon-Shortage-Threatens-Automakers.html (accessed on June 10, 2022)
23. US: OESA Mulls Supply diversion as Evonik fire fallout continues. Just Auto. (2012). Retrieved from https://www.just-auto.com/news/us-oesa-mulls-supply-diversion-as-evonik-fire-fallout-continues/ (accessed on June 10, 2022)
24. WDIV ClickOnDetroit. (2012). Auto industry minds meet in Troy to discuss possible problems arising from shortage of PA-12 resin. WDIV. Retrieved from https://www.clickondetroit.com/business/2012/04/17/auto-industry-minds-meet-in-troy-to-discuss-possible-problems-arising-from-shortage-of-pa-12-resin/ (accessed on June 10, 2022)

Cadbury salmonella scare case sources

1. BBC. (2006). *Cadbury salmonella scare probed*. BBC News. Retrieved from http://news.bbc.co.uk/2/hi/uk_news/5112470.stm (accessed on April 14, 2022)
2. Boal, C. (2006). *Cadbury contamination proves costly*. confectionerynews.com. Retrieved from https://www.confectionerynews.com/Article/2006/08/02/Cadbury-contamination-proves-costly (accessed on April 14, 2022)
3. *Cadbury faces backlash over chocolate recalls*. The Economic Times. (2006). Retrieved https://economictimes.indiatimes.com/industry/cons-products/food/cadbury-faces-backlash-over-chocolate-recalls/articleshow/1679101.cms?from=mdr (accessed on April 15, 2022)
4. *Cadbury's linked to salmonella*. Talking Retail. (2006). Retrieved from https://www.talkingretail.com/news/industry-news/cadburys-linked-to-salmonella-21-07-2006/ (accessed on April 15, 2022)
5. CampaignUK. (2007). *Cadbury: Crisis, what crisis?* Campaign UK. Retrieved April 14, 2022, from https://www.campaignlive.co.uk/article/cadbury-crisis-crisis/735985 (accessed on April 14, 2022)
6. Dolan, A. (2007). *Cadbury fined £1 million over chocolate salmonella outbreak*. Daily Mail Online. Retrieved from https://www.dailymail.co.uk/news/article-468811/Cadbury-fined-1-million-chocolate-salmonella-outbreak.html (accessed on April 14, 2022)
7. ElAmin, A. (2006). *Cadbury apologises for salmonella outbreak*. foodnavigator.com. Retrieved from https://www.foodnavigator.com/Article/2006/07/25/Cadbury-apologises-for-Salmonella-outbreak (accessed on April 15, 2022)
8. Evening Standard. (2007). *Cadbury fined £1 million over chocolate salmonella outbreak*. Evening Standard. Retrieved from https://www.standard.co.uk/hp/front/cadbury-fined-ps1-million-over-chocolate-salmonella-outbreak-6598276.html (accessed on April 14, 2022)
9. Eyre, C. (2007). Cadbury pleads guilty to all salmonella charges. bakeryandsnacks.com. Retrieved from https://www.bakeryandsnacks.com/Article/2007/07/04/Cadbury-pleads-guilty-to-all-salmonella-charges (accessed on April 14, 2022)
10. Eyre, C. (2008). *Cadbury adopts New Pathogen Testing System*. bakeryandsnacks.com. Retrieved from https://www.bakeryandsnacks.com/Article/2008/02/04/Cadbury-adopts-new-pathogen-testing-system (accessed on April 15, 2022)
11. Hickman, M. (2006). *Salmonella outbreak hit Cadbury's plant in 2002*. The Independent. Retrieved from https://www.independent.co.uk/life-style/health-and-families/health-news/salmonella-outbreak-hit-cadbury-s-plant-in-2002-6096251.html (accessed on April 14, 2022)
12. The Irish Times. (2006). *Cadbury recalls 20,000 bars in salmonella scare*. The Irish Times. Retrieved from https://www.irishtimes.com/news/cadbury-recalls-20-000-bars-in-salmonella-scare-1.787827 (accessed on April 14, 2022)
13. Marketing Week. (2006). *Guilty of sweet nothing*. Marketing Week. Retrieved from https://www.marketingweek.com/guilty-of-sweet-nothing/ (accessed on April 15, 2022)
14. Poulter, S. (2006). *Cadbury Salmonella alert has spread to 30 products*. Daily Mail Online. Retrieved from https://www.dailymail.co.uk/news/article-393657/Cadbury-salmonella-alert-spread-30-products.html (accessed on April 15, 2022)
15. Smithers, R. (2007). *Cadbury faces prosecution after contamination*. The Guardian. Retrieved April 14, 2022, from https://www.theguardian.com/society/2007/feb/13/health.food (accessed on April 14, 2022)
16. Thomson Reuters. (2007). *Cadbury to be prosecuted over salmonella scare*. Reuters. Retrieved from https://www.reuters.com/article/uk-cadbury-salmonella-idUKL23170518200704 23 (accessed on April 14, 2022)
17. Thomson Reuters. (2022). *EU investigates chocolate-linked salmonella outbreak before Easter*. Reuters. Retrieved from https://www.reuters.com/world/europe/eu-investigates-chocolate-linked-salmonella-outbreak-before-easter-2022-04-06/ (accessed on April 14, 2022)
18. Tran, M. (2006). *Cadbury named over salmonella outbreak*. The Guardian. Retrieved April 14, 2022, from https://www.theguardian.com/business/2006/jul/21/food.foodanddrink (accessed on April 14, 2022)
19. *UK: Cadbury product recall sparks criticism over dangerous delays*. Just Food. (2006). Retrieved from https://www.just-food.com/news/uk-cadbury-product-recall-sparks-criticism-over-dangerous-delays/ (accessed on April 15, 2022)
20. Walker, P. (2007). *Cadbury 'moving on' from difficult 2006*. The Guardian. Retrieved from https://www.theguardian.com/business/2007/feb/20/cadburyschweppesbusiness (accessed on April 14, 2022)
21. Walsh, F. (2006). *Salmonella outbreak costs Cadbury £20 m*. The Guardian. Retrieved April 14, 2022, from https://www.theguardian.com/business/2006/aug/03/food.foodanddrink (accessed on April 14, 2022)
22. Watson, E. (2008). *Unanswered questions in Cadbury Salmonella Case*. foodmanufacture.co.uk. Retrieved from https://www.foodmanufacture.co.uk/Article/2008/09/15/Unanswered-questions-in-Cadbury-salmonella-case (accessed on April 15, 2022)

