Managing cyber risk in supply chains: A review and research agenda

Abhijeet Ghadge[1], Maximillian Weiß[2], Nigel D. Caldwell[2] and Richard Wilding[1]*

[1]Centre for Logistics and Supply Chain Management, Cranfield School of Management, Cranfield University, UK

[2]Logistics Research Centre, School of Social Sciences, Heriot-Watt University, Edinburgh, UK

Purpose:

Despite growing research interest in cyber security, inter-firm based cyber risk studies are rare. Therefore, this study investigates cyber risk management in supply chain contexts.

Methodology:

Adapting a systematic literature review process, papers from interdisciplinary areas published between 1990 and 2017 were selected. Different typologies, developed for conducting descriptive and thematic analysis were established using data mining techniques to conduct a comprehensive, replicable and transparent review.

Findings:

The review identifies multiple future research directions for cyber security/resilience in supply chains. A conceptual model is developed, which indicates a strong link between IT, organisational and supply chain security systems. The human/behavioural elements within cyber security risk are found to be critical; however, behavioural risks have attracted less attention due to a perceived bias towards technical (data, application and network) risks. There is a need for raising risk awareness, standardised policies, collaborative strategies and empirical models for creating supply chain cyber-resilience.

Research implications:

Different type of cyber risks and their points of penetration, propagation levels, consequences and mitigation measures are identified. The conceptual model developed in this study drives an agenda for future research on supply chain cyber security/resilience.

Practical implications:

A multi-perspective, systematic study provides a holistic guide for practitioners in understanding cyber-physical systems. The cyber risk challenges and the mitigation strategies identified support supply chain managers in making informed decisions.

Originality: This is the first systematic literature review on managing cyber risks in supply chains. The review defines supply chain cyber risk and develops a conceptual model for supply chain cyber security systems and an agenda for future studies.

Keywords: Cyber risks, Cybersecurity, Cyber-attacks, Cyber resilience, Supply chain risk management, Supply chain resilience, Systematic literature review, Text mining

1 Introduction

Much work supports the view that the links of supply chains are increasingly global, and therefore, their integration is core to a successful supply chain (Mustafa Kamal and Irani, 2014). The dependencies inherent in integration have led to work on the risks of connectedness in supply chains (Kache and Seuring, 2014; Garvey et al., 2015). Supply chains mandate a holistic approach to risk management (Ghadge et al., 2012); heightened levels of cooperation and integration create their own risks (Yoon et al., 2017). This study takes as its starting point the risks inherent in literally networking (supply chain) actors together through Information Technology (IT) infrastructures (Warren and Hutchinson, 2000), as every node and connection between them poses a potential threat for the chain (The Institute of Risk Management, 2014). Supply chains that extensively utilise IT systems to satisfy customers' requirements have been termed '*cyber supply chains'* (CSC) (Boyson, 2014:346). The UK National Cyber Security Centre (NCSC), acts as a bridge between government and industry/society for advice, guidance and support on cyber security, including the management of cyber security threats within the UK. Similar National government cyber security organisations across the world attempt to protect their citizens and businesses from cyber threats and share vital information with their allies (e.g. EU, NATO) and other central bodies (e.g. Interpol) for global cyber security. The UK Office of Science and Technology produced a succinct definition of cyber security as *'defences against electronic attacks launched via computer systems*' (Houses of Parliament, 2011). First, though, a cautionary note has to be raised concerning the additional complication that in such an emergent area, technology changes and dates.

Descriptions such as ‘IT security event’, ‘cybercrime’ or ‘cyber-event’ all substantially refer to the concept of risk in the cyber context; yet, for example in their seminal paper, Faisal *et al.* (2007) refer to information risks as characterised by the presence of worms, viruses and Trojans.

A traditional or physical supply chain (SC) is dominated by the movement of products, finance and information (Peck, 2006); whereas a cyber supply chain is a network of IT infrastructure and technologies that are used to connect, build and share data in virtual networks (Smith et al., 2007) enabling new forms of risk un-connected to physical products or even a distinct physical location (e.g. WannaCry ransomware). Supply chains are the backbone of evolving technological ecosystems, *Industry 4.0* concepts such as the Internet of Things, Additive Manufacturing, Virtual Reality, Artificial Intelligence, Blockchain, both reflect, expand, alter and innovate the relationships between supply chain partners. However, developments in cyber security responses lag these advances in the digitalisation of supply chains. It has been argued that supply chains have unintentionally expanded their vulnerability by imprudently collaborating with many diverse partners (Boone, 2017). Smith et al. (2007) take the view that increasingly accessible IT systems have removed traditional, often bureaucratic, layers which used to function as protective barriers for organisations. In line with the growing capability of shared IT systems, modern cyber threats have also advanced dramatically, with increased consequences (Sokolov et al., 2014). A recent example of the developing capability of cyber threats was observed in the food industry, where complacency led to the belief that IT-related risks would only affect office based work (Khursheed et al., 2016). However, more elaborate malware goes beyond the boundaries of offices and can infect automated production systems and the wider supply chain network. Cyber supply chains do not necessarily make business simpler and safer; they add complexity and can become more challenging to manage (Kunnathur, 2015). Intriguingly, a difference between cyber and conventional risk has been identified as the anonymity of cyber risk, as it can remain undetectable until it impacts businesses (Renaud et al., 2018).

Organisations are increasingly becoming aware of cyber risks and their consequences and have increased cyber security response budgets (KPMG, 2017). Everyday media reports on cyber threats highlight the criticality of these risks for practice,

yet the topic has attracted minimal academic attention in spite of its significant implication for the global supply chains (Davis, 2015; Eling and Wirfs, 2019). According to a global risk survey conducted by various consultancy and insurance firms (e.g. Gartner, AXA, Society of actuaries, Deloitte) in 2018, cyber security and data breaches emerged as the top enterprise risk. Extant literature has failed to address the implications of cyber threats at the level of supply chains (Smith et al., 2007; Urciuoli et al., 2013; Xue et al., 2013). To the best of research team's knowledge, this study is the first to contribute a supply chain perspective on cyber risk/security/resilience in the form of a structured literature review (SLR). It is therefore crucial to identify, assess and mitigate cyber risks to reduce supply chain vulnerability. Following on from the above discussion, the study will address the following research question: ***How can organisations manage cyber risks in supply chains?*** Through addressing this question, this study will identify, classify, assess and mitigate cyber risks in supply chains.

The remainder of this paper is structured as follows. Section 2 explains the adopted research design and the use of a data mining approach for developing multiple typologies. Sections 3 and 4 discuss the findings from the descriptive and thematic analysis. Lastly, section 5 discusses key findings, the conceptual model and critical directions for further research along with implications for research and practice.

2 Research Design

A systematic literature review (SLR) is the universally preferred approach for executing an objective and extensive investigation of literature relevant to a specific research topic. The SLR follows a structured procedure that is scientific, replicable and transparent (Tranfield et al., 2003). Traditional literature reviews can be criticised for bias, as they steer the reader toward a specific direction based on the researchers' perception (Wilding and Wagner, 2012). In contrast to avoid claims of bias, this study presents a *'concept-centric'* approach (Webster and Watson, 2002) for conducting an SLR by adapting key elements from Tranfield et al. (2003), Rousseau et al. (2008) and Denyer and Tranfield (2009). The specific SLR process adopted here is divided into three stages, with each stage containing the set of activities shown in Figure 1.

2.1 Systematic literature review

2.1.1 Identification of data sources

This exploratory stage of identifying data sources maps a wide range of literature and helps in building an understanding of critical concepts and developing '*search strings'* (Ehrich et al., 2002; Arksey and O'Malley, 2005). The initial step is to identify key search terms derived from the research question. Since the study examines how an organisation can manage cyber risks in supply chains, i.e. the risk associated with combining supply chains and information technology, the choice of keywords was judiciously selected to include two connected fields namely supply chain risk management (SCRM) and information technology (IT). Boolean search was used since the search domain comprised of many interfaces. Different search string combinations were identified based on an initial understanding of the existing literature on cyber risk in supply chains. Appendix I provides an exhaustive list of the keywords selected by the research team. Following a mind mapping session, the most important search string combinations were finalised. Keywords such as '*cyber*', '*data*', '*information*' and '*technology*' were combined with risk, disruption, security, attack, along with other related words frequently used in the SCRM/Risk management literature.

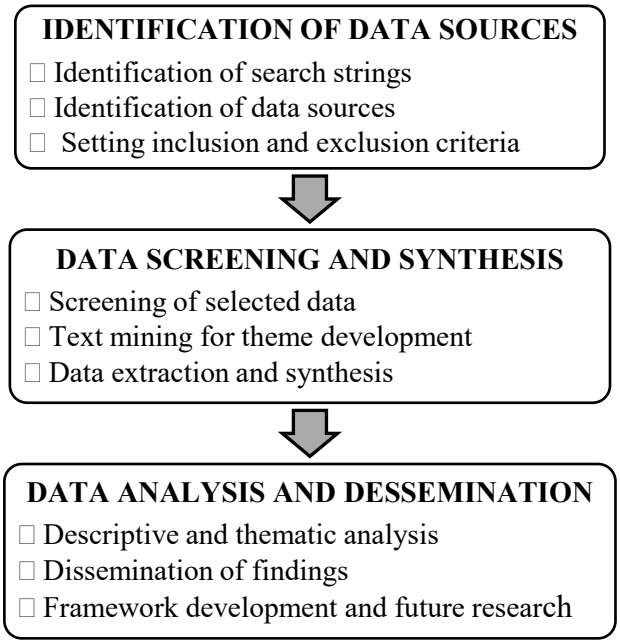

Figure 1. Systematic literature review process

(Adapted from Tranfield et al., 2003; Rousseau et al., 2008; Denyer and Tranfield, 2009)

Figure 2 shows the search string combinations used for the identification of data sources. To obtain a wide range of literature, two electronic databases- *Scopus* and *ProQuest* were searched using the search strings identified. Although broader selection criteria are recommended for an SLR, it is critical to define the boundaries and scope of the research. Including articles published in peer-reviewed journals positively influences the quality of the study (Burgess et al., 2006); hence, books, conference papers, editorials, HTML-links as well as both 'grey literature' and 'white literature' were excluded (Ghadge et al. 2019). Furthermore, only academic articles published in the last twenty years (1997-2017) were considered in order to capture more recent developments in the area.

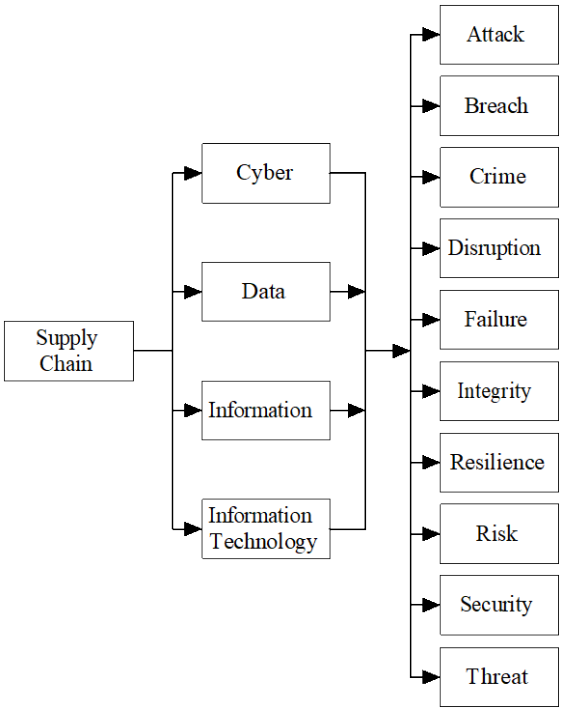

Figure 2. Search String combinations used for identification of data sources

2.1.2 Data screening and synthesis

Another essential stage of framing the SLR is to assess the quality of the papers identified. While there is no consensus across academic fields on one quality appraisal method for SLRs, in management studies, researchers frequently rely on the journal quality-rankings to determine article inclusion (Tranfield et al., 2003). The decision was taken that due to the comparative sparsity of extant literature in this area, instead of a particular journal

quality ranking guide (i.e. CABS, ABDC), article quality appraisal would be based on the judgment of the research team, with additional quality validation by an external third-party expert.

