Technical University of Denmark

Master Thesis

Cyber Risks in Supply Chains

This work is submitted for the degree of
MSc in Industrial Engineering and Management

Author:
Pablo Jose Guerra Guerra (s150907)

Supervisor:
Peter Jacobsen

Co-Supervisor:
Daniel Alberto Sepúlveda Estay

DTU Management Engineering
Department of Management Engineering

May 2018

Contents

List of Figures

List of Tables

List of Abbreviations

CI - Critical Infrastructure

CPS - Cyber-Physical System

IC - Integrated Circuit

IIoT - Industrial Internet of Things

IoT - Internet of Things

IS - Information Systems

IT - Information Technology

KM - Knowledge Management

RFID - Radio-Frequency Identification

SCCRM - Supply Chain Cyber Risk Management

SLR - Structured Literature Review

1 Introduction

Nowadays, the presence of IT systems and the cyberspace in the global industry is becoming ever more relevant. The current "fourth industrial revolution", or Industry 4.0, is causing a radical shift in the way industry operates. It has brought digitalisation and the Internet to potentially every part of a product's value chain. This has resulted in Cyber-Physical Systems (CPS), which combine software and production assets, giving way to the integration of elements like higher automation, Industrial Internet of Things (IIoT), data sharing and cloud computing with the industry (Boyes 2015, Khan & Estay 2015, Tjahjono et al. 2017, Jayaram 2016, Manners-Bell 2014, Jarvelainen 2013).

On the other hand, competitive pressure encourages organisations to make use of advances in information technologies and connectivity to adapt their supply chains in a global economy (Boyes 2015, Estay & Khan 2015). From this supply chain perspective, companies have gained the ability to identify and respond faster to changes in the external environment (i.e. customer preferences), through automating processes using cyber-physical systems (CPS), implementing management systems based on computers, and the reduction of stocks by means of just-in-time manufacturing and production-to-order systems (Tjahjono et al. 2017, Boyes 2015).

Nonetheless, the higher automation and integration of IT and cyber-technologies in the industry carries new risks with itself. Advanced manufacturing systems are not secure in the same way as traditional systems. Cybersecurity has become critical for the success of smart manufacturing, as IoT enabled cyber-physical systems can be threatened by a broad range of cyber-attacks coming from criminals, terrorists and hacktivists (He et al. 2016). These cyber-attackers could use new channels to exploit poorly-secured systems for different purposes, giving way to threats like harassment, corporate espionage, extortion, stock market manipulation, or planning and carrying out terrorist activities. In parallel, there is the risk that failing to ensure continuous IT systems may also cause disruptions in operations (Jarvelainen 2013), and consequent challenges for mission assurance of the enterprise (Bodeau et al. 2010). McAfee (2014) estimates that cybercrime's annual cost to the global economy could range between US$375 billion and US$575 billion.

Modern industries face IT-risks and cyber-risks that are associated not only to their own data and control systems, but also to their supply chains (He et al. 2016). Different processes can now be connected both with suppliers and customers through the internet, forming part of a shared network. This means that cyber-attackers can potentially access and impact actors sharing this same network, gaining access to companies systems through the weakest link in the supply network (He et al. 2016, Estay & Khan 2015). Furthermore, information in modern supply chains is shared mainly digitally, resulting in supply chains being so reliant on good quality information that, without it, "supply chain managers would not be able to make decisions on forecasts, production, distribution, etc." (Khan & Estay 2015). Therefore, even in the most efficient and responsive supply chains, compromised data and IT systems could translate into performance being enormously affected, without the much-needed good quality information.

As a way of managing these risks, a lot of research effort had been put into the technical aspects (He et al. 2016). However, growing complexity of supply chains, as well as a increasing sophistication in cyber-attacks, has suggested that holistic approaches must be taken, as technical solutions are just not enough in today's socio-cyber systems (Demchak 2012). In fact, several sources defend that companies must prepare "for the inevitable" PWC (2017) and, in recent years, it has been suggested that the research focus in the area should lean more towards how to build cyber-resilient supply chains (Khan & Estay 2015).

In general, there seems to be very few frameworks available, specifically adapted and/or validated for the management of this kind of risks (Gaudenzi & Siciliano 2018, Khan & Estay 2015). As Boyes (2015) defends, there is still the "common misconception" that cybersecurity is "solely about technology", while in fact it encompasses people, processes, physical aspects and technological aspects, and all of those aspects must be treated or else the overall cyber-security of a system will be undermined. Gaudenzi & Siciliano (2017), similarly, finds that even though technical solutions are important to protect value creation, a major integration among organisational, relational and technical capabilities is also relevant when it comes to dealing with technological issues.

'Cyber attacks' figured in the Global Risks Report 2017 by the World Economic Forum (WEF

2017), as the top 1 risk to doing business in North America, and in the top 5 for East Asia and Pacific. However, despite the widespread recognition of this threat, Gaudenzi & Siciliano (2018) showed that there is a lack of awareness and preparedness at different organisational levels, stressing that managerial action has not given enough attention to the management of risks generated by IT systems and the Cyberspace. The Global State of Information Security® Survey (GSISS) 2018, by PWC (2017), supported this view by highlighting that 48% of the 9,500 executives in 122 countries surveyed do not have an employee security awareness training program, and 54% do not have an incident response process. But, what results more shocking is that despite the relevance of this issue, 44% of respondents recognised not having an overall information security strategy.

In fact, from looking at the scientific literature available, supply chain cyber risk management is a relatively novel field, and it has been seen that authors only recently investigated the impacts of cyber risks and IT risks on supply chains (Boyson 2014, Jarvelainen 2013, Gaudenzi & Siciliano 2017, Khan & Estay 2015, Olson & Wu 2010). The number of theoretical frameworks that can guide managers to assess and manage IT and cyber risks in protecting supply chain processes is currently very limited (Gaudenzi & Siciliano 2018). However, first it is needed to increase our understanding of the occurrence, detection and reaction to cyber attacks and IT incidents (Khan & Estay 2015), as more data is needed in order to validate any theories and conceptual frameworks and models.

Therefore, the following research question is proposed:

RQ: How should the risks derived from the use of IT systems be managed along the supply chain?

To answer this research question, this thesis is structured in the following way: in chapter 2.4 the methodology to follow is defined and argued. Then, the execution of this methodology and the findings of the process are described in section 3. Section 4 makes use of the findings from the previous section to provide a more meaningful answer to the research question. The validity of the results obtained throughout this thesis and the improvement of the process are then debated in section 5, while the contributions of this work are presented in section 6. To finalise, section 7 sums and concludes this document.

2 Methodology

In order to address the research question, a structured literature review (SLR) approach is conducted. Systematic reviews are different from other traditional narrative reviews, as they adopt a process that is replicable, scientific and transparent (Tranfield et al. 2003).

The steps that are followed are in accordance with those proposed by Durach et al. (2017) to conduct SLRs in the field of supply chain management, which can be seen below:

- **Step 1:** Definition of the research question
- **Step 2:** Determination of the required characteristics of primary studies
- **Step 3:** Retrieving baseline sample
- **Step 4:** Selection of the pertinent literature from the sample
- **Step 5:** Synthesising the literature
- **Step 6:** Reporting and using the results

However, as Tranfield et al. (2003) argues, literature reviews in the area of management (like this one) are often regarded as a "process of exploration, discovery and development", which usually makes unsuitable the planning the SLR in high detail. Therefore, although the basic ideas behind each step for the SLR are followed in a similar way as described by Durach et al. (2017), intentionally some of them are left very roughly defined at the start of the SLR, while being more closely defined and refined later in the process, to find a better fit for the particularities of the project, which are in some cases realised along the way.

For example, there is a fine balance that must be addressed, which is the size of the review sample versus the time resource available. The definition of broader search terms and criteria for categorising publications as "valid" to be reviewed results in the obtention of a bigger sample. A bigger sample provides statistical benefits when it comes to finding relevant publications, but at a time cost (Tranfield et al. 2003). However, research projects usually have a limited duration. When those publications must be analysed, there is the risk of ending up with a number big enough to exceed the maximum time allowed for the project.

The specifics and a detailed account of the final process followed in the SLR will be described next.

2.1 Definition of the research question

The first step in the systematic literature review is the definition of the research question, which should justify the review and highlight its expected contribution (Durach et al. 2017).

The research question was defined in the introduction of this thesis as *"How should the risks derived from the use of IT systems be managed along the supply chain?"*. In the introduction, it was highlighted that the management of cyber risks in the supply chain has not been completely unified as a body of knowledge yet. Therefore, a SLR should provide a general overview of this relatively new field, gathering the different viewpoints and linking them in a meaningful way. Consequently, in order to clarify and provide insights into the research question, as well as to shed more lights into the goals pursued by the SLR, the following sub-questions are also defined:

1. *What are the risks related to the use of IT systems in the supply chain?*
2. *What are the constructs, tools and practices proposed in the literature to approach the management of risks related to the use of IT systems in the supply chain?*
3. *How can those constructs, tools and practices be linked to improve conceptual clarity?*

2.2 Determination of the required characteristics of primary studies

In this second step, the inclusion and exclusion criteria are defined, which will be used in clarifying whether a publication can provide information that answers the research question (Durach et al. 2017)

The publications to be reviewed must have the potential to answer the research question or any of its sub-questions, and therefore the inclusion criteria are defined to include the publications that answer the aforementioned questions, while excluding the ones that clearly would not answer them, as in when they address a topic that is not directly related to the research question, or when they focus on an area related to the research question that is not relevant to answer the research question.

A preliminary reading is carried out with a few selected articles in the area of supply chain cyber risk management, spanning over a few years till the present, like Boyson (2014), Khan & Estay (2015) and Gaudenzi & Siciliano (2018). The goal is to spot the most common terminology used in this area of research, to include as many publications reflecting the most important trends as possible.

As a result of this process, the following inclusion criteria are defined:

1. The publication has a focus on supply chain, or its results can be specifically applied to supply chains.
2. The publication has a focus on the management of risks, through concepts like risk management, resilience, cyber security, IT security or information security.
3. The threats, vulnerabilities or risks that the publication discusses have to be linked to the use of IT systems. However, articles on how IT systems can be used to manage other risks in the supply chain are NOT necessarily considered, unless they refer to other IT-related risks. Exceptionally, publications that are found from cross-references and do not directly mention the link to IT-related risks can be considered to meet this criteria if, and only if, the topic they handle is linked to the management of IT-related risks by another publication in the final set of publications reviewed.
4. Only publications dated from the year 2000 to February 2018 are considered.
5. Only publications with a scientific article-like structure will be considered.