Horsemeat Scandal case sources

1. Addy, R. (2014) Supermarkets took supply chain 'on trust' – horsemeat, 10-Jan-2014, *Food Manufacture*, available at: https://www.foodmanufacture.co.uk/article/2014/01/10/horsemeat-industry-took-supply-chain-on-trust (accessed 12 Jun 2020)

2. BBC (2013) Horsemeat scandal: Food supply chain 'too complex' – Morrisons. 09 Feb 2013, available at: https://www.bbc.com/news/av/uk-21394451/horsemeat-scandal-food-supply-chain-too-complex-morrisons (accessed 12 Jun 2020)
3. BBC news (2013) Horsemeat scandal: 'Too trusting' on meat supplies, BBC 12 February 2013, available at: https://www.bbc.com/news/uk-21421477 (accessed 12 Jun 2020)
4. BBC (2013) Meat needs 'good traceability systems' First broadcast on BBC Radio 4's *Today Programme* on Saturday 9 February 2013.available at https://www.bbc.com/news/av/uk-21393407/meat-needs-good-traceability-systems (accessed 12 Jun 2020)
5. de Castella, T., & Wheeler, B. (2013). Horsemeat scandal: How often does food fraud happen? BBC News. Retrieved from https://www.bbc.com/news/magazine-21381689 (accessed on April 7, 2022)
6. Gibbons, L. (2014). "Government demands more detail from Elliott review", 19 May, Retrieved from: https://www.foodmanufacture.co.uk/Article/2014/05/19/Government-demands-more-detail-from-horse-meat-review (accessed 21 April 2020)
7. Hinks, G. (2018). Horsemeat scandal: The meat of the matter. The CFO. Retrieved from https://the-cfo.io/2013/03/18/horsemeat-scandal-the-meat-of-the-matter/ (accessed on April 7, 2022)
8. Holmes, H. (2022). Horsemeat seised in Europe as experts predict rise in food fraud from coronavirus. The Grocer. Retrieved from https://www.thegrocer.co.uk/food-safety/horsemeat-seised-in-europe-as-experts-predict-rise-in-food-fraud-from-coronavirus/604691.article (accessed on April 7, 2022)
9. HuffPost UK. (2013). What does the horsemeat scandal tell us about our supply chain? HuffPost UK. Retrieved from https://www.huffingtonpost.co.uk/2013/02/13/horsemeat-scandal-findus-supply-chain_n_2675465.html (accessed on April 7, 2022)
10. Lawrence, F. (2013). Horsemeat scandal: The Essential Guide. The Guardian. Retrieved from https://www.theguardian.com/uk/2013/feb/15/horsemeat-scandal-the-essential-guide (accessed on April 7, 2022)
11. Lawless, J. and Hinnant, L. (2013) Horsemeat Scandal Exposes Complex Food Chain, *manufacturing.net* Feb 13th, 2013, available at https://www.manufacturing.net/supplychain/news/13090287/horse-meat-scandal-exposes-complex-food-chain (accessed 12 Jun 2020)
12. Levitt, T. (2016). Three years on from the horsemeat scandal: 3 lessons we have learned. The Guardian. Retrieved from https://www.theguardian.com/sustainable-business/2016/jan/07/horsemeat-scandal-food-safety-uk-criminal-networks-supermarkets (accessed on April 7, 2022)
13. Levs, J., & Nyberg, P. (2013). Battle over blame after horse meat found in beef products. CNN. Retrieved from https://edition.cnn.com/2013/02/10/world/europe/uk-horsemeat-probe/index.html (accessed on April 7, 2022)