The initial search run on *ProQuest* produced 2,856 hits in the literature, while 6,637 potential papers were found via *Scopus*. Making use of these databases' built-in functions, inclusion and exclusion criteria (explained earlier) were applied to the articles leaving a total of 3,890 peer-reviewed papers, 2,149 from *ProQuest* and 1,741 from *Scopus*. After the removal of duplicates, a total of 1,434 papers meeting the selection criteria were taken into consideration.

The next necessary step was to identify papers closely related to cyber security/risk in supply chains. This was done by manually screening the titles and abstracts; two groups (from the research team) independently selected papers and compiled them together to identify common papers. Following this iterative step, further 1373 papers were excluded. Full-text reading of the 61 remaining papers led to further exclusion of 22 papers. Finally following a rigorous screening process to achieve a high-quality output, 39 papers were considered relevant. Besides, bibliography screening of the selected papers identified a further 3 related articles; giving a total of 41 articles to inform the analysis and were agreed with the external third-party expert.

2.1.3 Data analysis and dissemination

The data analysis stage aims to break the vast amounts of accumulated data into smaller, coherent parts and examine the extent to which they relate to each other (Denyer and Tranfield, 2009). *QDA Miner©*, a qualitative data analysis software developed by Provalis Research, was used as a text mining platform. Text mining was applied to cross-validate the search strings manually derived from the data identification process and to provide further support for the data analysis. Text mining identified the most important words or phrases by frequency (Figure 3); the manually selected key strings strongly match with those identified through the text mining. This cross-validation of the choice of search strings helps to limit research team bias and validate the reliability of the SLR process. Connectivity-based clustering or hierarchical clustering is an algorithm based on the core idea of filtering objects that are more related to nearby objects (than to objects farther

	FREQUENCY	% SHOWN	% PROCESSED	% TOTAL	NO. CASES	% CASES	TF · IDF
SECURITY	2485	7.5%	2.4%	1.2%	36	85.7%	166.4
INFORMATION	2195	6.6%	2.1%	1.1%	37	88.1%	120.8
CHAIN	2121	6.4%	2.0%	1.1%	38	90.5%	92.2
RISK	1160	3.5%	1.1%	0.6%	35	83.3%	91.9
MANAGEMENT	783	2.4%	0.8%	0.4%	35	83.3%	62.0
SYSTEMS	682	2.1%	0.7%	0.3%	37	88.1%	37.5
CYBER	660	2.0%	0.6%	0.3%	23	54.8%	172.6
DATA	647	2.0%	0.6%	0.3%	33	78.6%	67.8
LEVEL	394	1.2%	0.4%	0.2%	33	78.6%	41.3
ORGANIZATION	374	1.1%	0.4%	0.2%	26	61.9%	77.9
MODEL	360	1.1%	0.3%	0.2%	24	57.1%	87.5
NETWORK	349	1.1%	0.3%	0.2%	32	76.2%	41.2
SERVICES	302	0.9%	0.3%	0.2%	30	71.4%	44.1
THREATS	282	0.9%	0.3%	0.1%	25	59.5%	63.5
SHARING	281	0.8%	0.3%	0.1%	22	52.4%	78.9
SOFTWARE	272	0.8%	0.3%	0.1%	30	71.4%	39.7
ORGANIZATIONAL	250	0.8%	0.2%	0.1%	20	47.6%	80.6
IMPACT	247	0.7%	0.2%	0.1%	29	69.0%	39.7
COST	244	0.7%	0.2%	0.1%	30	71.4%	35.7
QUALITY	244	0.7%	0.2%	0.1%	23	54.8%	63.8
INTEGRATION	234	0.7%	0.2%	0.1%	21	50.0%	70.4
PERFORMANCE	209	0.6%	0.2%	0.1%	28	66.7%	36.8
ANALYSIS	203	0.6%	0.2%	0.1%	29	69.0%	32.7
ATTACKS	201	0.6%	0.2%	0.1%	29	69.0%	32.3

	FREQUENCY	NO. CASES	% CASES	LENGTH	TF · IDF
INFORMATION SECURITY	565	27	64.3%	2	108.4
RISK MANAGEMENT	170	23	54.8%	2	44.5
CYBER SUPPLY CHAIN	162	10	23.8%	3	101.0
INFORMATION SHARING	162	18	42.9%	2	59.6
CYBER SECURITY	138	15	35.7%	2	61.7
CHAIN MANAGEMENT	120	23	54.8%	2	31.4
DIGITAL SUPPLY CHAIN	101	1	2.4%	3	163.9
INFORMATION SYSTEMS	95	22	52.4%	2	26.7
CYBER RESILIENCE	86	4	9.5%	2	87.8
NETWORK VULNERABILITY	82	3	7.1%	2	94.0
SECURITY MANAGEMENT	82	14	33.3%	2	39.1
INFORMATION TECHNOLOGY	77	22	52.4%	2	21.6
INTER ORGANIZATIONAL	73	5	11.9%	2	67.5
SECURITY RISK	70	15	35.7%	2	31.3
INFORMATION RISK	64	5	11.9%	2	59.2
PERCEIVED RISK	63	2	4.8%	2	83.3
INFORMATION LEAKAGE	62	5	11.9%	2	57.3
SC DIGITIZATION	62	1	2.4%	2	100.6
DECISION MAKING	60	14	33.3%	2	28.6
DIGITAL SUPPLY CHAIN SYSTEMS	60	1	2.4%	4	97.4
RISK FACTORS	56	5	11.9%	2	51.8
SECURITY ISSUES	56	17	40.5%	2	22.0
SECURITY PRACTICES	51	10	23.8%	2	31.8

Figure 3: Key terms and phrases identified following data mining

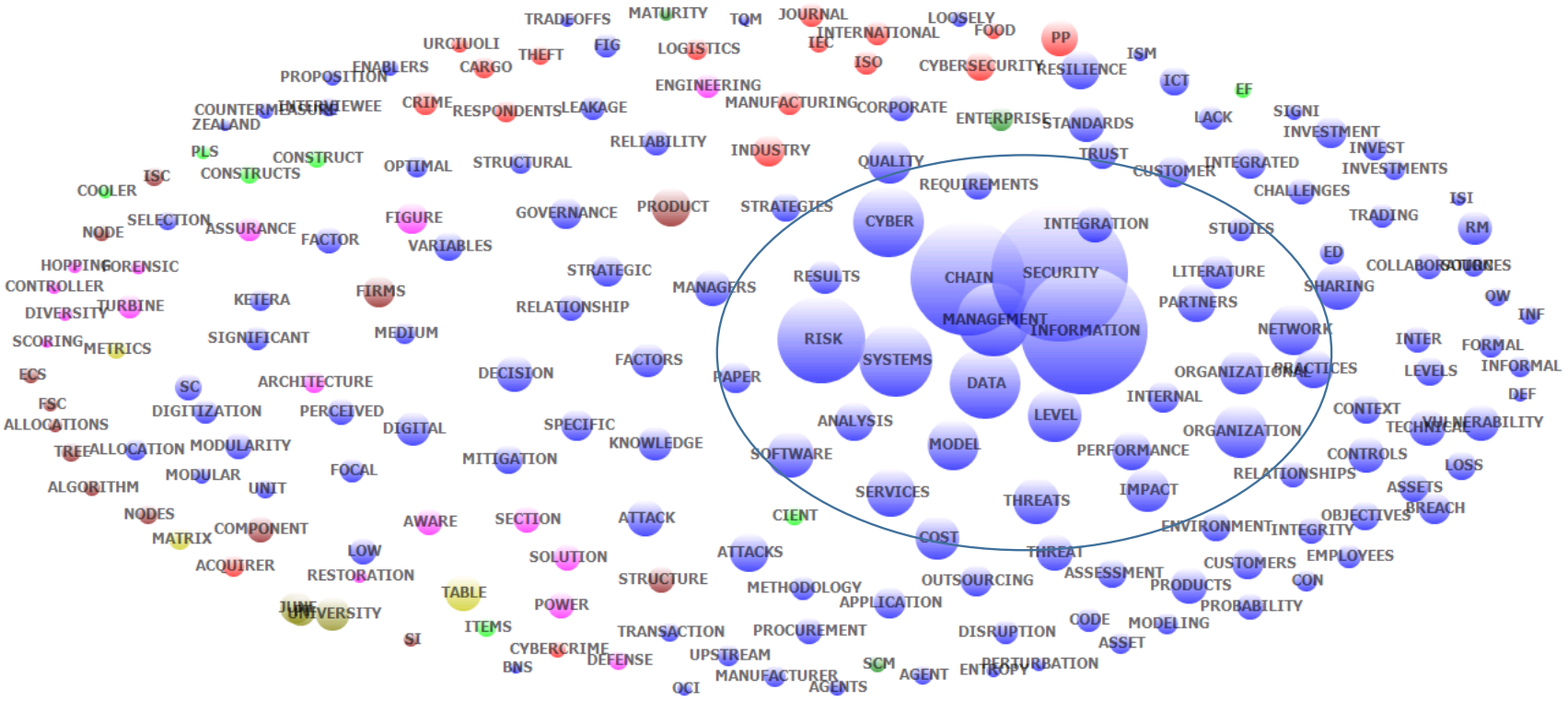

Figure 4. Exploded view of cluster diagram for cyber risk in supply chains (specimen)

Table I. Descriptive analysis

Reference	**Research Methodology**				**Research Design**			
Author et al. (year)	*Quant.*	*Quali.*	*Mixed*	*Review*	*Survey/ interview*	*Experiment /model*	*Case study*	*Concept.*
Al Kattan et al. (2009)			✓			✓	✓	
Bahl and Wali (2014)			✓		✓			
Bandyopadhyay et al. (2010)	✓							
Barlow and Li (2007)		✓			✓		✓	
Bartol (2014)		✓						✓
Boone (2017)		✓						✓
Boyes (2015)		✓						✓
Boyson (2014)		✓						✓
Cai and Jun (2008)		✓			✓			
Charitoudi et al. (2014)		✓					✓	✓
Davis (2015)		✓						✓
Deane et al. (2009)	✓					✓		
Durowoju (2012)	✓					✓		
Faisal et al. (2007)	✓					✓		
Hamlen et al. (2013)		✓						✓