The last criterion was added later in the process, as a way of better targeting and reducing the amount of literature to be reviewed, as well as streamlining the SLR process, which risked exceeding the available time resources.

On a side note, the lower time boundary is decided to be formally set at the year 2000 because preliminary searches rarely returned any result older than 2000. However, in the end the search results returned only one publication older than 2000, but it did not meet the other inclusion criteria either.

2.3 Retrieving baseline sample

In the third step, the process of search is established, by defining the search engines to be used, as well as the key words used in them (Durach et al. 2017).

The chosen key words consider the scope of the research question and sub-questions, as well as the terminology used in the inclusion and exclusion criteria. This way, it is decided that the search queries should include a combination of the key terms: *supply chain, information technology, cyber, security, risk, management, resilience.*

From this point, a relevant issue arises, which is the need to produce a number of combinations of key terms and searches that allows to gather the most relevant publications in the topic, with the

offset that the bigger the number of results obtained, the bigger is the amount of time needed to process them. Moreover, without any previous knowledge of the success ratio of each search (i.e. % of publications in the sample that meet inclusion criteria), the target amount of search results becomes subjective and dependant on the reviewer's intuition.

In the end, eight different combinations of those terms are chosen, as to produce a meaningful baseline of publications that encompasses the main trends that answer the research question. Those combinations of terms are:

- supply chain, cyber, risk management
- "supply chain", resilience, cyber
- "supply chain", cyber risk, resilience
- "supply chain", cyber security
- "supply chain", "information technology", cyber security
- "supply chain", "information technology", cyber security, risk management
- "supply chain", "information technology", resilience, risk management
- "supply chain", "information technology", resilience

The chosen search engines are Scopus and DTU Findit. The main reason for this is that both of those search engines allow to quickly download a summary of the search results that includes relevant metadata such as the title of each publication, authors, year of publication and source of publication, as well as the full abstract of each publication. Both of those search engines allow to download this metadata after each search result, in a format that can be directly visualised and used in data processing software like Excel, or easily translatable to Excel after a few workarounds. Other popular search engines, like Google Scholar, do not have this functionality.

The value seen in such approach is that having all the previous information arranged in data sheets would allow for a much faster and structured processing of the information, consequently being able to handle a bigger search sample in less time, through functionalities like finding and discarding duplicated results from different search queries and different search engines more easily, or allowing for a faster initial screening of the search sample as it is explained in the next step.

2.4 Selection of the pertinent literature from the sample

In this part, inclusion criteria are applied to select the final publications to review, therefore discarding those search results that do not meet them (Durach et al. 2017). Additionally, as hinted by the inclusion criteria number 3, other publications could be added from outside of the sample, when identified through cross-referenced citations in the sample, in either this step or the next one.

First, all of the unique search results would be screened, reading only the title and abstract of each article. Then, they would be rated based on the perception of whether they meet the inclusion criteria or not, with one of the following three labels: "Include", "Maybe" and "Clearly excluded".

Then the publications labelled as "Include" (which should clearly meet the inclusion criteria, according to their title and abstract) would be downloaded, proceeding to the next phase in the SLR and the synthesising of their content.

The articles labelled as "Maybe" would be looked at later in the process, and then re-labelled as "Include" and "Clearly excluded", proceeding as well to synthesise their content.

Nonetheless, a few important considerations must be taken into account to understand the reasoning behind this process. First, the time required for the initial screening is "considerable" and it grows with the size of the base sample, therefore needing to balance the statistical benefits of a bigger sample with the limited time resource available (Tranfield et al. 2003). The use of spreadsheets

containing all the publications' metadata, and obtained in a semi-automated fashion, was seen as a way of increasing the sample size, through avoiding or reducing some time-wasters inherent in the first screening.

Some of those time-wasters include jumping from one web page to the next, or clicking on one link at a time to read an abstract. Others include reading the same title and abstract more than once, without noticing, and/or coming back to previously read publications to check whether it is repeated or if it was already found through other similar search queries. Moreover, search results are shown in pages in the web browser with a determined number of results in each page, which have to be screened through as a single batch, unless it is certain that search results will keep the same order of appearance if the process is stopped and continued on a different date.

Downloading and reading publications whose usefulness is not certain also increases the risk of wasting time. The expertise of the reviewer is particularly instrumental in the case where only titles and abstracts are used to distinguish articles that meet the inclusion criteria from those which do not. It can be argued that some publications that meet the inclusion criteria are easier to spot than others because of the terminology used in titles and abstracts, for reasons like complex or previously unknown terminology, or the ambiguity of the terms used. Those publications whose allegiance to the inclusion criteria is initially doubted, instead, enter a "grey area" where it is needed to read further (i.e. section containing the conclusions of the publication) to determine if they meet the criteria or not. The opposite case can also take place, when an article thought to meet the inclusion criteria is actually not relevant to the topic, which is also warned by Tranfield et al. (2003).

In less experienced reviewers, because of the lack of knowledge about the terminology and/or experience in the topic, this "grey area" tends to be greater, increasing the time wasted in reading publications that will not add value to the SLR.

In order to reduce the possibility of "accidentally" reading articles that do not meet the criteria, the publications in this "grey area" are labelled as "Maybe", and will only be reviewed after the first group of publications (labelled as "Include") are synthesised. A key point in this is the assumption that the reviewer (who is one person in this case) will have a more in-depth overview of the study field and its associated terminologies by then, being a that point more capable of reasoning whether a publication meets the inclusion criteria or not.

2.5 Synthesising the literature

As part of the process of analysis, the final list of publications is reviewed, applying "coding schemes" (also known as *themes* in our case) that will assist in extracting information from the literature (Durach et al. 2017). The synthesis process is divided into two major parts: the definition of the themes on one side, and the review and synthesis of the selected literature on the other.

A final spreadsheet, containing a list of all the publications that are considered to meet the criteria, is arranged to include all the relevant findings from each publication, while structuring those findings according to the theme they relate to, as shown in figure 1.

Themes, in our case, refer to the terminology that will be used to structure (or "label") each finding from the literature reviewed that helps in answering the research question and sub-questions.

Publication	Theme 1	Theme 2	Theme 3	Theme 4	...	...
A	X	X			X	
B		X		X		
...						

Figure 1: Example of table for structuring literature findings on different themes

The purpose of the themes, then, is to ease the final step in the SLR process, which is the reporting of results, via a more efficient and structured extraction of the findings from the different publications. As part of this process, each relevant finding is categorised in different thematic areas from the beginning, thus saving time in the final analysis of the data set, where a general picture of all

the findings relating to a certain theme can be presented.

First, the themes to be used on the review spreadsheet are defined through an iterative and dynamic process, which starts in the previous phase of the SLR, when identifying the final literature to review from the initial sample, and continues to be improved during the review and synthesis process.

As the process of reading titles and abstracts goes (in the previous step of the SLR process), terms found to be repeatedly mentioned are noted down. The focus is on identifying the terms that could represent relevant trends (or "themes") in the field of study, which could be previously overlooked by the reviewer or previously unknown to him/her, therefore filling initial "gaps" in the reviewer's awareness about the relevant terminology.

This part of the process attempts to partly reduce the risk of within-study bias mentioned by Durach et al. (2017), which is the variability in the themes used, if the study was to be repeated. This is done by reducing the probability of falsely coding data because of overlooking relevant themes. Nonetheless, the risk of coding data wrongly continues being relevant and it is not possible to completely mitigate it, due to being only one reviewer.

Once the whole sample of publications is first screened in the previous SLR step, then the terms found are assessed and complemented with others, based on the previous experience of the reviewer and a process of individual brainstorming. The end product should be a list (or "cloud") of terms that could help the reviewer in deciding what terminology should by used to start the synthesis of the literature process.

So, the next step take is to make sense of the cloud of terms found, identifying patterns that could be useful in structuring the most relevant findings captured from each publication. Main themes are identified, and sub-themes under them as well. Then, those themes and sub-themes are internally defined by the reviewer, giving them a formal meaning, as to ensure consistency in their later content, when collecting and structuring the findings.

After this, the process of reviewing and synthesising the literature starts. In each publication the following process is followed:

1. Read title, abstract and conclusions of the publication. If it turns out that the publication does not meet the inclusion criteria, then it must be labelled as such under the proper column in the spreadsheet, and discarded.
2. Screen the abstract and conclusions of the publication to spot findings that are relevant to answer the research question and sub-questions. If so, then proceed to highlight said findings, reviewing different sections when relevant.
3. Copy all the relevant findings (already highlighted) to the spreadsheet, categorising them under the best suited theme. Some comments can belong to more than one theme, in which case they are copied to both or them. In this step, it is also relevant to summarise, scrapping not-relevant information when possible. Other comments from the reviewer can also be left under the relevant columns in the spreadsheet.
4. When the publication is finished with, then it must be labelled as "Read" under the proper section in the spreadsheet, and jumping to the next publication.

During each iteration the validity and suitability of the themes in the spreadsheet must also be assessed, especially at the beginning of the review and synthesis process. If considered that it could improve the review process, those themes and their definitions could be adjusted, as well as new themes added, with the offset of having to check whether the previously written findings are still labelled under the right theme.

2.6 Reporting and using the results

The final step consists on reporting the results of the literature review, where an overview and discussion of the findings is provided (Durach et al. 2017).

Once all the findings are inputted into the spreadsheet (previous step), it is possible to sort all the publications by different categories, like themes or year. This functionality is used to provide a general overview of each theme, helping in the process of summarising and structuring the findings from each one, as well as in linking those themes together into a framework that makes sense of the body of knowledge found through the SLR steps.

Those findings that help in answering the research question and sub-questions are presented in the next sections of this thesis, proceeded by an analysis in which a framework will be proposed as part of another attempt in answering the research question. Then the implications of this work in regards to theory and practice will be discussed, finalising with the conclusions resulting of this thesis, and future work.

3 Results

In this section, the results from the literature review and synthesis are presented. The main explicit goal is to answer research sub-questions RQ1.1 and RQ1.2, and doing so by presenting what are the supply chain-related risks found to be associated to the use of IT systems, as well as by presenting the constructs, tools and practices found in the literature that could be used for the management of those risks.