14. Nunes, K. (2014). Tesco C.E.O.: Horse Meat scandal a 'pivotal moment for our industry'. Food Business News. Retrieved from https://www.foodbusinessnews.net/articles/1925-tesco-c-e-o-horse-meat-scandal-a-pivotal-moment-for-our-industry#:~:text=BELFAST%2C%20IRELAND%20%E2%80%93%20Philip%20Clarke%2C,labelling%20it%20as%20100%25%20beef. (accessed on April 7, 2022)
15. Pierce, F. (2020), Globalised supply chain to blame for horsemeat scandal? Supply Chain, Feb 15 https://www.supplychaindigital.com/procurement/globalised-supply-chain-blame-horsemeat-scandal (accessed 12 Jun 2020)
16. Pendrous, R (2017), "Marks & Spencer Plans to cut its food supply base, 13 Oct, Retrieved from https://www.foodmanufacture.co.uk/Article/2017/06/30/Marks-Spencer-plans-to-cut-its-food-supplier-base (accessed 21 April 2020)
17. Rawlinson, K. (2017). Horsemeat scandal: Businessman found guilty of fraud. The Guardian. Retrieved April from https://www.theguardian.com/uk-news/2017/jul/26/horsemeat-scandal-businessman-andronicos-sideras (accessed on April 7, 2022)
18. Stones, M. (2013), "Government launches wide-ranging horsemeat review", 17 April, Retrieved from: https://www.foodmanufacture.co.uk/Article/2013/04/17/Horsemeat-government-launches-review-to-beat-food-fraud (accessed 21 April 2020)
19. Taylor, A. (2013). Europe's horse meat scandal is a direct consequence of the financial crisis. Yahoo! Finance. Retrieved from https://finance.yahoo.com/news/economic-crisis-created-europes-horse-193732076.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANpatfK93jiCJje98PS1cBOnwZW4s3DzDH2hDtj1q16Vut37FWH3Z0Fiko5FPkMJieL0w7eaAr6V-b4328NlAlfUaa7-jGDMAH1WV1qZ5cn__Rkuofx8JQlnpKp3ZJM7Z0m0msZLkOwZQm_J0lGgTK82leMsBlpfyM19cMe4ZSecR (accessed on April 7, 2022)
20. The Consumer Council. (2013), Food supply chain issues and the horsemeat scandal – the consumer view July 2013 *The Consumer Council* available at https://www.consumercouncil.org.uk/sites/default/files/original/Food_Supply_Chain_Issues_And_The_Horsemeat_Scandal_-_The_Consumer_View_July_2013.pdf (accessed 12 Jun 2020)
21. Willsher, K. (2019). Horsemeat scandal: Four on trial in Paris accused of fraud. The Guardian. Retrieved April from https://www.theguardian.com/uk-news/2019/jan/21/horsemeat-scandal-paris-fraud-trial#:~:text=The%20trial%20of%20four%20people,burgers%20labelled%20%E2%80%9Cpure%20beef%E2%80%9D. (accessed on April 7, 2022)
22. Wood, Z., & Lawrence, F. (2014). Horsemeat scandal: Food safety expert warns issues have not been addressed. The Guardian. Retrieved from https://www.theguardian.com/uk-news/2014/sep/04/horsemeat-food-safety-expert-chris-elliott (accessed on April 7, 2022)
23. Zuckerman, C. (2021). Europe's horse meat scandal escalates, investigations ensue. Culture. Retrieved from https://www.nationalgeographic.com/culture/article/130222-horse-meat-beef-scandal-food-france-england-europe-science-romania-nestle-horsemeat#:~:text=Authorities%20probe%20a%20murky%20food%20supply%20chain%20to%20pin%20down%20the%20source.&text=Europe's%20horse%20meat%20scandal%20escalated,Spain%2C%20Italy%2C%20and%20France. (accessed on April 7, 2022)