Huang et al. (2008)	✓						✓
Jones and Horowitz (2012)		✓					
Keegan (2014)	✓						✓
Khursheed et al. (2016)	✓						✓
Kim and Im (2014)	✓						✓
Linton et al. (2014)	✓			✓			
Manzouri et al. (2013)	✓			✓			
Pfleeger et al. (2007)	✓			✓			
Rongping and Yonggang (2014)	✓						✓
Sharma and Routroy (2016)		✓	✓		✓		
Sindhuja (2015)	✓		✓				
Kunnathur (2014)	✓			✓			✓
Sokolov et al. (2014)	✓						✓
Stephens and Valverde (2013)	✓					✓	
Tran et al. (2016)	✓			✓		✓	
Urciuoli (2015)	✓						✓
Urciuoli and Hintsa (2017)	✓			✓			
Urciuoli et al. (2013)	✓		✓				
Venter (2014)	✓						✓
Warren and Hutchinson (2000)	✓						✓
Williams (2014)	✓						✓

Windelberg (2013)			✓
Xue et al. (2013)		✓	
Zhang et al. (2012)	✓		
Smith et al. (2006)			✓
Linkov (2013)			✓

Table II. Definitions from the literature: Cyber supply chain

Perspective	Definitions	Reference
Supply Chain	*"E-supply chains involve organisations using online information, to perform, rather than just support, some value-adding activities in the supply chain more efficiently and effectively."*	(Barlow and Li, 2007, p. 289)
	"[Cyber supply chain is] the entire set of key actors and their organisational and process-level interactions that plan, build, manage, maintain, and defend the IT system infrastructure."	(Boyson et al., 2010, p. 200)
	"IT system supply chain is a globally distributed and dynamic collection of people, process, and technology."	(Simpson, 2010, p. 3)
	"A cyber supply chain is a supply chain enhanced by cyber-based technologies to establish an effective value chain."	(Kim and Im, 2014, p. 387)
	"The probability of loss arising because of incorrect, incomplete, or illegal access to information."	(Faisal et al., 2007, p. 679)

Supply Chain Risk	*"[…] degradation or disruption to a supply chain's infrastructure or structural resources resulting from the successful exploitation of IT vulnerabilities by threats within an organisation, within the supply chain network, or in the external environment."*	(Smith et al., 2007)
	"IT security incidents occur when a threat directed against an organisational asset causes a compromise in one (or more) of three areas: confidentiality, integrity or availability (CIA)."	(Deane et al., 2009, p. 5)
	Operational risks to information and technology assets that have consequences affecting the confidentiality, availability or integrity of information systems."	(Cebula and Young, 2010)
	"Cybercrime can be defined as any crime that is facilitated or committed using a computer, network, or hardware device; in particular, the computer or the device may be the agent, facilitator, or target of the crime that takes place in virtual or non-virtual places."	(Urciuoli et al., 2013, p. 51)
	"A cyber-event is any disturbance to this interdependent network that leads to loss of functionality, connectivity, performance, or capacity."	(Boyes, 2015, p. 29)
Supply Chain Risk Management	*"CSCRM (cyber supply chain risk management) can be defined as the organisational strategy and programmatic activities to assess and mitigate risks across the end-to-end processes (including design, development, production, integration, and deployment) that constitute the supply chains for IT networks, hardware, and software systems."*	(Boyson, 2014, p. 342)
	"[…] the application of policies, procedures, and controls (technical, formal, informal and management) to protect supply chain information assets (product, facilities, equipment, information, and personnel) from theft, loss, damage, interceptions or unauthorized access, use, disclosure, interruptions or disruption, modification or fabrication."	(Sindhuja and Kunnathur, 2015, p. 483)

away), to build a hierarchical network (Tan et al., 2017). Cluster analysis was conducted to identify a group of entities based on their similarities and differences in the subject area. An exploded view of the identified clusters is provided as an example in Figure 4. It can be observed that sub-areas having a close affinity to each other come together (circled in Figure 4 for clarity) following a hierarchical clustering approach. After studying all the clusters for patterns and dendrograms for the taxonomic relationships (example shown in Figure 5), different themes were identified for the data analysis. Furthermore, sub-categories for themes emerged during the iterative process of data screening, and synthesis and these were utilised for developing a 'theme-based' typology. A comprehensive list of meta themes and associated sub-categories identified are shown in Figure 6.

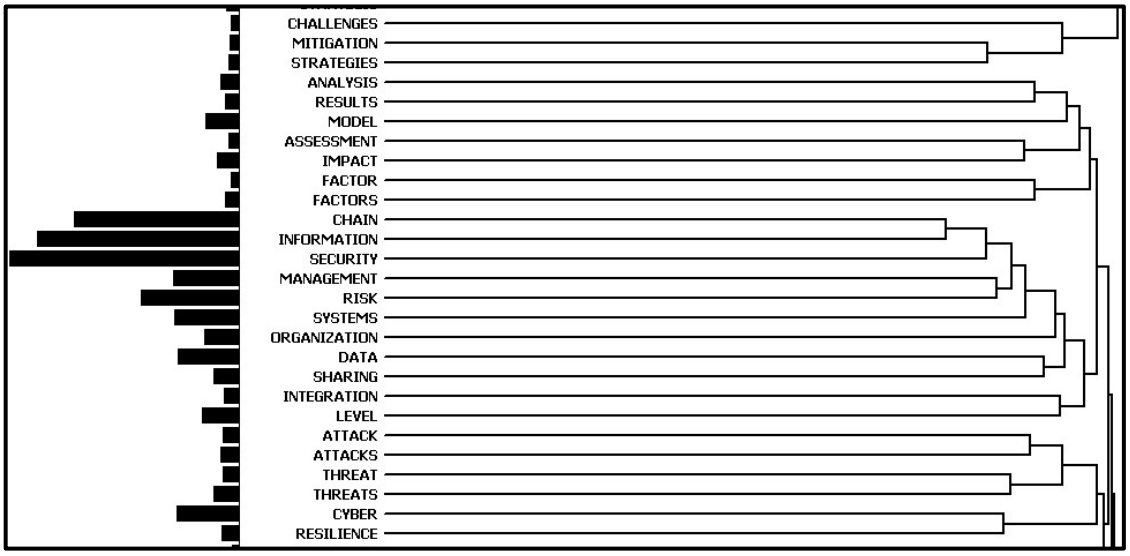

Figure 5. Dendrogram used for developing typologies (specimen)

The two-fold reporting approach recommended by Tranfield et al. (2003) is adopted in this paper. Descriptive analysis will report an overview of the field of study. Furthermore, a thematic analysis will report the findings in detail and help in drawing conclusions and future research avenues.

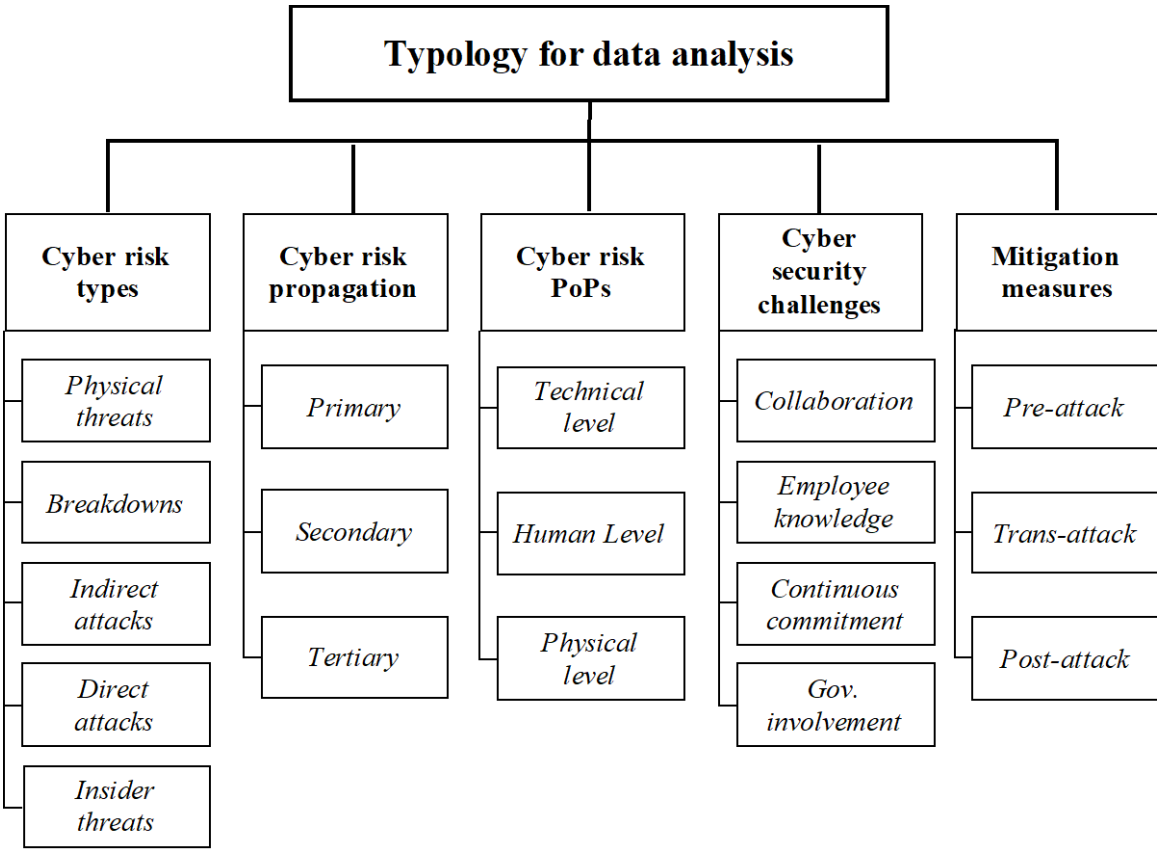

Figure 6. Typologies: 'theme-based' framework for analysis

3. Descriptive analysis

Table I presents an overview of the SLR content in terms of the research methodology and different types of research design adopted for data collection and analysis.

3.1 Definitions

In the evolving definition of what constitutes a cyber supply chain (Table II), we see broadening of scope over time, from the earliest definition linking online activities undertaken by firms or chain (Barlow and Li, 2007; Sindhuja and Kunnathur, 2015). What is notable is the consistent use of terms relating to the value creation. Kim and Im (2014) believe that cyber supply is '*an effective value chain'*. In terms of supply chain risk, the same broadening of the scope is seen over time, but early work is heavily focused on technology and exogenous threats. Later definitions include awareness of endogenous

threats "*...theft, loss, damage, interceptions or unauthorized access, use, disclosure, interruptions or disruption, modification or fabrication"* (ibid.). In Table II, we see cohesion on definitions of SCRM as it being the application of various tools and a guiding process for endogenous and exogenous risks. Therefore, the study takes forward from these definitions that supply chain cyber security systems are an integrated alignment of processes involving infrastructure network, IT system and organization.

3.2 Research distribution

The work by Warren and Hutchinson (2000) can be seen as a milestone for the field and a key paper for this study; they report a survey that found approximately 60% of IT managers had no awareness of, or policy on cyber security. Ironically, attacks in 2005 and 2006 on Homeland Security, the department tasked with keeping the USA secure, seem to have piqued academic interest in the latter half of this period. Looking at the trend in the publications between 1997 and 2017, the first article that relates to cyber supply chains was only published in 2000; since then, academic research on cyber security has grown, particularly in the IT and computer engineering fields.