First, the results of the SLR process up until the review process (steps 1 to 5) are summarised and presented, aiming to provide more clarity and transparency to the process followed and the findings obtained, which should also strengthen the argument of replicability of this work. Then, a subsection will be provided to clarify the meaning of the terminology used in this thesis with respect to the topic of study. Finally, the qualitative findings from the literature review process, separated into themes, will be presented in the subsequent subsections.

In order to structure the findings that answer our research question and sub-questions, a dynamic approach is followed, taking as a point of reference in time the occurrence of a risk-event, which allows for the identification of three moments in time, namely *before*, *during*, and *post* risk-event. This is further explained in section 3.3.

3.1 Summary of results from the literature review process

In this section, an account of the results obtained after following the steps of the defined SLR process are presented.

- Retrieving the Baseline Sample -

As explained before, each of the eight combinations of the key defined terms are used in the process of searching for publications in the two selected search engines (Scopus and DTU Findit). The number of unique publications from each search in each search engine, and the total numbers, are shown in figure 2. Moreover, the histogram on figure 3 shows the year of publication of each search result in the final sample. As it can be seen, the shape of the histogram clearly indicates a correlation with an exponential trend in the growth of the publications associated to the search terms, that spans almost two decades, highlighting the continued growing academic interest and attention associated to those terms. Year 2018 only shows results up until February.

Search	Number of publications		Search query
	Scopus	DTU Findit	
A	237	120	supply chain, cyber, risk management
B	69	52	"supply chain", resilience, cyber
C	54	31	"supply chain", cyber risk, resilience
D	304	269	"supply chain", cyber security
E	103	103	"supply chain", "information technology", cyber security
F	74	41	"supply chain", "information technology", cyber security, risk management
G	261	111	"supply chain", "information technology", resilience, risk management
H	328	71	"supply chain", "information technology", resilience
Unique results	**706**	**417**	**Total unique results** **897**

Figure 2: Summary of the search results from Scopus and DTU Findit databases

- Selecting the Pertinent Literature from the Sample -

After retrieving the baseline sample and structuring it into a single spreadsheet, all the titles and abstracts are screened to determine which are the ones that meet the inclusion criteria. As explained before, the outcome of this process is the obtention of three groups of publications, labelled as "Include", "Maybe" and "Clearly excluded" in relation to whether they meet the inclusion criteria or not. A summary of the results of this process can be seen on table 1.

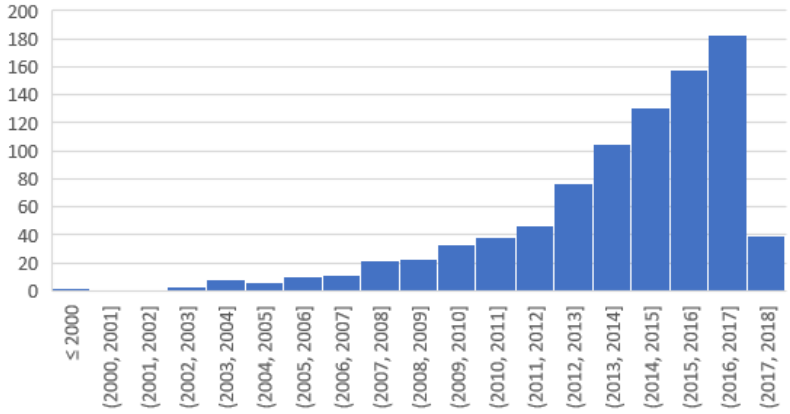

Figure 3: Year of the publications in the baseline sample

Table 1: Results from the screening of the sample

Initial sample	897
Included	181
Maybe	304
Excluded	412

As explained before in the Methodology (section 2.4), the group initially labelled as "Maybe" was re-labelled after the first group of publications ("Include") was reviewed. As a result, 103 out of the 304 publications labelled as "Maybe" were re-labelled as "Include".

However, there was not enough time left to take those publications through the synthesis process, and they were not reviewed. It is believed that this was most probably a consequence of the size of the initial sample (897 search results), which did not allow for a full review of all the sample with the available time resources.

- Synthesising the literature -

As also explained before, a very important part of the methodology defined is the identification of the terms that best encompass the findings from the literature review process.

This starts with the identification of terms that seem to recursively appear in the titles and abstracts, while they are being read. In our case, this led to the creation of an initial "cloud of terms" that can be seen in figure 4.

Counterfeits	preparedness	ambidexterity
e-supply chain	alertness	information management
forensic	capability	insurance
dynamic capability	robustness	governance
security	risk management	IP
cyber-security	mitigation	RFID
resilience	risk identification	Blockchain
supply chain	risk assessment	Hardware
strategy	prevention	IC (Integrated Circuit)
operational	network	Microprocessors
disruption	IoT	CPS (Cyber-Phys.-Syst.)
policy	Industry 4.0	Hardware Trojan
legislation	Big Data	Cyber attacks
Obfuscation	Authentication protocol	

Figure 4: Cloud of terms from the first screening

This figure, nonetheless, must be taken "with a pinch of salt". The focus is on the identification of terms not thought before by the reviewer, and the inclusion of them in the first list of themes in the spreadsheet is based on the subjective perception of the reviewer on whether or not they

could be relevant to codify the findings later on the process. Therefore, it must not be understood as a full list of the most important themes found in the field of study. Whether they are actually relevant or not, is seen later on the process, as some of those terms are also found in literature that does not meet the inclusion criteria.

The first list of themes used in the spreadsheet was decided through a process that takes input from the previous experience of the reviewer, the cloud of terms previously depicted and individual brainstorming. The resulting list of themes is shown on figure 5, while a section of the resulting initial spreadsheet can be seen on figure 6.

Theme	Sub-themes
Downloaded (-), read (x)	
Other/unclassified	
Focus on a specific product / industry / supply chain	
Operational vs strategic	
Risk identification	Threat/ source identification
	Vulnerability
	Risk id.
Risk assessment	
Governance	General findings
	Investment
	Procedures and rules for making decisions
	Distribution of rights and responsibilities
	Policies
	Standardisation and codification

Theme	Sub-themes
(Risk) Avoidance/ Prevention / Defense	General findings
	Cyber security
(Risk) Mitigation / Reduction	General findings
	Resilience
	Capability
	Flexibility, Velocity, Visibility, and Collaboration + Redundancy, Agility
	Readiness, Responsiveness, and Recovery
(Risk) Sharing/ Transferal	General findings
	Insurance
(Risk) Acceptance/ Retention	
(Risk) Termination	
Compliance	General findings
	Standards/Regulations mentioned

Figure 5: Initial themes defined

L	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR
	(Risk) Sharing/ Transferal		(Risk) Acceptance/ Retention	(Risk) Termination	Compliance		Governance			
Full title	General	Insurance			General	Standards/Regulations mentioned	General	Investment	Procedures and rules for making	Distribution of rights and responsibiliti
Design considerations for building distributed supply										
Design for hardware trust										
Designing security policies for complex SCADA systen										
Development of a supply chain management security										
Disaster and risk conference IDRC davos 2014: Insurab										
Economic costs of firm-level information infrastructur										
Economic impacts of cyber security in energy sector: A										
Embedded reconfigurable logic for ASIC design obfus										
Emergent risks In critical infrastructures										
Enabling better supply chain decisions through a gene										

Figure 6: A section of the initial spreadsheet template used for collecting findings from publications

During the review and synthesis process, this list was dynamically adapted, to better fit the findings from the different publications. The final list of themes and sub-themes can be seen in figure 7, while a section of the spreadsheet can be seen in figure 8, to give an idea of its final outlook.

In total, 181 publications made it to this step of the SLR. Of those 181, 44 were not obtainable (for technical reasons or because of the need of a paid license), leaving a total of 137 publications screened. From those 137 publications screened, 21 were excluded due to not meeting the inclusion criteria, which could not be spotted from only reading their titles and abstracts (i.e. the ambiguity of the terminology used in the first place led to a "false-positive", or the publication did not have a scientific article-like style). Moreover, 7 publications were added from cross-references and hand search, adding up to the total of 123 publications reviewed.

As mentioned before, due to lack of time, it was not possible to review and synthesise the second group of 103 publications from the sample, obtained from the group of publications initially labelled as "maybe" meeting the inclusion criteria. The second group of publications account for the 39.2% of the publications labelled as "Included" at the end of the process, while the literature reviewed from the first group (137 publications) account for the 44.1%. They do not add up to a 100%

Theme	Sub-themes
Other comments / findings	
Focus on a specific product / industry / supply chain	
Risk identification	Threat/ source identification
	Vulnerability
	Risk id.
Risk assessment	
General risk treatment	
Resilience	General comments
	Capability
Pre-disruption (readiness)	Readiness, anticipate, avoidance
	Situation Awareness, Robustness, KM (pre)
	Security, Visibility
During disruption (responsiveness)	General comments
	Adapt (flexibility, redundancy)
	Respond (collaboration, agility)

Theme	Sub-themes
Post-disruption (recovery)	General comments
	Contingency planning, market position
	Learn, KM (post), building social capital
(Risk) Sharing/ Transferal	General comments
	Insurance
Compliance	General comments
	Standards/Regulations mentioned
Governance	General comments
	Investment / budget
	Structural component - Distribution of rights and responsibilities
	Relational component
(Governance) Process component	Standardisation and codification
	Policies
	Procedures and rules for making decisions

Figure 7: Themes as finally used in the review spreadsheet

L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA
	Downloaded (-), read (x)							Other comments	Focus on a	Risk identification			Risk assessment	General risk treatment	Resilience
Full title		Abstract	Author	Year	Where	Grade	Revised grade		(expl	Threat/ source identification	Vulnerability (SCV)	Risk id.			General
When Intrusion Detection M	x	With the purpose of	Meng	2018	Both	1			blockchain						
A Comprehensive Assessmer	x	International busine	Häyhti	2017	Both	1		"Critical in	critic	Current global t	Because a su	All of the orga	Each of the five components is subject to v		
A supply chain network game	x	In this paper, we de	Naguri	2017	Scopus	1			investments		vulnerability				
A system dynamics case stud	x	Undesirable change	Sepúlv	2017	DTUfindi	1									This paper u
Adapting supply chain manag	x	The purpose of this	Urciuo	2017	Scopus	1		"As this study re		"Respondents p	Previous research has indic		Data collected	Previous studie	
An information security risk	x	Internet of Things (I	Sohrab	2017	Scopus	1		Difficut to understand. Problem					An information security assess		
Analysing supply chain resili	x	Purpose: The purpo	Ali A.,	2017	Both	1		The categories of SC resilience in							What are the
Blockchain's roles in strength	x	This paper evaluate	Kshetr	2017	Both	1		This article	Blockchain, applied to						
Business Resilience System (	x	This book provides a	Zohuri	2017	Both	1	3	BOOK							
Can Blockchain Strengthen th	x	This column evaluat	Kshetr	2017	Both	1		Very simil	Blockchain, applied to						

Figure 8: A section of the spreadsheet used for collecting findings from publications, at the end of the process

because 44 publications from the first group (16.7% of the total) were not accessible.