Appendix II: Crisis Timeline

NotPetya cyberattack on Maersk Timeline

27 June 2017	Maersk computer systems were attacked by NotPetya, a file-scrambling software targeting Microsoft Windows PCs was targeting businesses in Ukraine spread around the world
27 June 2017	The malware was contained to affect only the container-related businesses of Maersk, and therefore six out of nine businesses, including all Energy businesses, could uphold normal operations.
28 June 2017	Relying heavily on human resilience, managed 80% of shipping volume manually.
29 June 2017	Maersk operations around the globe returned to manual for the last 48 h
3 July 2017	Maersk gradually progressed to more normalized operations
6 July 2017	Maersk install over 4000 servers, 45,000 PCs and 2500 applications over the course of 10 d

Claire Tills, C. (2018). Case study: A.P. Møller-Maersk and NotPetya, clear security communication, May 21, available at: https://www.clairetills.com/post/2018/05/20/case-study-ap-m%C3%B8ller-maersk-and-notpetya, accessed on June 2020

Evonik plant explosion crisis timeline

31 March 2012	The plant at the Marl Chemicals Park near Duisburg in the north of Germany caught a fire leading to explosion of the plant leading to shutdown of the plant.
17 Apr 2012	200 representatives from auto suppliers and major automaker executives convened in Detroit on Tuesday to figure out how to replace PA-12. Also, Evonik told Reuters on Tuesday that it will take three months for its plant to resume normal production.
November 2012	An operation permit issued by Münster district government to the German Federal Emissions Law (BImSchG)
December 2012	CDT plant starts operating
January 2013	The first shipment of PA12 goes out

Carty, S. S. (2017). Obscure chemical shortage threatens to disrupt U.S. auto industry. HuffPost. Retrieved December 5, 2022, from https://www.huffpost.com/entry/pa-12-resin-shortages-evonik-industries_n_1432386

Evonik: Münster District Government Approves Operating Permit for CDT Plant. Plastinfo.ru. (2012, December 5). Retrieved December 5, 2022, from https://plastinfo.com/information/news/3409_05.12.2012/

Logistics, A. (2012). Evonik explosion threatens severe parts shortage. Automotive Logistics. Retrieved December 5, 2022, from https://www.automotivelogistics.media/evonik-explosion-threatens-severe-parts-shortage/7709.article

Snyder, J. (2017). 'Nylon 12' shortage? Watch Logistics Wizards work. Automotive News. Retrieved December 5, 2022, from https://www.autonews.com/article/20120417/BLOG06/120419905/nylon-12-shortage-watch-logistics-wizards-work

Cadbury salmonella scandal timeline

19 January 2006	Cadbury detected salmonella at Marlbrook, which produces chocolate crumb mixture, as a result dozens of people became ill with food poisoning in span of two months.
23 June 2006	FAS announced that Cadbury recalled 7 types of chocolate products -more than 1 million bars- due to possible contamination of "salmonella Montevideo"
04 July 2006	FSA revealed that extracted records of Cadbury's factories show that the same factory suffered outbreaks of the Salmonella Montevideo strain in April and November 2002. Also, the advisory committee reports that Cadbury's system for checking product safety is outdated and unreliable
21 July 2006	Health Protection Agency concludes Cadbury's chocolate to be the cause of a salmonella outbreak in more than 30 people and alerts the company after which Cadbury admitted to contamination
29 July 2006	Cadbury's sales have dropped down by 25% since the recall, by 14% in the last four weeks
01 August 2006	FSA was notified by Cadbury that it intends to restock 5types of chocolates that were recalled at first place, although the investigation was still in progress
03 August 2006	Cadbury apologises to consumers