3.3 Geographic distribution

Approximately half of the selected papers originate from researchers based in either the USA or UK (Figure 7); Government institutions from both countries have raised the profile of cyber security through different initiatives aimed at promoting its importance among both practitioners and academics (see Luiijf et al., 2013). Keegan (2014) and Rongping and Yonggang (2014) claim that inducements and support from governmental bodies will be crucial for the progression of research in this field. Surprisingly, while countries like the USA or UK developed their first national cyber security strategies long before 2010, European countries such as Germany, France or the Czech Republic did not present theirs until 2011. India has emerged as one of the leading low-cost destinations for outsourcing IT operations (Bahl et al., 2011); Luiijf et al. (2013) supports the strength and economic ambition of India with regard to ICT systems and argue that Indian firms see cyber security as an opportunity for further economic growth.

Figure 7. Geographic distribution of research

3.4 Methodological distribution

The research methodologies can be separated into qualitative, quantitative and mixed approaches. Most of the research methods in this field are qualitative, whereas only a limited number of quantitative research designs have been identified. These findings support the initial claims made about the progression stage of the literature on the topic and are consistent with Creswell (2014) positing that prevalence of qualitative works in an academic field is an indicator of the immaturity of the field and the lack of consensus on key concepts. Maturity and relatively stable constructs are associated with more quantitative research designs (ibid.); by implication, research on the topic of cyber security in SCs is still at a nascent stage. In part this unequal split reflects the multidisciplinary nature of the research topic. Research in IT-related fields is usually dominated by quantitative approaches, while qualitative modes are more prominent in the area of SCM (Ho et al., 2015). Qualitative and quantitative methodologies are not substitutes for each other as they approach different aspects of the same reality (McCracken, 1988), but are simultaneously necessary to understand complexities in the research thoroughly. Only 12% of the sample for this SLR is purely quantitative; Charitoudi and Blyth (2014) propose that the lack of accessible quantitative cyber data critically limits researchers' ability to model

supply chain cyber risks.

4 Thematic analysis

The thematic analysis combines the careful reading of the selected papers, as a part of the data screening and synthesis stage with categories confirmed following the text mining approach.

4.1 Type of cyber risks

Extant literature has a variety of theoretical frameworks for the classification of different supply chain risks (e.g., Jüttner et al., 2003; Manuj and Mentzer, 2008; Ho et al., 2015). In an attempt to make sense of these new and unexplored risks, Gordon and Ford (2006) and Urciuoli *et al.* (2013) posit Type I and Type II cyber risks. Type I cyber risks include incidents of phishing and theft or manipulation of data or services, Type II covers cyberstalking and harassment, stock market manipulation or blackmailing and corporate espionage. However, this classification of cyber risks only focusses on deliberate acts carried out by malicious actors. Other classifications of cyber risks, such as those provided by Smith et al. (2007) or Tran et al. (2016), either miss out on principal (focal firm) risks or become very engaged with other, mostly technical risks. Simialry, NCSC, UK (2016) classify cyber attacks into un-targetted and targetted attacks. Phishing, ransomware and scanning are covered under un-targeted attacks, as they target multiple devices or users. Spear-phishing, denial of service and subverting supply chains are captured under targetted attacks. This classification does not consider attacks arising from physical breakdown and internal activities. Based on the data synthesis of selected papers, a holistic classification of cyber risks is developed as shown in Figure 8. Each of the identified ‘cyber risks’ are explained below.

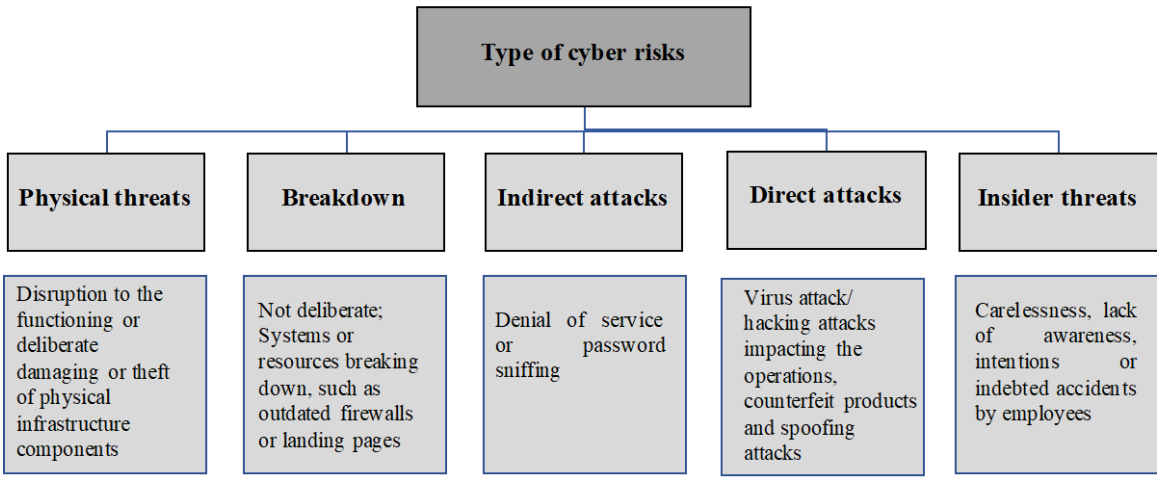

Figure 8. Classification of cyber risks

4.1.1 Physical threats

The physical dimension includes tangibles such as switches, servers, routers and other ICT devices. According to Boyes (2015), the presence of physical and environmental risks seems to be ignored by many risk managers, when talking about cyber risks. In this study, a few articles (e.g. Faisal et al., 2007; Smith et al., 2007; Charitoudi and Blyth, 2014; Tran et al., 2016; Urciuoli and Hintsa, 2017) acknowledge natural disasters as a critical driver for cyber risks. For example, when a flood or a tornado disrupts the functioning of servers, which then interferes with the seamless flow of the cyber supply chain network. Meanwhile, Smith *et al.* (2007) and Urciuoli and Hintsa (2017) go one step further and add the deliberate damaging or theft of physical infrastructure components to this physical risk category. Faisal et al. (2007) also consider terrorist attacks to be a part of the physical aspect of cyber risks. Risks that affect the functioning and security of a supply chain's physical assets are, paradoxically, cyber risks.

4.1.2 Breakdown

The, perhaps, humdrum risk of systems or resources breaking down through causes such as outdated firewalls and overdue security updates have only attracted attention in two articles (Boyes, 2015; Tran et al., 2016). While the least exotic cyber risk (e.g., website failure due to a peak in data traffic), cannot be ignored, such failures are easier to predict than natural disasters or intentional attacks; however, their potential consequences can be equally severe.

4.1.3 Indirect and direct attacks

The cyber risk of deliberate assaults falls into two categories - direct attacks and indirect attacks. The first category comprises acts such as hacking attacks (Deane et al., 2009; Khursheed et al., 2016; Sharma and Routroy, 2016; Boone, 2017), denial-of-service (Faisal et al., 2007; Deane et al., 2010) or password sniffing (Warren and Hutchinson, 2000) for financial gains. Several authors, for example, Faisal et al. (2007) and Tran et al. (2016), include the risks of industrial espionage or compromises to intellectual property, under direct attack.

In the Indirect attacks the attackers lay out *'bait'* which enables them to access the target system. Commonly discussed methods in the literature include viruses, worms and Trojans (Warren and Hutchinson, 2000; Faisal et al., 2007; Smith et al., 2007; Jones and Horowitz, 2012), counterfeit products, soft- and hardware (Urciuoli et al., 2013; Linton et al., 2014; Williams, 2014; Boyes, 2015), malicious codes (Smith et al., 2007; Deane et al., 2010; Kunnathur, 2015) and spoofing attacks (Warren and Hutchinson, 2000; Smith et al., 2007). If employees accept the bait by, for example, visiting a website or downloading software, the attacker gains access to the system. Cyber-attacks that originate via phishing, i.e. gaining access to sensitive information by disguising the threat as a trustworthy entity, are on the rise (Verizon, 2018), and heightened cyber awareness is necessary to tackle such disguised attacks.

4.1.4 Insider threat

According to Kunnathur (2015), employees often represent the most significant risk to a company's cyber security. Internally, employees were found to be careless with password confidentiality (Stephens and Valverde, 2013), including writing passwords down for easy recall (Venter, 2014). Furthermore, absent-mindedly disclosing sensitive information while discussing with colleagues or others is identified as a risk that companies need to be aware of (Kunnathur, 2015). In connection with these acts of thoughtlessness, the literature also reports incidents in which employees consciously misuse or even sabotage a company's information. For example, opportunistic misuse of confidential data (Deane *et al.*, 2009) or a premeditated personal vendetta against an employer (Sharma and Routroy, 2016). As the employee cyber threat is internal, whether deliberate or accidental, this is termed an insider threat.

Reporting on deliberately executed, maliciously motivated cyber-attacks (Urciuoli, 2010) should not be allowed to crowd out cyber supply risks resulting from merely careless employees (Urciuoli et al., 2013; Urciuoli et al., 2017). In both the negligent and premeditated mode, the human factor can pose the biggest and most unpredictable threat to a company's cyber security. Employees could act as insiders and support criminals in perpetuating their actions, or they could perpetrate a crime on their own, as they may have easy access to facilities or cargo (Urciuoli, 2010).

4.2 Points of penetration

To allocate security resources, organisations need to know the weak points of the supply chain network where these risks are most likely to penetrate (Smith et al., 2007); referred to as 'points of penetration' (PoP). Urciuoli et al. (2013) reported that 50% of malicious cyber-attacks target smaller organisations due to the lack of adequate protection measures installed in their information systems. SMEs might have a lower security capability, but their attack surface and visibility are also dramatically smaller (Caldwell, 2015). Data synthesis identifies three key 'failure points' where cyber risks emerge. PoPs are classified into technical, human and physical dimensions.

4.2.1 Technical PoPs

Smith et al. (2007) define the weakest link of a SC quite broadly by claiming all IT-related assets are prone to cyber risks including systems, software, personnel and equipment. ICT systems and related resources may improve performance while also increasing technology risk (Xue et al., 2013). In particular, legacy (inherited) or outdated and poorly maintained systems attract wilful attacks. Outsourcing servers to save up-front capital costs reduces overall direct costs (Boyson, 2014), but the loss of control over security may increase long-term indirect costs dramatically.

4.2.2 Human PoPs

Most companies, as claimed by Sindhuja (2014), complacently assume that cyber security is only about technical security. In reality, technical cyber security solutions will have been grounded in security analysis; the same is often not the case with human involvement, individuals, who theoretically should be the first layer of protection. Boone (2017) argues that companies are only as secure as the most susceptible stakeholder in their supply

networks. Urciuoli and Hintsa (2017) suggest that human resources could either willingly choose to harm their own company, or pose a threat by accident or be forced to collaborate with criminals by means of viruses, blackmailing, etc. Kim and Im (2014) found that internal human errors are likely to have severe consequences, but also more challenging to identify than external events. Kunnathur (2015) builds on the importance of human PoPs, arguing that potential cyber aggressors are well aware of this vulnerability. Consequently, they suggest *(ibid.)* that future cyber risks, and especially intended attacks, are expected to exploit human PoPs rather than, hitherto, focus on the technical domain. This vulnerability is then intensified when SC employees interact with each other across organisational boundaries. Ill-secured inter-organisational supply chain connections between companies are a PoP for cyber risks, which may work as facilitators for the propagation of these risks.