A summary of the SLR process up to this point is depicted in figure 9. It took approximately 2.5 months to go from the first step of the SLR to the end this last step, in which the review of the first group of publications was finished. This meant that there were only 1.5 months left, which were decide to be spent on the analysis of the data and writing of this document.

Moreover, figure 10 provides a summary of the number of publications from each search result that met the inclusion criteria. Please note, the numbers in this last figure include, on one side, the publications initially labelled as meeting the inclusion criteria ("Include"), whether they were accessible or not, minus the ones excluded later in the review process. On the other side, it also considers the publications relabelled as "Include" from the "Maybe" group, although it should be expected that a relatively small number of them may turn out not compliant with the inclusion criteria in the end. The seven publications brought in from cross-references are not considered in those statistics either.

From the data shown in figure 10, some interesting conclusions can be drawn. Firstly, in can be seen that, for every search, Scopus has provided more publications that meet the inclusion criteria than DTU Findit - 214 against 186, which is 15% more publications. However, DTU Findit had a better success rate (47% against 31%) when compared to the total of publications returned. Nonehteless, on table 2 it can be seen that DTU Findit provided 24% of the unique results included, and Scopus a 32%. Therefore, the fact that Scopus returns more results than DTU Findit does not mean that it can completely substitute it. At some extent, these two search engines complement each other.

Table 2: Search engine where the publications meeting the inclusion criteria were found

Found via	**Publications**	**%**
Only DTU Findit	64	24%
Only Scopus	83	32%
Both	116	44%

Moreover, it could also be observed that the publications in the field of SCCRM are fairly scattered, source-wise. As it can be seen on table 3, the top six journals with most publications in the area held between 3 and 9 publications each, while all the other 233 publications did not seem to correlate with the same scientific journal more than twice in the whole set. As the journal with most publications in this area concentrated just 3.4% of the publications, this seems to indicate that there is not any journal of reference in the area of study.

Finally, figure 11 shows the year of each publication labelled as meeting the inclusion criteria. This histogram also seems to visually correlate with an exponential growth. Moreover, represented in a numeric way, table 4 shows that the number of yearly publications in the area of SCCRM has doubled every 2 or 3 years since the year 2000, which is the oldest result. All this, points to a very obviously-accentuated increase of academic interest in this area over the past two decades, which seems to still be exponentially growing. Tables listing the publications contained in each group are shown on Appendix A.

Table 3: Publications per journal

Journal	**Publications meeting inclusion criteria**
Technovation	9
CrossTalk	8
Computer Fraud and Security	4
Communications in Computer and Information Science	3
Computer	3
Computers and Security	3
Other sources	233

Table 4: Publications meeting inclusion criteria, per year

Year	**Publications**	**Cumulative**	**%Cumulative**
2000	1	1	0%
2001	1	2	1%
2002	0	2	1%
2003	0	2	1%
2004	3	5	2%
2005	3	8	3%
2006	4	12	5%
2007	5	17	6%
2008	2	19	7%
2009	8	27	10%
2010	6	33	13%
2011	11	44	17%
2012	16	60	23%
2013	23	83	32%
2014	38	121	46%
2015	38	159	61%
2016	44	203	77%
2017	50	253	97%
2018	9	262	100%

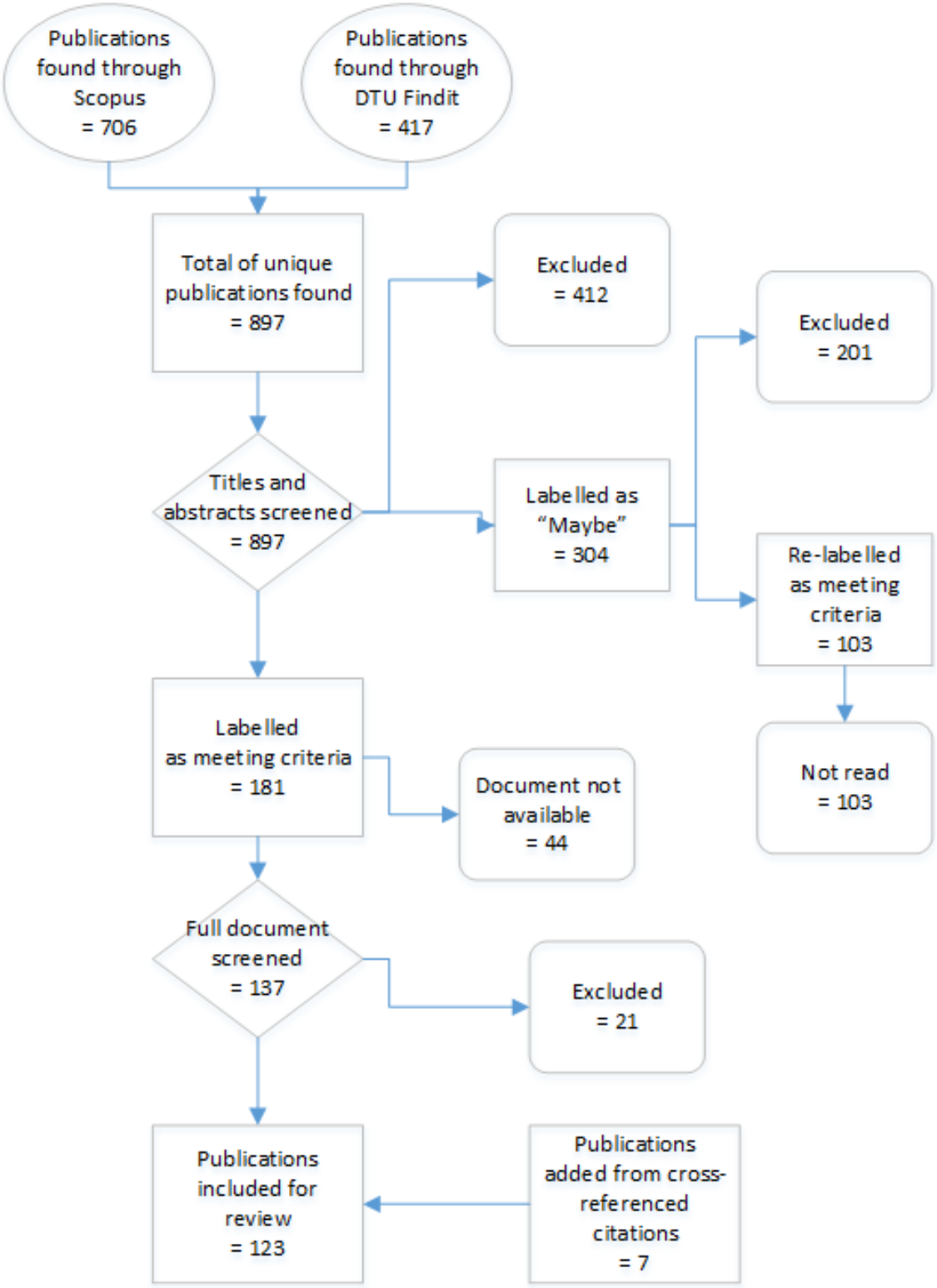

Figure 9: Flowchart summarising the results of the SLR until the review

		Scopus			DTU Findit			Both search engines		
	Search string	**Search results**	**Meet criteria**	**Success rate**	**Search results**	**Meet criteria**	**Success rate**	**Unique Search results**	**Meet criteria**	**Success rate**
A	supply chain, cyber, risk management	241	107	44%	115	76	66%	277	122	44%
B	"supply chain", resilience, cyber	70	39	56%	48	34	71%	89	50	56%
C	"supply chain", cyber risk, resilience	54	32	59%	31	23	74%	65	38	58%
D	"supply chain", cyber security	317	189	60%	245	152	62%	394	219	56%
E	"supply chain", "information technology", cyber security	110	67	61%	100	60	60%	130	73	56%
F	"supply chain", "information technology", cyber security, risk management	75	51	68%	39	31	79%	85	54	64%
G	"supply chain", "information technology", resilience, risk management	261	29	11%	107	23	21%	336	37	11%
H	"supply chain", "information technology", resilience	328	32	10%	64	14	22%	358	36	10%
	The eight search strings combined	**691**	**214**	**31%**	**395**	**186**	**47%**	**897**	**263**	**29%**

Figure 10: Successful results and success rate of search terms

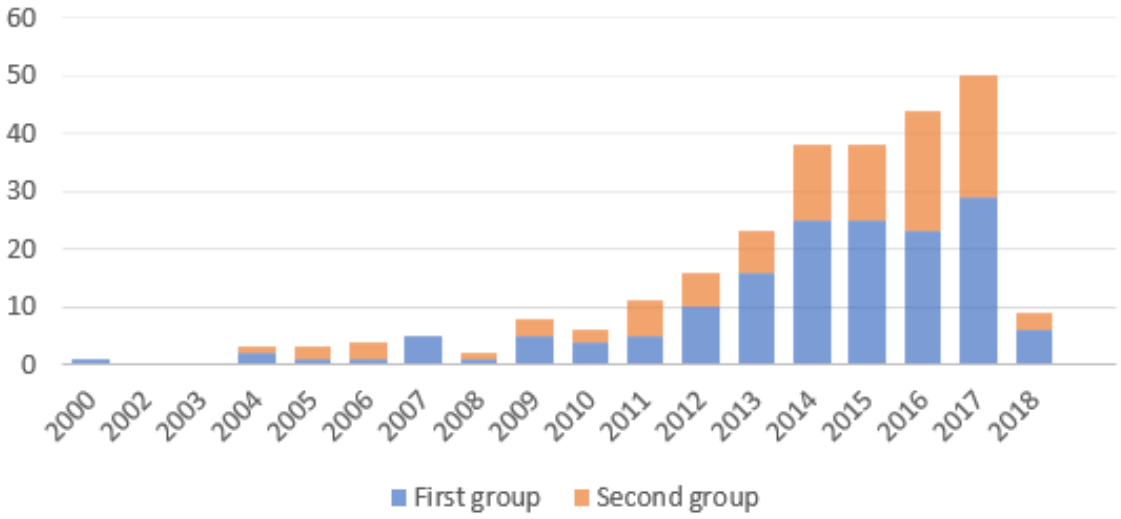

Figure 11: Histogram of publications meeting inclusion criteria, per year

3.2 Remarks on the Terminology

Some of the most basic issues encountered while reviewing the literature was the language used. Different terminology seems to be used across the area of management of IT risks in the supply chain. Moreover, much of the terminology used is similar across different fields and although they may have different connotations, in occasions they are used interchangeably which can add to the confusion.