BBC. (2007). UK | England | Cadbury fined £1 m over salmonella. BBC News. Retrieved December 5, 2022, from http://news.bbc.co.uk/2/hi/uk_news/england/6900467.stm

Boal, C. (2006). Cadbury contamination proves costly. confectionerynews.-com. Retrieved December 5, 2022, from https://www.confectionerynews.com/Article/2006/08/02/Cadbury-contamination-proves-costly

CampaignUK. (2013). Cadbury: Crisis, what crisis? Campaign UK. Retrieved December 5, 2022, from https://www.campaignlive.co.uk/article/cadbury-crisis-crisis/735985

Guardian News and Media. (2006, July 5). Salmonella outbreaks kept secret by Cadbury in 2002. The Guardian. Retrieved December 5, 2022, from https://www.theguardian.com/uk/2006/jul/05/foodanddrink

Guardian News and Media. (2007, February 13). Cadbury faces prosecution after contamination. The Guardian. Retrieved December 5, 2022, from https://www.theguardian.com/society/2007/feb/13/health.food

Horsemeat Scandal timeline

15 January 2013	Food Safety Authority (FSA) of Ireland publishes findings of a targeted study examining the authenticity, or labelling accuracy, of several burger products, which reveals horse and pig DNA, was found in frozen burgers sold in several British and Irish supermarkets.
16 January 2013	UK FSA announces urgent investigation- All of the retailers (i.e. Tesco, Lidl, Aldi, Iceland and Dunnes Stores) remove the offending products.
4 February 2013	Horse meat is found in North Ireland cold store
6 February 2013	FSA in collaboration with the industry published meat testing protocol published and surveyed food authenticity in processed meat products
7 February 2013	Findus announce the majority of its Beef Lasagne it had tested contained between 60% and 100% horsemeat, Findus withdrew the beef lasagne products after its French supplier, Comigel, raised concerns about the type of meat used in the lasagne.
8 February 2013	Aldi finds between 30% and 100% horsemeat in samples of beef lasagne and spaghetti Bolognese. FSA advice retailers/producers to withdraw beef products sourced from the French company Comigel
10 February 2013	The Agency issues interim advice to public institutions, such as schools and hospitals, caterers on procurement and reminds them to check meat supplies.
14 February 2013	The French Government announces a French company had its licence revoked A La Table de Spanghero licence after it was found knowingly selling horsemeat labelled as beef. They had sold to another French company, Comigel.
21 February 2013	Scotland reports a positive result for horse DNA in a frozen beef burger. Investigations ongoing to determine source of burger, thus Burger company withdraws products
8 March 2013	Update on progress of FSA beef product surveys. Sampling of the first and second phases of beef products completed, and initial results published. 212 of the 224 samples taken in phase one are negative horse DNA at or above the 1% threshold.
22 March 2013	Hungarian horse meat found labelled as 'diced beef'
16 April 2013	Results of Europe-wide beef product survey published. None of the UK's 150 samples are found to contain horse DNA at or above the 1% threshold for reporting
23 April 2013	Result from UK-wide beef survey confirmed that the remaining sample of beef products does not contain horse DNA at or above the 1% reporting threshold.
13 Jun 2013	More results of beef product testing published to show that three beef products contained horse DNA at or above the 1% threshold.
19 July 2013	Horse DNA detected in frozen meat pie from Latvia, thus has been withdrawn from sale.
31 October 2013	Horse DNA detected in canned beef from Romania, thus, has been withdrawn from sale.
14 April 2014	New European horse meat tests The FSA confirms details of a new round of tests of beef products for horse meat contamination and publishes sampling protocol
23 March 2015	The FSA welcomes the conclusion of the first prosecution brought as a result of the investigation into the horse meat incident in 2013

FSA (2015) Timeline on horsemeat issue, The National Archives, available at: https://webarchive.nationalarchives.gov.uk/20150403184406/http://www.food.gov.uk/enforcement/monitoring/horse-meat/timeline-horsemeat, accessed on 30 July 2020

Lawrence, F. (2013) Horsemeat scandal: timeline, The Guardian, Fri 10 May 2013, available at: https://www.theguardian.com/uk/2013/may/10/horse-meat-scandal-timeline-investigation, accessed on 30 July 2020