4.2.3 Physical PoPs

Charitoudi and Blyth (2014) state that physical objects such as buildings, machines and other surroundings can also represent a PoP for cyber risks. In a recent study on cyber security in the food industry, Khursheed et al. (2016) report incidents in which obsolete firewalls and inadequate control mechanisms allowed attackers to gain remote access to production lines. In addition, physical infrastructures are always vulnerable to tangible risks such as natural disaster or physical attacks that impact cyber systems. However, as such disasters are naturally rare and unavoidable (Smith et al., 2007), companies like to perceive them as less of a concern for cyber safety (Sharma and Routroy, 2016).

4.3. Propagation zones

The consequences of cyber risks can be short to long term. While damage to servers will have noticeable effects immediately following their occurrence, others, for example, information leakage, can take years to recognise (Boone, 2017) or will never be disclosed. Data theft is central to cybercrime (Urciuoli and Hintsa, 2017) which, to date, seems to have exempted communities from direct cyber-attack. The risk propagation model proposed here, suggests supply chain risks are not static and, propagate out from the centre of risk occurrence to other related areas with the *'cascading or ripple effect'* (Ghadge et al., 2013; Dolgui et al., 2018). Therefore, it is likely that cyber risks will typically follow similar risk propagation patterns, as shown in Figure 9.

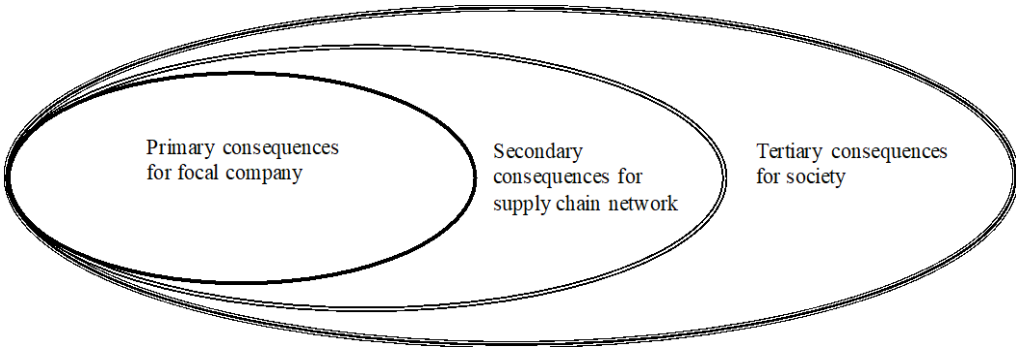

Figure 9. Propagation zones of cyber risk

4.3.1 Primary propagation

As indicated by the PoP discussion, regardless of where a risk finds its way into a system, there is always a disruption to the company's operations. Risk propagation compromises the operation's continuity (Warren and Hutchinson, 2000; Boyson, 2014), productivity (Manzouri et al., 2013) and quality (Jones and Horowitz, 2012). Cyber-attacks in Germany (Boyes, 2015) and Iran (Jones and Horowitz, 2012), report that blast furnaces and centrifuges, respectively, were damaged, threatening not just individual operations but the entire factory/output. A lone report on the consequences for employees (Manzouri et al., 2013) claims aggressor breaches of security systems discourage employees, particularly their willingness to continue working under such circumstances (echoing Reade's (2009) non cyber finding in terror act environments). Except for the above, there appears to be limited discussion on primary consequences from cyber-attacks, and there is a lack of studies focussing on the consequences for employees and organisational sustainability of such attacks, whether successful or not. This theme has exposed a strong tendency to a binary approach based on the success or failure of an attack/cyber risk episode; thus, more studies are needed on the impacts and how processes and people respond to the cyber-attacks.

4.3.2 Secondary propagation

Supply chain relationships facilitate information sharing, including detrimental information like cyber breaches. Several authors claim that reputational damage resulting from a cyber-attack discourages further collaboration with existing and prospective SC

partners (Urciuoli et al., 2013; Charitoudi and Blyth, 2014). Post-supply-chain cyber-attack, authors highlight the potential unavailability of information, services or products for further use (e.g., Warren and Hutchinson, 2000; Charitoudi and Blyth, 2014). Inter-connected systems and machinery will be affected, leading to unsatisfied customer requirements and loss of sales and profit. Losses will include near-time opportunity costs, but also potential longer-term reputational damage. Breaches of confidential information (such as supplier databases, contracts and payment details) could have major implications for the supply chain network. In spite of increased security in data storage platforms, data breaches are a regular occurrence; thus, there is a need for robust cyber security measures to protect cyber-physical systems.

4.3.3 Tertiary propagation

A study in the automotive industry found that hostile malware can corrupt the braking system of a car in a way that could not be detected by the manufacturer (Jones and Horowitz, 2012). Thus, individuals in the wider society face the initial brunt of this supply chain cyber-attack. According to Urciuoli and Hintsa (2013), the consequences of SC cyber-attacks for a community or society could be more serious, if criminals attack supply chains relevant to public health, e.g., food or pharmaceutical chains.

There is also a dynamic behaviour to cyber-attack consequences; as defences improve, the attacks move elsewhere. In two articles, Urciuoli and Hintsa (2013; 2017) explain that criminals can for now steal valuable cyber data – such as loading lists and transportation schedules - to plan and execute traditional non-cyber [theft] crimes; with relative impunity. It is evident that cyber risks directly impact organisations profit margins, market capitalisation and brand image (Mukhopadhyay et al., 2013), along with indirectly impacting wider businesses and society.

4.4 Challenges for cyber security

4.4.1 Inter-organizational collaboration

In traditional supply chains, two parties might share some information and very occasionally, the same IT platform. The risk is amplified when cyber supply chains and order management systems link multiple supply parties together or share the data in outsourced (e.g. Cloud) platforms. A lack of accepted standards and guidelines is hindering

the development of robust cyber defences (Boyson, 2014; Davis, 2015). Authors argue that supply chain partners must be more transparent with each other on security and should combine security resources and know-how to deal with increasingly sophisticated cyber risks (Rongping and Yonggang, 2014). The propagation of cyber consequences means companies cannot afford to focus only on their security systems and must also be aware of their partner's security conditions (Deane et al., 2010). Supply chain collaboration based on open, honest and trust-based relationships is needed to effectively deal with supply chain cyber-related risks (Tran et al. 2016). Smith et al. (2007) recommend that SC integration, by aligning systems and processes, will yield better returns through standardised ways of working, shared security objectives and better general communication (see conceptual model, Figure 10). Bandyopadhyay et al. (2010) argue that higher levels of integration and collaboration reduce free-riding behaviour when considering investment in cyber security.

4.4.2 Employee knowledge

One of the stand-out findings from this SLR is the important role played by employees as the front-line of cyber security in SCs. Although the most visible layer of security to outsiders, it is challenging to hire cyber–security-trained and skilled resources given the complex, emergent and technological demands of SC security (Xue et al., 2013; Venter, 2014; Khursheed et al., 2016). So far, cyber threats have outpaced training and study initiatives. Ideally, such staff members are proactive employees in contact with cyber applications who need to know not only how to operate the systems, but also how to react in cases of attack. Khursheed et al. (2016) describe the ideal situation in which highly skilled employees are not only cyber risk reactive, but also have the skill-set to pre-empt cyber PoP risks.

4.4.3 Continuous commitment

The eco-systems in which cyber SCs operate are constantly evolving (Kim and Im, 2014); compounded by different geopolitical situations, regulatory frameworks as well as corporate and national cultures that merge in one supply chain. Cyber risk management is not only about protecting data, but also maintaining the privacy, trust and safety of stakeholders involved in the business network. Hackers and other potential invaders, on the other hand, have no such encumbrances and with the advantage of agility can invest in being ahead of the curve thriving on awareness of cyber trends and new technologies

(Boyes, 2015), in order to create novel and ever more sophisticated and unpredictable cyber-crimes.

These two issues of timeframe and level of focus are built upon based on a theme found in the cyber supply chain literature, the disconnection between standard business practices and the requirement for a continuous commitment to cyber security. According to Linkov et al. (2013), many of the risks that have struck companies only manifest after months or even years; however, these manifestations exceed the attention (and job) span of most managers who are driven by short and medium-dated performance objectives (Urciuoli and Hintsa, 2017). Boone (2017) goes beyond timing and performance to argue that it is not merely a commitment to cyber security issues which is missing, but also responsibility and ownership. The introduction and maintenance of appropriate cyber security systems cannot be a one-person show; they require the contribution and commitment, over time, of many departments and much expertise.

4.4.4 Governmental involvement

Traditionally, governments have focused their interest on the security of military and national intelligence agencies (Keegan, 2014); however, they now have to include the security of supply chains that are significant contributors to their economies. More than 50 countries have issued national cyber security strategies with defined objectives (Rongping and Yonggang, 2014). The European Union regularly updates its *EU Cybersecurity Strategy*. The growing complexity of cyber SCs makes it impossible for individual companies acting alone to promote and coordinate holistic security efforts. Hence, Keegan (2014) claims governments have to sponsor and guide cyber security projects and create forums which allow for more accessible communication and planning of strategies to manage cyber risks.

4.5 Measures for mitigation

This section has identified measures to mitigate cyber risks from the extant literature. The risk mitigation typically depends on the type of cyber-attack, sophistication of the attack and resilience of the organisation (Amin et al., 2017). While some of the proposed countermeasures may look familiar from the traditional SCRM studies (e.g., supplier audits and information sharing), others focus on cyberspace more explicitly and are, therefore,

new to the literature. Building on the scope of cyber risks identified here, the study rejects using a conventional proactive and reactive risk mitigation classification and instead proposes a time phases classification of cyber-attack mitigation measures.

In their efforts to model a system-aware cyber security architecture, Jones and Horowitz (2012) differentiate between three phases of a cyber-attack, namely pre-, trans- and post-attack. This time phase structure is adopted in this study to use a wider analytical lens on the stages of, and countermeasures for a cyber-attack. Table III classifies cyber risk measures for mitigation following pre, trans and post cyber-attack stages. Pre-attack countermeasures can be divided between those aimed at the technical level and those which are either directed at or carried out by human factors. Firstly, technical countermeasures include aspects such as firewalls and passwords (access control) or the diversification of soft- and hardware and are frequently discussed in the literature as they form the most fundamental layer of protection. They specify the level of system accessibility (Kunnathur, 2015) and are designed to make aggression less attractive to attackers (Al Kattan et al., 2009). However, many authors argue that such technical countermeasures only provide a partial solution and, therefore, need to be complemented by actions that are directed at the backbone of every supply chain, i.e., the personnel (e.g., Smith et al., 2007; Boyson, 2014; Boyes, 2015).

The implementation of automated IT operations has allowed companies to employ fewer staff (Urciuoli et al., 2013). In addition, some argue that, the few remaining IT staff are then over challenged as employees and have little time for security awareness (Sindhuja, 2014; Venter, 2014; Kunnathur, 2015), holistic understanding of systems (Faisal et al., 2007; Urciuoli and Hintsa, 2017) and commitment (Tran et al., 2016; Boone, 2017). To nurture the capabilities of their employees and prepare them for the new challenges of cyber chains, risk awareness initiatives and training are among the most cited countermeasures in the literature (Table III).