One of those points of confusion is the use of terms like "Cyber" and "IT" (Information Technology). For example, Smith et al. (2007) refers to "IT-enabled supply chains" as supply chains where IT systems are used, while Bartol (2014) uses the term "cyber supply chain", with very subtle differences that are not easily identifiable to readers as they are not usually described in other publications.

Gaudenzi & Siciliano (2018) also highlight this issue, pointing out different existing approaches towards understanding "IT" and "Cyber". IT can be understood as the foundation for the Cyberspace, while other approaches point at IT as mere infrastructure, and then defining hardware, software and data as "Cyber assets". This way, they define IT risks as "strictly technical", while cyber risks go well beyond IT disruptions, by including human variables (like their behaviour and goals) into its scope. As a result, they always keep IT risks and Cyber risks as two separate issues. However, this same distinction is not made in the rest of the literature.

As it has been perceived from the literature reviewed, both of those terms are very closely linked, and it is seen that IT and cyber aspects are sometimes difficult to keep separated. Therefore, for the sake of simplicity, in this thesis the use of the term "*Cyber Risk*" encompasses both IT risks and cyber risks, unless stated otherwise.

Another conflicting point of understanding in the literature comes when referring to this field of study. In order to manage cyber risks in the supply chain, Khan & Estay (2015) coin the term "Supply Chain Cyber-Resilience", which is described as the meeting point of three main bodies of knowledge, which are: information technology management, supply chain management, and risk and resilience management. Boyson (2014) uses the term "Cyber Supply Chain Risk Management". Moreover, Bartol (2014) also lists a number of other terms that have been found used to refer to this field over the years, like "Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM)", "Information and Communication Technology (ICT) supply chain security".

Because of this lack of consensus in the literature, there is no single-valid way of referring to this topic. Therefore, it has been decided to use the term "*Cyber Supply Chain Risk Management*" (also *SCCRM*) across this thesis, as was also seen in Khan & Estay (2015), which must not be understood uniquely as risk management in supply chains dealing with the supply of cyber and IT products, but also IT-enabled supply chains and supply chains that can be affected by cyber risks in general.

It is also understood that SCCRM can and will draw knowledge from the areas of Risk Management, IT Management and Supply Chain Management, as defined by Khan & Estay (2015), and any of their sub-fields. For example, different risk management approaches and techniques, like resilience, can subsequently be included in this field. Cybersecurity and the branch of Information Security dealing with information risks stemming from IT and cyber aspects are also considered.

It must be noted that those aspects are not the only ones where terminology can be ambiguous in the literature. So, the following terms are also defined, in the area of risk management:

- *Risk:* according to the Cambridge Dictionary (Cambridge-Dictionary 2018), *risk* is defined as *the possibility of something bad happening.* Linked to this term, there is the *likelihood* of it succeeding, and the *impacts* to the system (Smith et al. 2007).
- *Threat:* it is also understood as the *source* or *cause* of the risk (Smith et al. 2007).
- *Vulnerability:* threats can lead to a risk when combined with vulnerabilities. Vulnerabilities are defined as a weakness of a resource or an asset which can be exploited by threats (ISO/IEC 2011).

- *Event:* it refers to the realisation of a risk. In the literature, in can be found that other terms may adopt this same meaning. Examples in the field of IT are *breaches* or cyber-events (Dedeke 2017).
- *Impact:* it refers to the effects that the realisation of the risk have on the system (Smith et al. 2007).

Moreover, as Smith et al. (2007) point out, many taxonomies fail to make a distinction between causes and effects (threats and impacts). This is also linked to the attribution of the terms *causes* and *effects* on a certain event, which depends on the relative point of reference, as certain impacts of a risk can be seen as a source for another risk. This must be taken into consideration.

3.3 Dynamic Approach

As it was explained before, the approach followed to structure the findings from the literature was the use of themes that were dynamically changed and adapted, to ensure a better fit for to the data gathered at the end of the process. One of the implicit outcomes of this process is the identification of a taxonomy that could encompass the most important bodies of knowledge contained in the field of supply chain cyber risk management, which would be instrumental in answering the main research question and sub-questions.

As a consequence, it is identified that, by taking a dynamic approach, it is possible to better classify the information gathered and differentiate between the different themes. A dynamic approach, as it is understood here, considers time as the main variable of study.

In this case, the realisation of a hypothetical cyber-related risk event is taken as our point of reference in time, and findings from the literature are clustered and presented as belonging to a moment in time *before*, *during* or *post* (after) the realisation of this hypothetical risk event.

In the literature, it can also be seen that other authors use similar approaches, especially in the area of supply chain resilience. Herrera & Janczewski (2015) and Ali et al. (2017) present frameworks where the different elements shown belong to one of the three stages in a disruption event: pre-disruption, during-disruption and post-disruption. Said division in time can also be observed through other triads of terms, like *proactive, concurrent and reactive strategies*, *readiness, responsiveness and recovery/growth*, and *protection, response and adaptation* (Herrera & Janczewski 2016, Ali et al. 2017).

Those three main phases are further described next, which also serves as an introduction to the other themes present in the Results section of this thesis.

3.3.1 Pre- Risk Event

This pre-event situation has also received the name of *pre-disruption phase* in the literature (Hosseini & Barker 2016, Ali et al. 2017), and is also associated to the concepts of *readiness* (Axelrod 2014, Radke & Tseng 2015), *protection* (Herrera & Janczewski 2016) and *proactive strategies* (Boyson 2014, Osborn & Simpson 2017).

In this phase, Ali et al. (2017) define as critical the *ability to anticipate* risks, through both identification and monitoring of risks. According to them, there are five core elements associated to anticipating the risks: situation awareness, robustness, knowledge management, security and visibility. Herrera & Janczewski (2016) use a somewhat similar terminology, identifying a number of mechanisms for coordination, namely situational awareness, architectural, vulnerability assessment, and visibility. Nonetheless, from the literature review findings, it is believed that other aspects are also relevant to this phase, which were not explicitly described by the aforementioned authors, like compliance and governance.

As a consequence, findings from the pre-risk event phase are grouped into the following areas, which will be further described and discussed in subsequent sections: *compliance*, *situation awareness*, *governance*, *pre-event knowledge management*, *cyber security* and *visibility*.

3.3.2 During- Risk Event

Striving during a disruption is closely linked to being *responsive* (Herrera & Janczewski 2015, Ali et al. 2017). The themes used to refer to this phase are the *ability to adapt*, as well as *velocity*, which is described as a sub-component of supply chain agility, together with visibility. This taxonomy is very similar to the one described by Ali et al. (2017).

3.3.3 Post - Risk Event

Long-term survival, in the post-disruption stage, is associated to the ability to recover from a risk event, so to return to the normal state of operations, and the ability to learn and grow from it, which allows to understand past events and improve future performance (Ali et al. 2017).

To present the findings in this aspect, similar terminology is used, namely *recovery* and *growth*. On one side the ability to recover is covered by two themes: *recovery management* and *market position and financial strength*, while on the other the ability to grow is encompassed by *post-event knowledge management* and *social capital*.

3.4 Compliance

In the context of supply chain cyber risk management, risk compliance can be understood as to identifying and conforming to the legislation affecting this field and the standards that must be met (Gaudenzi & Siciliano 2018). It must be noted, here we understand legislation as the set of regulations that must be met according to the applicable laws, while standards can be understood as the minimum-expected from good practice in the area, which could be required to comply to by legislation. The most widely recognised standards are often overseen by international bodies, like ISO/IEC (2011).

In the literature, compliance is regarded as relevant for the management of these risks (Johnson 2015, Gaudenzi & Siciliano 2018). On one side, it has been suggested that compliance feeds into the process of risk assessment, through the obligation of meeting legislation or the conformation to security standards (Roy & Kundu 2012, Gaudenzi & Siciliano 2018).

However, it has also been reported that there is a lack of expertise in cyber security or forensic engineering in many government agencies, leading to the fact that many regulations often lag behind the faster advancements on technology, not providing the most appropriate guidance on the acceptable means of compliance (Johnson 2015). Therefore, it can be observed that compliance to standards has been much more discussed in the field of SCCRM than compliance to national regulations (Bartol 2014).

To illustrate Dedeke (2017) uses the terms "Compliance-Oriented Cybersecurity" and compares it to "Risk-Oriented Cybersecurity", to argue that the first one does not offer "adequate cybersecurity protection". The Compliance-Oriented approach is criticised because compliance is often perceived as a cost of doing business and adopters of this approach are more "likely to deploy the minimum number of controls required" when seeking for certification (Dedeke 2017). Companies that adopt a Risk-Oriented approach to cybersecurity, on the other hand, focus on ensuring that their internal and external processes can resist emerging external threats, and are more likely to implement not only baseline controls, but also controls that are needed to help the organisation reduce other emerging threats.

Despite this, standards could inherently provide advice on best practices, and guide the actions of different organisations to make better informed decisions and this way protect their supply chains (Johnson 2015). So, it has been observed across the literature reviewed that different international standards have been widely referenced to, and their implementation also discussed. More generally, Bartol (2014) gives an overview in the evolution of the standards and practices in the area of cyber supply chain security, and listing different general requirements, and "essential security and foundational practices", tools and techniques.

In general, the international standards that have been found to be (by far) the most mentioned are the ISO 27000 series of standards, from ISO/IEC (2011). This family of standards is related to information management systems, and at least eleven of the publications reviewed mention it. The second most referenced standards were from the NIST (National Institure of Standards and Technology), like the NIST SP800-30 which is intended for conducting risk assessments of information systems (NIST 2012), mentioned by at least four publications. The publications found to mention those standards are referenced on table 5.

Table 5: Publications mentioning the ISO 27000 and NIST SP 800-30 standards

ISO 27000 family of standards	Murphy & Murphy (2013), Shankles et al. (2013), Patnayakuni & Patnayakuni (2014), Bartol (2014), Finnegan & McCaffery (2014), Caldwell (2015), Ab Rahman et al. (2016), Polemi & Papastergiou (2016), Barreto et al. (2017), Safa et al. (2017*b*), Polatidis et al. (2018)
NIST SP 800-30 standards	Finnegan & McCaffery (2014), Polemi & Papastergiou (2016), Barreto et al. (2017), Polatidis et al. (2018)

3.5 Situation awareness

In this section, methods and frameworks found to be used for identifying supply chain cyber risks are described, together with the threat sources, vulnerabilities and risks found to be highlighted in the literature.

For this, findings from the literature review are structured to first introduce the risks associated to the use of IT in more generic supply chains, as well as the sources of threat that can lead to them and how to assess them.

Then, the same concepts are reviewed for the specific areas which are found to have attracted more research interest. As a result of the literature review, a number of industries or areas were found to have attracted more attention in the academic field of cyber supply chain risk management. Those findings are grouped in the following sections: the Industry 4.0, the supply chain of electronic products, the software supply chain, and critical infrastructure sectors. In their respective sections, those areas are presented, together with the findings regarding risk identification and assessment practices in each one.

3.5.1 Risk identification

When it comes to identifying the cyber risks affecting supply chains, various methodologies can be found in the literature. Although they may differ from each other depending on the context in which they are proposed, many of those methodologies share some common points. For example, Smith et al. (2007), Urciuoli et al. (2013) and Boyes (2015) point out to interactions between threats to and vulnerabilities in IT systems to identify cyber risks in the supply chain. Their methodologies differ basically on what threats and vulnerabilities are highlighted, as well as the way those aspects are categorised. The framework presented by Boyes (2015) is shown below, in figure 12.

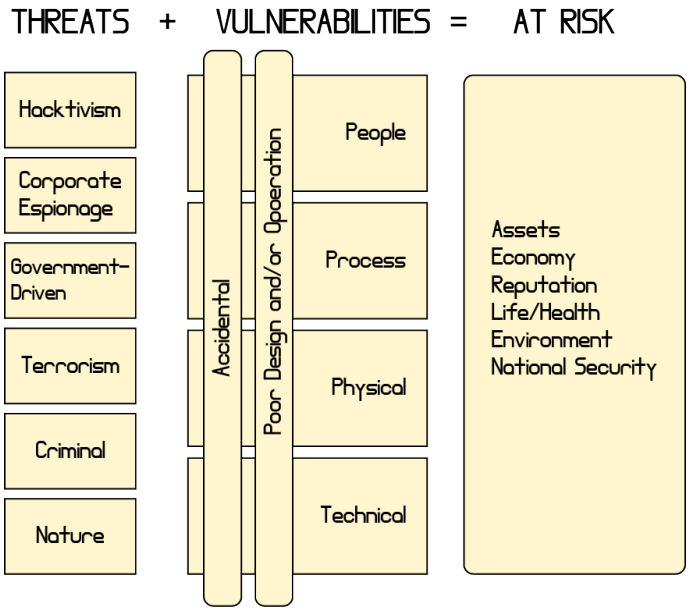

Figure 12: Threats and vulnerabilities that affect cyber-resilience. Adapted from Boyes (2015)

When it comes to identifying the threats, Smith et al. (2007) list seven categories of potential threats to IT resources, categorised in *Malicious Code and Programs*, *Malicious Hacking* and *Intrusion Attempts*, *Fraud and Deception*, *Misuse and Sabotage*, *Errors and Omissions*, and *Physical and Environmental Hazards*. Boyes (2015) depicts six categories of threats that affect the supply chain from a cyber-resilience point of view: *Hacktivism*, *Corporate Espionage*, *Government-driven*, *Terrorism*, *Criminal* and *Nature*. Urciuoli et al. (2013), on the other hand, try to combine possible cybersecurity threats (clustered as *Access to confidential information*, *Control over computer systems*, and *Communication*) with typical supply chain security threats (*Cargo crime*, *Smuggling*,

Counterfeiting, and *Sabotage*), while answering the question "How does cyber-crime support offline supply chain crime?".

Vulnerabilities, on the other hand, could be exploited by threats to cause damage to both enterprise and communities (Urciuoli et al. 2013). Hutchins et al. (2015) propose a framework to identify generic and manufacturing-specific vulnerabilities, by taking into account the data flows within a manufacturing enterprise and throughout the supply chain. In a similar way, Estay & Khan (2016) propose a way of representing the flow of information on a supply chain, which could also be used for identifying vulnerabilities. It includes agents interacting in the supply system, communication paths and feedback loops.

Filippini & Silva (2015) report on the use of a modelling language (I-ML) that could be used for identifying structural and dynamic vulnerabilities and criticalities. This is done through modelling operational inter-dependencies among elements of the infrastructure, considering both technical and socio-technical elements in the organisation. Boyes (2015) also points out to the need of a holistic approach to security, concluding that purely technical solutions will not likely cover the breadth of potential threats and vulnerabilities. Therefore, he suggests that vulnerabilities that affect cyber-resilience can be related to any of the following four aspects: *people*, *processes*, *physical* and *technical*, while being *accidental* in nature, or due to *poor design and/or operation*. Safa et al. (2017*b*) follow a similar perspective, emphasising *people, technology and processes* as the main entities in information security. When it comes to information security, for example, Safa et al. (2017*b*) defend that breaches may be caused by *people* elements like the movement of employees, dissatisfied staff, the use of temporary experts and the lack of awareness regarding organisational information security policies, while Boyson (2014) points at the "insider threat". Others, like Boyes (2015), relate to vulnerabilities in "the cloud", cloud services and the global navigation satellite systems (GNSS), as well as vulnerabilities derived from the dependence on those technologies.

In general, Reddy (2014) defends the importance of using a framework for mapping IT component vulnerabilities and communicating those vulnerabilities along the supply chain in a meaningful manner, so that it can also assist SC partner's vulnerability assessments.

As seen in figure 12, the interaction between threats and vulnerabilities will translate into elements at risk, which can then be identified. Those elements could be related to *assets*, *economy*, *reputation*, *life/health*, *environment* or *national security* (Boyes 2015). Torabi et al. (2016), referring to disruption risks, provides lists with identified "potential disruption risks" (which could be Natural, Environmental, Technological or Man-Made) as well as "potential operational risks" (related to Supplier risks, Internal risks, Environmental risks, and Market risks). Another tool could be used for identifying information security-related risks, in this case by looking at the Confidentiality, Integrity and Availability of information, namely "CIA triad" (Boyes 2015). Chabinsky (2014), from a cybersecurity perspective, suggests the combination of three dimensions with three elements each, in which all of them resonate with the frameworks mentioned in this section:

1. Threats, Vulnerabilities and Consequences
2. Confidentiality, Integrity and Availability
3. Insider, Proximate, Remote and Supply Chain

Finally, it is important to involve a multidisciplinary team in the risk identification process (Dynes 2006), which in this case should include members and leaders of the supply chain management, risk management and IT management of the firm (Khan & Estay 2015).

3.5.2 Assessment of Cyber Risks

As mentioned before, risks are conceptually linked to the likelihood of succeeding and the impact that they may cause, in many occasions being referred to as the product of both factors (Smith et al. 2007). The process of risks assessment is generally understood as one in which those parameters of likelihood and impact are determined either qualitatively or quantitatively for the identified risks.

Hale et al. (2004) follow a very similar approach in their "susceptibility audit", in which the likelihood of a successful attack is measured against the cost of it being successful. Torabi et al.

(2016), on the other hand, propose what they call "an enhanced Risk Assessment framework", consisting of the steps of *identification*, *risk analysis*, *risk evaluation* and *risk response planning*. Their framework is intended to be applied in the context of implementing a business continuity management system (BCMS), and not necessarily an IT-enabled supply chain, but they mention the disruptive potential of cyber-attacks as a context in which it could be applied.

In support of this, Smith et al. (2007) and Bandyopadhyay et al. (2010) defend that, while IT-enabled supply chains tend to increase the level of integration, the offset is that highly integrated supply chains are at a greater risk when it comes to security incidents, compared to less integrated supply chains. Smith et al. (2007) emphasises the rise in the amount of information exchange, while Bandyopadhyay et al. (2010) argue that network incentives lead to a level of investment in security that is by default less than the socially optimal.

In general, from the literature review it is noted that there is a lack of empirical data provided by previous studies, regarding Cyber risks in supply chains. In this regard, Urciuoli & Hintsa (2017) highlight how little evidence there is regarding risks of cyber-crime in supply chains. Nonetheless, it can be seen that most of the research in this aspect has been on the impacts of the risks, rather than on the likelihood component, at least in the literature reviewed.

Smith et al. argued in 2007 that a true financial accounting for the consequences of an IT security incident was "beyond the capabilities of both practitioners and academicians" at that time, and the situation does not seem to have changed much. Torabi et al. (2016) recommend to use the deviation from certain pre-defined organisation's goals (i.e. financial goals) as a measurement. Durowoju et al. (2012) suggest the use of entropy theory in "assessing the emergent impact of the threats in information systems", by means of an "entropy score". Khan & Estay (2015) argue for including recovery costs when evaluating cyber-attacks. Nonetheless, so far most empirical quantitative data seems to be found on independent reports, like PWC (2017), WEF (2017) or McAfee (2014) as examples.

Alternatively, other frameworks and methodologies have been proposed to assess risks in a more qualitative way. Bodeau et al. (2010) propose the Cyber Preparedness methodology, which aims to characterise the level of cyber threats that an organisation may face depending on the threat-actor involved. According to this framework, different levels are defined corresponding to different "break points in adversary capabilities, intent and technical sophistication". Those levels are: *Cyber Vandalism*, *Cyber Theft/Crime*, *Cyber Incursion/Surveillance*, *Cyber Sabotage/Espionage*, and *Cyber Conflict/Warfare*). A similar approach is followed by Demchak (2012), who defines four "levels of surprise in cyberspace".