Table III. Measures for mitigating cyber risk

Pre-attack phase

Access control	Warren and Hutchinson (2000); Deane *et al.* (2009); Sindhuja and Kunnathur (2015)
Accreditation against security standards	Warren and Hutchinson (2000); Stephens and Valverde (2013); Bahl and Wali (2014); Keegan (2014) Venter (2014); Davis (2015); Sindhuja and Kunnathur (2015)
Certified hard- and software	Boyson (2014); Kim and Im (2014); Sokolov *et al*. (2014); Windelberg (2016)
Cross-functional communication	Boyson (2014); Sindhuja and Kunnathur (2015)
Formal agreements between SC partners	Cai and Jun (2008); Boyson (2014); Sindhuja and Kunnathur (2015); Tran *et al.* (2016)
Information sharing	Barlow and Li (2007); Boyson (2014); Linton *et al.* (2014); Urciouli (2015)
Internalisation of operations	Boone (2017)
More sophisticated and diverse applications	Jones and Horowitz (2012); Tran *et al.* (2016)
Network audit	Deane *et al.* (2009); Stephens and Valverde (2013); Davis (2015); Windelberg (2016)
Risk awareness initiatives	Warren and Hutchinson (2000); Deane *et al.* (2009); Stephens and Valverde (2013); Boyson (2014); Davis (2015); Sindhuja and Kunnathur (2015)
Risk classification	Faisal *et al.* (2007); Stephens and Valverde (2013); Boyson (2014); Davis (2015); Windelberg (2016)
Risk identification software	Zhang *et al.* (2012) Manzouri *et al.* (2013); Bartol (2014); Boyson (2014); Charitoudi and Blyth (2014)

Standard guidelines for SC collaboration	Pfleeger *et al.* (2007); Rongping and Yonggang (2014); Davis (2015); Sindhuja and Kunnathur (2015)
Supplier audit	Zhang *et al.* (2012); Bartol (2014); Windelberg (2016)
Training	Warren and Hutchinson (2000); Pfleeger *et al.* (2007); Deane *et al.* (2009); Deane *et al.* (2010); Bartol (2014); Davis (2015); Sindhuja and Kunnathur (2015); Tran *et al.* (2016)
Vulnerability checks	Jones and Horowitz (2012); Stephens and Valverde (2013); Boyes (2015)
"Zero-trust" policy	Boone (2017)
Trans-attack phase	
Data consistency checks	Jones and Horowitz (2012)
Task force	Davis (2015)
Post-attack phase	
Forensics	Jones and Horowitz (2012)
Incident documentation	Deane *et al.* (2009); Davis (2015); Windelberg (2016)
Insurances	Huang *et al.* (2008); Boyson (2014); Camillo (2017)
Recovery and backup procedures	Deane *et al.* (2009); Windelberg (2016)

Equally prominent in the literature is the accreditation of cyber systems against security standards, such as ISO/IEC. Until now, official bodies have developed and introduced dozens of standards for different industries and sectors covering cyber security issues (Bartol, 2014). The adherence to these standards can serve as a base for a standard set of terminology and understanding of key security concepts (Davis, 2015), but also as a guideline to desired security objectives (Kunnathur, 2015). Nevertheless, from a SC perspective, the implementation of these standards has often been criticised for various reasons. Kunnathur (2015) argue that current standards are designed for independent

companies; although there is a strong need for standardised inter-organisational practices, it lacks as evidenced by the variety of accrediting bodies/organisations (*ibid*). Keegan (2014) and Davis (2015) argue that due to the numbers of entities in most supply chains, successful implementation of inter-organisational standards is only replicable at the level of direct supply (Tier 1 suppliers), but cannot extend further up the supply chain network. Hence, the focal company spending resources on accreditation against these standards cannot ensure that the entire SC will follow their example. Venter (2014) is particularly critical of the standards, stating that some of the proposed methods are not feasible or are simply bad practice. Another criticism is that there is a common misconception of ISO standards, that they do not have an expiration date (Al-Najjar and Jawad, 2011). This makes companies believe that once they have acquired accreditation, they will always meet the required standards. Consequently, companies which have acquired a certificate often assume they do not have to improve their processes continuously, thus risking complacency.

Another countermeasure which is frequently examined in the literature but still requires thorough evaluation is information sharing. As stated in Table IV, many authors consider information sharing as a promising way to cope with cyber risks, because it allows for intra- and inter-organisational communication and processing of risk-relevant data. The enforcement of the General Data Protection Regulation (GDPR) in May 2018 is likely to standardise information sharing to protect breaches of individual and business rights and freedom (National Cyber Security Centre, UK, 2018). Paradoxically, many scholars claim that information sharing is one of the most severe threats to cyberspaces. This is due to the level of support required to handle large volumes of highly sensitive information, without which human errors increase (Smith et al., 2007; Deane et al., 2009; Kim and Im, 2014). Nevertheless, as Tran et al. (2016) found in a series of interviews, many companies do not perceive potential ‘information leakage' as a security risk. It is critical that employees frequently change their passwords and do not share passwords with others to avoid information leakage.

Most of the risks discussed in the literature can be attributed to the pre-attack phase; few articles address countermeasures for subsequent phases (trans-attack and post-attack). To address this imbalance, more work is needed on the proactive mitigation of

cyber risks and reactive mitigation strategies. ‘Cyber-insurance' is one prominent mitigating measure for the post-attack stage. Cyber insurance dates from projections for Y2K related crashes but has burgeoned due to the increase in virtual events and their impact on businesses (Camillo, 2017). The growth of *Industry 4.0* is likely to be regulated by similar insurance policies. It may be impossible to design the perfect cyber security system that can deter all risks; therefore, it is expedient to have a diverse set of countermeasures at hand, covering different risk attack scenarios and contingencies.

5 Conclusion

At its core, supply chain management is a discipline of connectedness; integrating the activities and processes of diverse organisations into effectively functioning networks. But with supply chain integration comes dependencies, some purely commercial, but many arising from integrating IT systems to exchange data/information, giving rise to supply chain cyber risk. This study defines supply chain cyber risk as accidental or deliberate IT events that threaten the integrity of a supply chain’s infrastructure, leading to cascading disruptions. Similar to conventional supply chain risks, cyber risk impacts in terms of financial losses, delays and loss of customer service on a short-term basis; and market value and brand reputation on a long-term basis.

A SLR on the nascent area of cyber risks in supply chains was conducted applying a rigorous, transparent and replicable methodology. The study addressed the research question: *How can organisations manage cyber risks in supply chains?* Text mining was followed by connectivity-based clustering to identify and verify the core themes (Figure 6) that guide and inform the analysis. Five meta themes were selected: cyber risk types; cyber risk propagation; cyber risk points of penetration; cyber security challenges and mitigation measures.

Under cyber risks, the study classifies cyber risks into five categories: physical threats, breakdown, indirect attacks, direct attacks and insider threats. Cyber risk propagation zones were identified (primary, secondary and tertiary) drawing on previous work which suggests supply chain risks are not static and follows the ‘*risk propagation*’ phenomenon (Ghadge et al., 2013; Garvey et al., 2015). The third meta-theme identifies three key failure points where cyber risks are likeliest to emerge. The study classifies these

‘points of penetration' (PoPs) into technical, human and physical dimensions. Four critical challenges for an organisation trying to manage supply chain cyber risks are recognised; inter-organisational collaboration; employee knowledge, continuous improvement and the need for government level involvement. The fifth and final meta-theme is measures for mitigation. Although carry over measures from traditional risk mitigation work are identified in the literature, the study rejects using a conventional proactive and reactive risk mitigation classification and instead adopts a time phase-based classification. See Table III for classification of cyber risk measures for mitigation following pre, trans and post cyber-attack stages.

While indirect and direct attacks (i.e., viruses, hacker attacks, spoofing attacks) are undoubtedly the most commonly discussed types of attack, the study found that the increasing integration and complexity of cyber SCs, facilitates the occurrence of unintentional cyber risk events such as the underperformance of a critical cyber system or an unintended human error. With the latter, the employee could potentially be anywhere in the interconnected SC, adding to unpredictability and compounding consequences. For capturing these consequences, this study used a risk propagation approach and depicted how cyber risks occurring at one point of penetration spread to other linked entities driven by SC inter-connectivity.

5.1. Conceptual model

This study finds that companies need to implement identified control measures holistically at the SC level to create an extensive supply chain cyber security system that builds upon elements from both IT and organisational security systems. To address this need and building on the finding that cyber supply chain risks can emerge from different sources, the study proposes a ‘*supply chain cyber security system*’ as a unifying conceptual model (Figure 10). These sources are identified as either associated with IT (e.g., such as a direct or indirect attack), organisational (e.g., insider threat) or the supply chain (e.g., physical threat) systems. Thus, all three diverse elements namely, IT system, organisation process, and supply chain security system (which includes process and infrastructure network) must be aligned to manage cyber risk in supply chains. Each of these three can then be linked to specific PoPs weak points and linked with technical, human and physical levels. Thus, IT

security systems can counter cyber threats by buying hardware, the latest technology and secure software platforms. Organisational security system mitigates cyber-attack by securing physical assets, adhering to set guidelines and by raising awareness among employees. Information sharing, collaborative risk management, and adaptability are found to be key strategies for supply chain security. This interlinked relationship between different (sub) system (shown in overlapping circles in Figure 10) and distinct mitigation strategies (shown in the triangles) is critical for managing cyber risk in supply chains. Coordination of these security systems, joint information sharing and applying appropriate mitigating strategies can effectively manage cyber risk in supply chains.

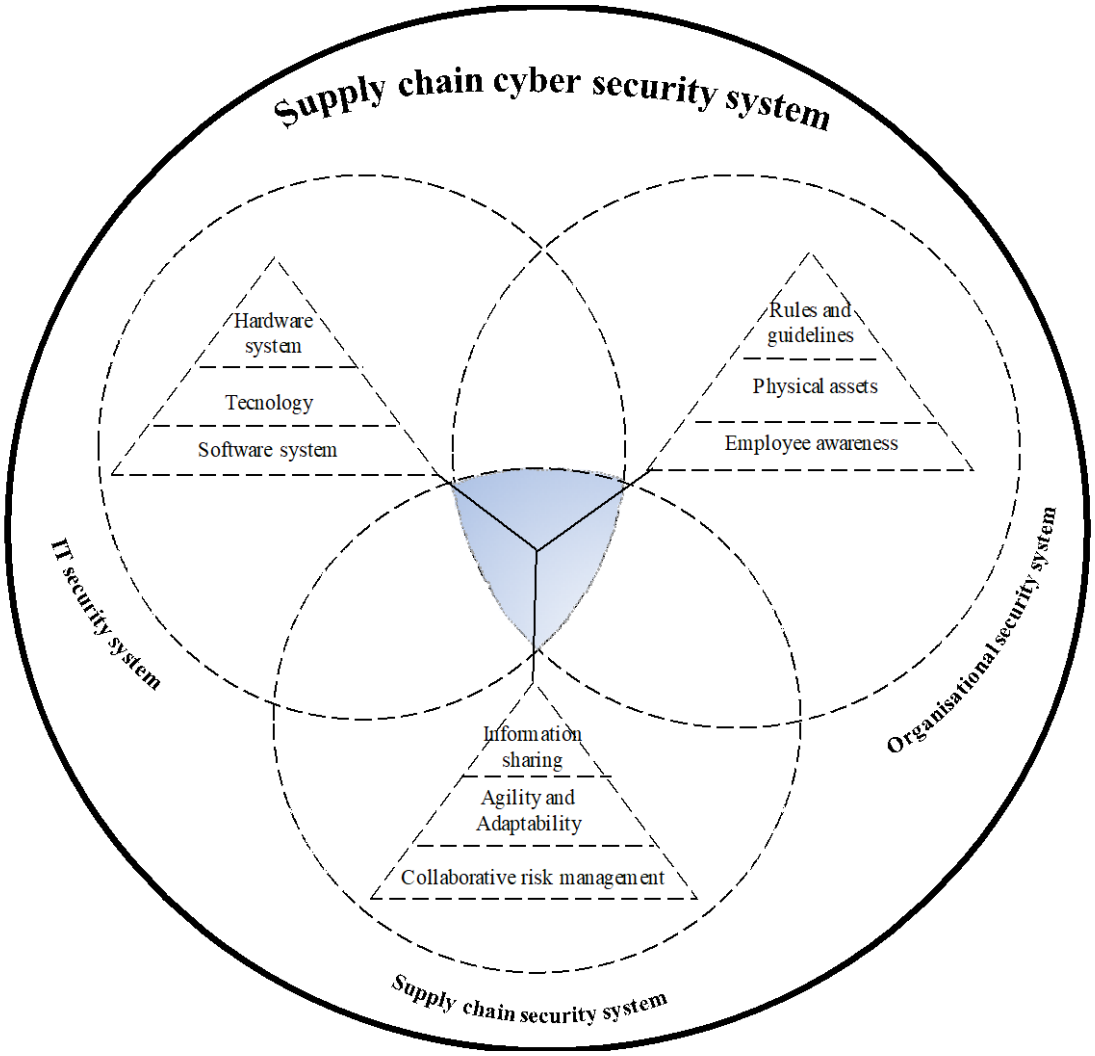

Figure 10. A conceptual model for *Supply Chain Cyber Security System*

This integrated model shown in Figure 10, is termed a Supply Chain Cyber Security System. The conceptual model shows that IT, organisation and supply chain security systems are interlinked, and closer collaboration is essential for successful implementation of cyber risk mitigation strategies (Stephens and Valverde, 2013; Hamlen and Thuraisingham, 2013; Urciuoli et al., 2013; Bartol, 2014). These inter-disciplinary security systems should be coordinated to standardise and implement agreed cyber security strategies for supply chains and wider networks. Alignment of responsibilities and managing conflicting policies/regulations in each system is a challenging problem to handle. There is however the age-old threat that a chain is only as strong as its weakest link; hence our model's focus on the integration of IT system, organisation and supply chain (including process and network infrastructure) security system.

5.2 A research agenda for managing cyber risk in supply chains

A literature review is expected to provide critical knowledge gaps along with the development of new models, proposition or theories (Webster and Watson, 2002). The main avenues for future research that emerged from this review are now presented. Recent research has suggested several dimensions that have a substantial influence on a SC's vulnerability to cyber risk. These include different network configurations (Bandyopadhyay et al., 2010; Zhang et al., 2012), firm sizes (Tran et al., 2016), corporate cultures (Xue et al., 2013), industry sectors (Sharma and Routroy, 2016; Tran et al., 2016) and business principles (Durowoju et al., 2012; Charitoudi and Blyth, 2014). This research found that most studies take a generic perspective, and therefore, this study pinpoints the need for contextualised studies that address such dimensions in-depth to relate specific cyber risks to specific dimensions. Similarly, an array of mitigation measures against cyber risks have been identified; however, there is little evidence of specific measures for mitigation being empirically tested. So, to make the mitigation decision useful, for clarity of when and where responses work best, strategies are identified and separated into the three phases namely, pre-, trans- and post-attack. Adopting this approach reveals that there is a lack of research on developing tailored measures for cyber security threats. In addition to highly context-specific studies, large-scale data-driven research is necessary, which can then be utilised to test hypotheses and models (Barlow and Li, 2007; Kunnathur, 2015).

Empirical research on building robust cyber security models utilising modern big data analytics tools and techniques is also required to inform and fuel the next generation of research in this field.

It is evident from this SLR that human/behavioural factors play a vital role in cyber security, and yet have been neglected in favour of studying more technical factors such as data, applications and networks. In cyberspace, employees are a major failure point (PoPs), yet technologically empowered employees manage developments such as IoT, blockchain and decentralised distribution (omnichannel retailing) with little awareness or training on data security. Incriminating human interactions have widely been ignored (Kunnathur, 2015). A variety of supply chain stakeholders can sabotage, either deliberately or unwillingly, even the most sophisticated security systems. However, this study also detects a related lack of research on the *impact of cyber risk on employees* (and by definition therefore their employing organisation). This is very much an under-explored area (Manzouri et al., 2013), which will become of increasing interest to employees, employers and society.

5.3 Implications for research and practice

To identify relevant literature of an appropriate quality and quantity, the SLR had to extend beyond articles in the operations, logistics and supply chain area. Following a replicable and reiterative screening and synthesis process, the scope of this study was still limited to 41 independently verified interdisciplinary papers published between 1990 and 2017. Complementary cluster analysis following data mining approach provided support for transparency and rigour in conducting what is believed to be a first SLR on cyber risk in supply chains.

The paper provides the following implications for research and practice. The negative consequences of cyber security disruptions could impact not only individual firms or SCs, but entire globally-connected communities. The limited set of papers available for this study suggests that little academic attention has addressed this field compared to other topics/technologies interfacing with supply chain management such as the Internet of Things (IoT), Blockchain, digitalisation, autonomous transportation and virtual reality. Interestingly, all these disruptive technologies are vulnerable to cyber risks due to the rapid transformation of supply chains following the *Industry 4.0* revolution. Supply chain

integration and digitalisation go hand in hand. Recently Gartner (2018) predicted that there would be 14.2 billion devices connected worldwide by 2019. Consequently, it is vital to raise awareness of cyber security risks in supply chains and help both practitioners and academics manage future disruptive cyber risks.

There is an increased misuse of cyber-physical systems for counterfeits, forgeries, data theft, trafficking, attacks on transportation infrastructure, ransomware attacks and Crypto-jacking. Such cyber activities significantly impact multiple stakeholders with clear implications for a broader ecosystem. How will businesses, governments and society react to profound and frequent cyber-attacks? This is perhaps the most fundamental cyber risk-related line of questioning, as the answers will dictate the speed and level of investment in cyber security worldwide.

REFERENCES

Al Kattan, I., Al Nunu, A. and Saleh, K. (2009), "A stochastic model for improving information security in supply chain systems", *International Journal of Information Systems and Supply Chain Management*, Vol. 2 No. 3, pp. 35-49.

Al-Najjar, S. and Jawad, M. (2011), "ISO 9001 implementation barriers and misconceptions: An empirical study", *International Journal of Business Administration*, Vol. 2 No. 3, pp. 118-131.

Amin, Z. (2017), "A practical road map for assessing cyber risk", *Journal of Risk Research*, pp. 1-12.

Arksey, H. and O'Malley, L. (2005), "Scoping studies: towards a methodological framework', *International Journal of Social Research Methodology*, Vol. 8 No. 1, pp. 19-32.

Bahl, S., Wali, O. and Kumaraguru, P. (2011), "Information security practices followed in the Indian software services industry: An exploratory study", *Second Worldwide Cybersecurity Summit*. London, 2011.

Bandyopadhyay, T., Jacob, V. and Raghunathan, S. (2010), "Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest", *Information Technology and Management*, Vol. 11 No. 1, pp. 7-23.

Barlow, A. and Li, F. (2007), "E-supply chains: understanding current and future opportunities and barriers", *International Journal of Information Technology and Management*, Vol. 6 No. 2-3-4, pp. 286-298.

Bartol, N. (2014), "Cyber supply chain security practices DNA – filling in the puzzle using a diverse set of disciplines", *Technovation*, Vol. 34 No. 7, pp. 354-361.

Boone, A. (2017), "Cyber-security must be a C-suite priority", *Computer Fraud and Security*, Vol. 2, pp. 13-15.

Boyes, H. (2015), "Cybersecurity and cyber-resilient supply chains", *Technology Innovation Management Review*, Vol. 5 No. 4, pp. 28-34.

Boyson, S. (2014), "Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems", *Technovation*, Vol. 34 No. 7, pp. 342-353.

Burgess, K., Singh, P. J. and Koroglu, R. (2006), "Supply chain management: a structured literature review and implications for future research", *International Journal of Operations & Production Management*, Vol. 26 No. 7, pp. 703-729.

Caldwell, T. (2015), "Securing small businesses–the weakest link in a supply chain?" *Computer Fraud & Security*, Vol. 9, pp. 5-10.

Cebula, J. J., & Young, L. R. (2010). "A Taxonomy of Operational Cyber Security Risks", Technical Note CMU/SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H. and Stoddart, K. (2016), "A review of cyber security risk assessment methods for SCADA systems", Computers *& Security*, Vol. 56, 1-27.

Charitoudi, K. and Blyth, A. J. C. (2014), "An agent-based socio-technical approach to impact assessment for cyber defense", *Information Security Journal: A Global Perspective*, Vol. 23 No. 4-6, pp. 125-136.

Creswell, J. (2014), *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. Thousand Oaks, California: SAGE Publications Inc.

Davis, A. (2015), "Building cyber-resilience into supply chains", *Technology Innovation Management Review*, Vol. 5, No. 4, pp. 19-27.

Deane, J. K., Ragsdale, C. T., Rakes, T. R. and Rees, L. P. (2009), "Managing supply chain risk and disruption from IT security incidents", *Operations Management Research*, Vol. 2 No. 1-4, pp. 4-12.

Deane, J. K., Rees, C. L. and Baker, W. H. (2010), "Assessing the information technology security risk in medical supply chains", *International Journal of Electronic Marketing and Retailing*, Vol. 3 No. 2, pp. 145-155.

Denyer, D. and Tranfield, D. (2009), Producing a systematic review', in Buchanan, D. and Bryman, A. (eds.) *The Sage Handbook of Organizational Research Methods*. Thousand Oaks, CA: Sage Publications, pp. 671-689.

Denyer, D., Tranfield, D. and van Aken, J. (2008), "Developing design propositions through research synthesis", *Organization Studies*, Vol. 29 No. 3, pp. 393-413.

Dolgui, A., Ivanov, D., & Sokolov, B. (2018), "Ripple effect in the supply chain: an analysis and recent literature", *International Journal of Production Research*, Vol. 56 No. 1-2, pp. 414-430.

Durowoju, O., Chan, H. K. and Wang, X. (2012), "Entropy assessment of supply chain disruption", *Journal of Manufacturing Technology Management*, Vol. 23 No. 8, pp. 998-1014.

Ehrich, K., Freeman, G., Richards, S., Robinson, I. and Shepperd, S. (2002), "How to do a scoping exercise: continuity of care", *Research, Policy and Planning*, Vol. 20 No. 1, pp. 25-29.

Eling, M. and Wirfs, J. (2019), "What are the actual costs of cyber risk events?", *European Journal of Operational Research*, Vol. 272, pp. 1109–1119.

Faisal, M. N., Banwet, D. K. and Shankar, R. (2007), "Information risks management in supply chains: an assessment and mitigation framework", *Journal of Enterprise Information Management*, Vol. 20 No. 6, pp. 677-699.

Franke, U. and Brynielsson, J. (2014), "Cyber situational awareness–a systematic review of the literature", *Computers & Security*, Vol. 46, pp.18-31.

Gartner (2018), Gartner Identifies Top 10 Strategic IoT Technologies and Trends. Available at: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends (Accessed 18.07.2019).