3.5.3 Industry 4.0

The term Industrial Internet of Things (IIoT) is often closely associated to the fourth industrial revolution, or Industry 4.0 (Barreto et al. 2017). Industry 4.0 fosters the use of digitalisation and the Internet in industrial settings, transforming processes, operations and services with the integration of innovative developments from areas like big data, IoT and Artificial Intelligence (AI) (Tjahjono et al. 2017).

However, there are a number of threats associated to digitalisation, especially in the context of Industry 4.0. In this regard, Pan et al. (2017) present a taxonomy for classifying cyber-physical attacks targeted against IoT-based manufacturing processes. They classify those attacks into three categories, which make use of the information security "CIA triad":

- Confidentiality attacks (compromising intellectual property and confidential data)
- Integrity attacks (tampering with design models and configuration files)
- Availability attacks (affecting the availability of manufacturing resources)

Even though the cloud allows for remote monitoring and analysis, linking production facilities to the Internet gives room to vulnerabilities in security (Preuveneers et al. 2017). Lee & Kwon (2016) refer to the software update traffic as a point especially vulnerable in the IoT context, as

attackers could compromise "easily" unattended devices. In regards to the sensors supply chain, Alam et al. (2017) refer to vulnerabilities as a consequence of large-scale deployment of sensors, as this "demands simplification of associated hardware for cost minimisation". At the same time, they highlight trust issues stemming from present vulnerabilities, discussing about piracy, reverse engineering, recycling of circuitry, and physical attacks.

In order to identify the risks involved in a "smart" (or IoT-enabled) supply chain, Safa et al. (2017*a*) make use of a framework based on threat, environment, asset and vulnerability identification. Subsequently, every risk description is elaborated based on the previous four elements and a risk score and recovery activities.

3.5.4 Supply Chains of Electronic Products

The supply chains of physical electronic products, or hardware (as opposed to software), has attracted significant attention from the research community.

In general, not only producers of electronic products could face risks originated upstream and downstream their supply chains (Goertzel 2013), but also any enterprise making use of products or technology containing electronic elements, like integrated circuits (ICs) (McFadden & Arnold 2010). Among the risks involved, there is attackers extracting intellectual property (IP) and discovering sensitive data, theft and sabotage, both of ICs and the processes that depend on them (McFadden & Arnold 2010, Goertzel 2013).

Hardware itself is vulnerable to different attacks (Liu et al. 2015). Several authors look into supply chain attacks based on installing hardware backdoors or Hardware Trojan Horses (HTHs) on ICs (for example, Farag et al. (2012), Goertzel (2013), Ali et al. (2016)), supply chain attacks based on the USB interface (McFadden & Arnold 2010), reverse-engineering (Goertzel 2013, Liu et al. 2015, Ali et al. 2016), counterfeiting devices (for example, Meraglia & Miller (2014), Frazier et al. (2017), Miyamoto et al. (2017)), and tampering (Goertzel 2013, Boyson 2014).

Electronic products, their architecture and the data they contain are vulnerable, as they can be tampered with by malicious actors (McFadden & Arnold 2010). Security threats like those mentioned could come from different parts of the supply chain, including IC foundries, design houses, the design tools, and IP designed by third parties (Liu et al. 2015). McFadden & Arnold (2010) describe a supply chain for the case of counterfeits, where perpetrators could be found all the way from component manufacturers to the final customers. Miyamoto et al. (2017) defend that malicious insiders are needed for counterfeit ICs to enter the supply chain. They also point that the delivery method could follow two approaches, depending on whether attackers plan to single out specific targets, or reach a wider audience.

As part of assessing the risks involved, and finding out the likelihood of a specific incident, Rovito & Rhodes (2016) suggest the use of vulnerability assessment. They apply the Cause-Effect Mapping (CEM) analytic technique to a generic electronics supply chain case, with the intention of finding points where vulnerabilities could lead to mission failure. Then the Trusted Systems and Networks (TSN) methodology follow in their study. This methodology is intended for "protecting mission-critical functions and components" (Rovito & Rhodes 2016), and it makes use of criticality analysis in order to assess the consequence of loss, while the likelihood of loss would be estimated through a threat assessment and a vulnerability assessment.

In the case of an ICT components provider, Reddy (2014) also argues for the use of criticality analysis, in this case to assess the impact of a product's dependability on the supply chain.

3.5.5 The software supply chain

The software supply chain emphasises the flow of software components, as well as hardware would do, and it suffers not only from inherits risks comparable to those in traditional supply chains (like late product deliveries, counterfeit, and human errors), but also its own specific risks, like exploitable faulty code (Sabbagh & Kowalski 2015).

Sabbagh & Kowalski (2015) propose the use of a socio-technical framework to perform threat modelling for software supply chains which, according to them, allows reviewers to focus on individual layers (namely *cultural*, *structure*, *methods* and *machines*) to identify potential threats existing, and which could affect any of the four layers.

Axelrod (2014) suggests that specific threats can be related to several constituents (components) of the software supply chain. This way, the authors identify seventeen different threats and assign them to six components of the software supply chain (products, supply chain processes, product flows, supply chain data flows, management data, and people).

Jilcott (2015) reports on the Theseus project, which lead to the development of technology aimed at easing the vetting process of commodity IT devices provided by suppliers. The resulting product of the project is in theory able to explore the software architecture of said devices in search for vulnerabilities, generating attack scenarios for the device and prioritising components for further vulnerability analysis.

From the software point of view, the Common Weakness Enumeration (CWE) Initiative (MITRE 2018*a*) is a community-developed list of common software security vulnerabilities and, although its database identifies more than 700 weaknesses at the moment this is being written, it seems that there are only eight different technical impacts derived from them (MITRE 2018*b*, Martin 2014), which are:

1. Modify data
2. Read data
3. Denial-of-Service: unreliable execution
4. Denial-of-Service: resource consumption
5. Execute unauthorised code or commands
6. Gain privileges/assume identity
7. Bypass protection mechanism
8. Hide activities

Moreover, when it comes to the software supply chain, Axelrod (2014) indicates that the following attributes are at risk:

- Confidentiality (of intellectual property and personal and business data)
- Integrity (of processes, products and data)
- Availability (of flows, products and data)
- Authenticity (of products and data)
- Trustworthiness (of processes, products and people)

Axelrod (2014) also illustrates how some factors affect supply chain risk differently throughout the software development life cycle, and indicates the need to identify and assess those risks in advance. Shankles et al. (2013) seem to support this, while indicating that, even though it is more cost-efficient to identify code-level vulnerabilities during the technology acquisition and development phases, in practice companies tend to identify issues in the code during the operations and maintenance phase of the lifecycle, when costs of fixing those vulnerabilities are higher.

Regarding risk assessment, it is suggested that it considers the following three components: *attack analysis*, (threats and exploits leading to successful attacks), the ability to *limit vulnerabilities in the product by the supplier*, and the *identification of business risks and attack enablers by the acquirer* (Axelrod 2014).

Finally, Axelrod (2014) provides an account of the level of supply chain risk that might be expected from software of different origin, for three different risks.

3.5.6 Critical infrastructure

Critical infrastructure can be understood as "an asset or system which is essential for the maintenance of vital societal functions" (EC 2018). IT risks have attracted meaningful attention in the context of critical infrastructure, due to the relevance of IT systems to the well-functioning of many of the critical infrastructures nowadays (PITAC 2005, Croll & George 2007).

What sectors are considered as critical is not universally defined, as different governments may define them differently (Infracritical 2018). For example, the Department of Homeland Security of the USA identifies 16 critical infrastructure sectors, which include the IT sector, the energy sector, the healthcare and public health sector and defence, among others (DHS 2018). According to Häyhtiö & Zaerens (2017), critical infrastructure is divided into three levels. The first and most important one is formed by IT industry, energy sector and water supply industry. The second level consists of the finance sector and the chemical industry sector. The last level consists of armaments industry, distribution services, agriculture and food supply chains, health care, and search and rescue services.

The NIST Cybersecurity Framework (NIST 2018) is a framework designed by the National Institute of Standards and Technology (NIST), for critical infrastructure companies to manage cybersecurity risks. Similar to previously presented risk assessment frameworks, the NIST framework suggests the documentation of the known threats, breaches and vulnerabilities, while covering both the internal and external environment (Dedeke 2017). Moreover, an estimation is made of the likelihood and the impact of a cybersecurity event "for specific information, processes and technologies", which is complemented by an assessment of the regulatory environment (Dedeke 2017).

- Maritime transportation sector -

The maritime supply chain has also attracted interest, when it comes to cyber risks. During the literature review, it was found that a significant part of the research analysed in this area came as part of the project MITIGATE, from the European Union's Horizon 2020 research and innovation programme (Papastergiou & Polemi 2018, Polemi & Papastergiou 2016, Polatidis et al. 2017, 2018, Duzha et al. 2017). This project aims to help in assessing the effects of cyber threats in the maritime environment (Polemi & Papastergiou 2016).

Papastergiou & Polemi (2018) define MITIGATE as a Supply Chain Risk Assessment methodology, which is aimed to estimate cyber risks of any Supply Chain Service where the interaction of various cyber assets is required from various business partners. This risk assessment methodology has the following steps: *Boundary Setting, Threat Analysis, Vulnerability Analysis, Impact Analysis, Risk Estimation*, and *Mitigation Strategy*.

In identifying the threats, Meyer-larsen & Müller (2018) describe three different groups that may target ports. According to them, the first one are *criminals*, which mainly aim for cargo theft. Among the goals they try to achieve through cyber-attacks are: to retrieve data, track truck driver's habits (like routes and stops), and increase the effectiveness of their physical attacks. In some cases, they could also aim for stealing data (i.e. data of all containers in a port), and set a ransom fee for it. The second group are *hacktivists*, which according to the authors are mainly interested in "proving their abilities by detecting vulnerabilities in the systems of the port", which could lead to disruptions. The third group are *governments*, who may target foreign port systems to identify possible vulnerabilities or for espionage.

In order to identify vulnerabilities, Polatidis et al. (2018) propose the use of the attack path discovery method, which would be used in MITIGATE for risk management, on specified network fragments of the maritime supply chain infrastructure.

- Energy sector -

Different authors raise awareness about the effects that cyber risks may have on the energy sector. Babun et al. (2017), for example, discuss about the identification of counterfeit devices on the smart grid, which represent "a real problem".