Garvey, M. D., Carnovale, S. and Yeniyurt, S. (2015), "An analytical framework for supply network risk propagation: A Bayesian network approach", *European Journal of Operational Research*, Vol. 243 No. 2, pp. 618-627.

Ghadge, A., Dani, S. and Kalawsky, R. (2012), "Supply chain risk management: present and future scope", *The international journal of logistics management*, Vol. 23 No. 3, pp. 313-339.

Ghadge, A., Dani, S., Chester, M., & Kalawsky, R. (2013), "A systems approach for modelling supply chain risks", *Supply chain management: an international journal*, Vol. 18 No. 5, pp. 523-538.

Ghadge, A., Wurtmann, H., & Seuring, S. (2019), "Managing climate change risks in global supply chains: a review and research agenda", *International Journal of Production Research*, pp. 1-21.

Hamlen, K. W. and Thuraisingham, B. (2013), "Data security services, solutions and standards for outsourcing", *Computer Standards & Interfaces*, Vol. 35 No. 1, pp. 1-5.

Ho, W., Zheng, T., Yildiz, H. and Talluri, S. (2015), "Supply chain risk management: a literature review", *International Journal of Production Research*, Vol. 53 No. 16, pp. 5031-5069.

Houses of Parliament, (2011), Available at: https://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-uk.pdf (Accessed: 18.07.2019).

Huang, C. D., Behara, R. S. and Hu, Q. (2008), "Managing risk propagation in extended enterprise networks", *IT Professional*, Vol. 10 No. 4.

Jones, R. A. and Horowitz, B. (2012), "A system-aware cyber security architecture", *Systems Engineering*, Vol. 15 No. 2, pp. 225-240.

Jüttner, U., Peck, H. and Christopher, M. (2003), "Supply chain risk management: Outlining an agenda for future research", *International Journal of Logistics: Research & Applications*, Vol. 6 No. 4, pp. 197-210.

Kache, F. and Seuring, S. (2014), "Linking collaboration and integration to risk and performance in supply chains via a review of literature reviews", *Supply Chain Management: An International Journal*, Vol. 19 No. 5/6, pp. 664-682.

Keegan, C. (2014), "Cyber security in the supply chain: A perspective from the insurance industry", *Technovation*, Vol. 34 No. 7, pp. 380-381.

Khan, O. and Estay, D. A. S. (2015), "Supply chain cyber-resilience: Creating an agenda for future research", *Technology Innovation Management Review*, Vol. 5 No.4.

Khan, R., Haque, M. M. and Hasan, R. (2015), "Towards supply chain information integrity preservation", *CrossTalk*, Vol. 28 No.5, pp. 4-10.

Khursheed, A., Kumar, M. and Sharma, M. (2016), "Security against cyber-attacks in food industry", *International Journal of Control Theory and Applications*, Vol. 9 No.17, pp. 8623-8628.

Kim, K. C. and Im, I. (2014) "Research letter: Issues of cyber supply chain security in Korea", *Technovation*, Vol. 34 No. 7, pp. 387-387.

Kunnathur, A. (2015), "Information security in supply chains: A management control perspective", *Information and Computer Security*, Vol. 23 No. 5, pp. 476-496.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J. and Kott, A. (2013), "Resilience metrics for cyber systems", *Environment Systems and Decisions*, Vol. 33, No. 4, pp. 471-476.

Linton, J. D., Boyson, S. and Aje, J. (2014), "The challenge of cyber supply chain security to research and practice - An introduction", *Technovation*, Vol. 34 No. 7, pp. 339-339.

Luiijf, E., Besseling, K. and de Graaf, P. (2013), "Nineteen national cyber security strategies", *International Journal of Critical Infrastructures*, Vol. 9 No. 1-2, pp. 3-31.

Manuj, I. and Mentzer, J. T. (2008), "Global supply chain risk management strategies", *International Journal of Physical Distribution & Logistics Management*, Vol. 38 No. 3, pp. 192-223.

Manzouri, M., Ab Rahman, M. N., Nasimi, F. and Arshad, H. (2013), "A model for securing sharing information across the supply chain", *American Journal of Applied Sciences*, Vol. 10 No. 3, pp. 253-253.

McCracken, G. (1988) *The Long Interview*. Newsbury Park, CA: SAGE.

Mustafa Kamal, M. and Irani, Z. (2014), "Analysing supply chain integration through a systematic literature review: a normative perspective", *Supply Chain Management: An International Journal*, Vol. 19 No. 5/6, pp. 523-557.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. and Sadhukhan, S. K. (2013), "Cyber-risk decision models: To insure IT or not?" *Decision Support Systems*, Vol. 56, pp. 11-26.

National Cyber Security Centre, UK (2018), Public report on *the cyber threat to UK businesses,* 2017-18. Available at https://www.ncsc.gov.uk/cyberthreat, (Accessed: 12.02.2019).

National Cyber Security Centre, UK (2016), *Common Cyber Attacks: Reducing the Impact.* Available at https://www.ncsc.gov.uk/white-papers/common-cyber-attacks-reducing-impact, (Accessed: 12.02.2019).

Öğüt, H., Raghunathan, S. and Menon, N. (2011), "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection", *Risk Analysis: An International Journal*, Vol. 31, No. 3, pp. 497-512.

Peck, H. (2006), "Reconciling supply chain vulnerability, risk and supply chain management", *International Journal of Logistics Research and Applications*, Vol. 9 No. 2, pp. 127-142.

Pfleeger, S. L., Libicki, M. and Webber, M. (2007), "I'll buy that! Cybersecurity in the internet marketplace", *IEEE Security and Privacy*, Vol. 5 No. 3, pp. 25-31.

Reade, C. (2009), "Human resource management implications of terrorist threats to firms in the supply chain", *International Journal of Physical Distribution & Logistics Management*, Vol. 39 No. 6, pp. 469-485.

Renaud, K., Flower day, S., Warrenton, M., Cocksfoot, P. and Oregon, C. (2018), "Is the responsibilization of the cyber security risk reasonable and judicious?" *Computers & Security*, Vol. 78, pp. 198-211.

Rongping, M. and Yonggang, F. (2014), "Security in the cyber supply chain: A Chinese perspective", *Technovation*, Vol. 34 No. 7, pp. 385-385.

Rousseau, D. M., Manning, J. and Denyer, D. (2008), "Evidence in management and organizational science: Assembling the field's full weight of scientific knowledge through syntheses", *The Academy of Management Annals*, Vol. 2 No. 1, pp. 475-515.

Sharma, S. and Routroy, S. (2016), "Modelling information risk in supply chain using Bayesian networks", *Journal of Enterprise Information Management*, Vol. 29 No. 2, pp. 238-254.

Sindhuja, P. (2014), "Impact of information security initiatives on supply chain performance an empirical investigation", *Information Management and Computer Security*, Vol. 22 No. 5, pp. 450-473.

Smith, G. E., Watson, K. J., Baker, W. H. and Pokorski Ii, J. A. (2007), "A critical balance: Collaboration and security in the IT-enabled supply chain", *International Journal of Production Research*, Vol. 45 No. 11, pp. 2595-2613.

Sokolov, A., Mesropyan, V. and Chulok, A. (2014), "Supply chain cyber security: A Russian outlook", *Technovation*, Vol. 34 No. 7, pp. 389-389.

Stephens, J. and Valverde, R. (2013), "Security of E-Procurement Transactions in Supply Chain Reengineering", *Computer and Information Science*, Vol. 6 No. 3, pp. 1-20.

Tan, P. N., Steinbach, M., & Kumar, V. (2017), "Data mining cluster analysis: basic concepts and algorithms", *Introduction to data mining,* Second edition, Pearson, USA.

The Institute of Risk Management (2014) *Cyber Risk: Executive Summary*. [Online]. Available at: https://www.theirm.org/media/2612400/IRM_Cyber-Risk_Exec-Summ_A5_low-res.pdf (Accessed: 12.02.2019).

Tran, T., Childerhouse, P., Deakins, E. (2016), "Supply chain information sharing: challenges and risk mitigation strategies", *Journal of Manufacturing Technology Management*, Vol. 27 No. 8, pp. 1102-1126.

Tranfield, D., Denyer, D. and Smart, P. (2003), "Towards a methodology for developing evidence-informed management knowledge by means of systematic review", *British Journal of Management*, Vol. 14, pp. 207-222.

Urciuoli, L. and Hintsa, J. (2017), "Adapting supply chain management strategies to security - an analysis of existing gaps and recommendations for improvement", *International Journal of Logistics*, Vol. 20 No. 3, pp. 276-295.

Urciuoli, L., Männistö, T., Hintsa, J. and Khan, T. (2013), "Supply chain cyber security - potential threats", *Information & Security: An International Journal*, Vol. 29, pp. 51-68.

Venter, H. S. (2014), "Security issues in the security cyber supply chain in South Africa", *Technovation*, Vol. 34 No. 7, pp. 392-392.

Verizon (2018), *Data breach investigations report*, Available at: http://www.verizonenterprise.com/industry/public_sector/docs/2018_dbir_public_sector.pdf ((Accessed: 18.07.2019).

Warren, M. and Hutchinson, W. (2000), "Cyber-attacks against supply chain management systems: A short note", *International Journal of Physical Distribution & Logistics Management*, Vol. 30 No. 7/8, pp. 710-716.

Webster, J. and Watson, R. (2002), "Analyzing the Past to Prepare for the Future: Writing a Literature Review", *MIS Quarterly*, Vol. 26 No. 2, pp. Xiii-Xxiii.

Wilding, R.D and Wagner, B. (2012), "Systematic review and the need for evidence", *Supply Chain Management: An International Journal*, Vol. 17 No. 4.

Williams, C. (2014), "Security in the cyber supply chain: Is it achievable in a complex, interconnected world?", *Technovation*, Vol. 34 No. 7, pp. 382-384.

Xue, L., Zhang, C., Ling, H. and Zhao, X. (2013), "Risk mitigation in supply chain digitization: System modularity and information technology governance", *Journal of Management Information Systems*, Vol. 30 No. 1, pp. 325-325.

Yoon, J., Talluri, S., Yildiz, H. and Ho, W. (2017), "Models for supplier selection and risk mitigation: a holistic approach", *International Journal of Production Research*, pp. 1-26.

Zhang, D. Y., Cao, X., Wang, L. and Zeng, Y. (2012), "Mitigating the risk of information leakage in a two-level supply chain through optimal supplier selection", *Journal of Intelligent Manufacturing*, Vol. 23 No. 4, pp. 1351-1364.

APPENDIX I

Keyword identification based on inter-disciplinary literature review

Supply Chain Risk Management	Information Technology	Universal keywords
Enterprise risk management	Cyber security	Cybersecurity
Risk management	Cyber attack	Disruption
Supply chain attacks	Cyber breaches	Firewall
Supply chain crime	Cyber crime	Hacker
Supply chain integrity	Cyber crisis	Infrastructure
Supply chain integrity risk	Cyber disruptions	Phishing
Supply chain resilience	Cyber/IT failure	Sabotage
Supply chain risk(s)	Cyber incident	Security
Supply chain security	Cyber resilience	Spoofing
Supply chain threats	Cyber supply chain(s)	Surveillance
Risk identification	Cyber supply chain risk management	Terrorism
Risk assessment	Cyber systems	Threat
Risk mitigation	Cyber supply network	
Risk control	Data/Information security	
	Information infrastructure	
	Information security/risk	