Venkatachary et al. (2017) present a list of different facilities attacked by malicious software in the past, as well as the impact of those attacks. At the same time, they also model threatening agents

and adversaries, for which they also describe what assets they threaten, the motives of said agents and the potential impact of their success. Those modelled threat agents are: *state sponsored*, *organised crime*, *hacktivists*, and *insiders*. Finally, the authors also present an accounting of cyber security vulnerabilities on different elements in the energy industry (generators, transmission, metering and billing systems) as well as the potential financial impact of said vulnerabilities.

Kammerstetter et al. (2014) develop a methodology for assessing risks involved within their cumulative smart grid model. As part of their work, they compiled a list with 31 threats, clustered in the six categories: *Authentification/Authorization*, *Cryptography/Confidentiality*, *Integrity/Availability*, *Missing/Inadequate Security Controls*, *Internal/External Interfaces*, and *Maintenance/System Status*. Then, a "threat matrix" could be created when those threats where combined with the ten components of their architecture model, namely: *Functional Buildings*, *E-Mobility & Charge Infrastructure*, *Household*, *Generation Low Voltage*, *Generation Medium Voltage*, *Testpoints*, *Transmission (High/Medium Voltage)*, *Transmission (Medium/Low Voltage)*, *Grid Operation*, and *Metering*.

According to the methodology presented by Kammerstetter et al. (2014), the final step of the risk assessment involves estimating the risk potential for each element of the threat matrix, for which they provide a qualitative assessment of the probability and impact of each of the threats.

- Oil sector -

For the petrochemical industry, Dutcher (2013) profiles five groups to whom "almost any threat actor can be categorised": *criminals, hacktivists, insiders, nation-states,* and *terrorists*. According to him, each of these actor groups has different interests when it comes to "targeting refineries, petrochemical plants, gas processing plants, fertiliser plants and other facilities". Similarly, for each group their capabilities, tactics, tools used and procedures, which they would use to launch a mission or campaign, differ as well and could also be modelled (Dutcher 2013).

Couce-Vieira & Houmb (2016) provide an overview of the supply chain involved in handling cybersecurity incidents for drilling rigs. Nasir et al. (2015), on the other hand, provide a list with potential cyber-threats to each of nine different areas of the global oil supply chain.

However, Dutcher (2013) suggests that the identification of vulnerabilities is "easier to quantify than threats", while providing also a list with entities of which being aware of the location "is advisable".

When assessing the cyber risks in a drilling supply chain, Couce-Vieira & Houmb (2016) strongly recommend to understand the different stakeholders and their own perspectives, activities and goals. At assessing the impacts, Dutcher (2013) suggests the use of Business Impact Analysis (BIA). This method can be applied to determine costs linked with downtime "for the repair or delivery of new equipment", and dealing with "brand a reputation damage" or "the disclosure of sensitive information".

- Other CI sectors -

In the area of telecommunications, McGraw et al. (2014) simulate the effect that malware may have on space vehicles, concluding that it could have devastating effects on their functioning. Forbes et al. (2014) argue about the increasing vulnerability of commercial space systems, as a result of the growing use of off-the-shelf hardware and software.

In the area of healtchcare, Hawrylak & Hale (2015) raise awareness about the privacy issues involved in the use of RFIDs (Radio Frequency Identification) tags, which potentially introduces risks involving tracking and confidentiality of information. Finnegan & McCaffery (2014), on the other hand, discuss about the security of medical devices and provides a framework "to assist manufacturers to demonstrate and communicate the security capabilities" of such devices.

In the military and governmental area, the protection against the insertion of counterfeit and other tainted elements (software and hardware related) in the supply chain has attracted significant academic interest (Panko 2011, Baldwin et al. 2012, Alexander 2012, Meraglia & Miller 2014).

3.6 Supply Chain IT Governance

In this section, the role and importance of governance in managing cyber risks across the supply chain are discussed. According to Patnayakuni & Patnayakuni (2014), IT governance defines who, where and how decisions affecting IT are made. Moreover, it can be used to provides adequate authority to cyber security to affect decisions in other managerial areas which have an impact on or are impacted by cyber risks.

Peterson (2004) defines three main components in IT governance, which are the *process*, *structural* and *relational* capabilities. Those three elements are used to categorise the respective findings regarding governance, and are further explained below.

3.6.1 Process capabilities

In regards to IT governance, *process capabilities* refer to "the degree to which IT decision-making and decision-monitoring follows specified rules and standard procedures" (Peterson 2004). It involves the identification and formulation of the business logic behind IT decisions, the "prioritisation, justification, and authorisation of IT investment decisions", and the monitoring and evaluation of the implementation of IT decisions and IT performance (Peterson 2004). This can be connected to framework proposed by Gaudenzi & Siciliano (2018), where IT governance takes input from compliance and risk assessment practices in order to manage cyber risks.

When it comes to the governance of Information Security in the value chain, Patnayakuni & Patnayakuni (2014) refer to the "standardisation and codification of the decision making process", including examples of mechanisms to institutionalise them, like frameworks, methodologies and rules.

Part of the process component in IT governance is the use of tools to define the rationale behind certain business decisions (Peterson 2004). In the literature, there are many frameworks intended to assist and guide in making strategic and operational decisions in the area of supply chain cyber risk management. Some of them are mentioned and/or described throughout this document, like the "Cyber Prep levels" from Bodeau et al. (2010) which can be used to characterise the "desired level of preparedness against cyber adversaries, establishing goals and strategies", or the IT governance framework COBIT (Wolden et al. 2015) which provides procedures on how a certain software should be implemented and how security should be managed with a consumer.

The standardisation of decision making processes in the supply chain has been widely advised for the management of cyber risks in several contexts (Polemi & Papastergiou 2016, Yoshifu et al. 2018), and it is said to benefit the establishment of a more cyber security-minded culture (Safa et al. 2017*b*).

The use of internationally recognised standards is generally suggested, being the ISO/IEC 27000 family of standards, as previously mentioned in section 3.4, the most referred to. Bartol (2014) maps the landscape of cyber supply chain standards, providing an account of existing practices and processes that relate to this field of study. At the same time, Boyson (2014) points at a lack of empirically-proven best-practices body of knowledge in the area, and proposes the establishment of a "corporate cyber supply chain code of practice" that should fill this gap over time.

Nonetheless, some basic challenges are still being addressed, like the standardisation of the terminology used in the area of supply chain cyber risk management. This step is critical, because it enables meaningful understanding and reasoning between supply chain partners, as for example when discussing on possible attacks on their process chains, or what quality inspection measures are the most necessary (Bartol 2014, Pan et al. 2017). In connection to this, Windelberg (2016) refers to the appearance of misunderstandings when it comes to setting objectives for managing cyber risks in the supply chain, emphasising that "increased awareness of the connotations of each objective can reduce the risk of failures and cyber attacks and the associated recovery costs".

In general, there does not seem to be an homogeneous use of terminology in the area of supply chain cyber risk management, maybe because it draws concepts from several bodies of knowledge, some of which do not seem to have a standardised use of their terminology themselves, like supply

chain resilience (Ali et al. 2017). Therefore, attempts to standardise terminology have to be drawn from related fields. For example, the Common Weakness Enumeration (CWE) Initiative provides a list of software weakness types, created to "serve as a common language for describing software security weaknesses in architecture, design, or code" (MITRE 2018*a*). Goff et al. (2014), on the other side, propose the Cybersecurity Procurement Language for Energy Delivery Systems, to "encourage and support the incorporation of cybersecurity in the procurement of energy systems and components".

Patnayakuni & Patnayakuni (2014) discuss about how different types of value chain governance would affect the need for better standardisation and codification of the processes for decision making between supply chain partners. Variables that would play a role in those forms of governance are the complexity of the decisions to be taken, the ability to codify them, and the maturity of the supplier's capabilities.

As mentioned before, the process component of IT governance also involves the definition of the logic behind IT investment decisions. In this regard, Torabi et al. (2016) make use of benefit-cost analysis to assist in the development of strategies for allocating resources to counter different risks. Kelic et al. (2013) describe a method to evaluate the macroeconomic impact of certain cyber risks through the representation of the pathways of disruption propagation, which can be helpful in finding gaps in budget allocation.

Nagurney et al. (2017) and Daniele et al. (2017) use a game theory model to look into how companies invest in cybersecurity when faced by changing competition and other environmental aspects, and how their decisions affect their vulnerability and the network vulnerability. In a similar way, Bandyopadhyay et al. (2010) analyse the existing incentives for supply chain partners to invest in information security. They conclude that an increase in supply chain collaboration and IT integration tends to lead to an investment in IT security that is below the increase in vulnerability, which calls for the inclusion of mechanisms to encourage firms "to not only protect their own security but also those of other firms in the supply chain" (Bandyopadhyay et al. 2010).

Finally, processes must also be established to monitor and evaluate the implementation of security programs, as well as measure their performance. For this, the proper definition of KPIs (Key Performance Indicators) is critical (Ali et al. 2017). Their use allows for managers to continuously monitor the alignment between the risks faced and the real risk appetite of the organisation (Siciliano & Gaudenzi 2018).

Dedeke (2017) discusses about monitoring the implementation of a cybersecurity program, and provides a comparison between two frameworks that meet this function. The NIST "implementation tiers" is preferred for a company if the central issue is "monitoring the evolution of the risk management practices and culture", while the "maturity-oriented" framework from Intel is preferred for "creating a road map that covers the development of resources such as people, processes, technologies, and ecosystems" (Dedeke 2017).

3.6.2 Structural component

From an IT governance perspective, the structural component refers to mechanisms that enable contact between decision-making functions, taking the shape of formal positions, roles, formal groups and/or team arrangements (Peterson 2004). In this line of thought, and in the context of supply chain IT governance, Patnayakuni & Patnayakuni (2014) argue for structural integration, through the creation of "institutionalised team and inter-organisational liaison roles with suppliers", the "right to audit and compliance control by focal firm", and "clear ownership, accountability and responsibility for the protection of valuable information assets".

The creation of structural mechanisms for control of cyber risks is supported in the literature, as dealing with cyber-attacks in the supply chain usually involves information flows and interactions spanning over different areas of the company (Almadhoob & Valverde 2014, Estay & Khan 2016).

For this, the existence of hierarchies within an organisation as well as the assignment of responsibilities are highlighted in the literature (Wolden et al. 2015, Yoshifu et al. 2018), and hailed as a core contributor to the effectiveness of a given information security system Wolden et al. (2015).

More specifically, the role of managers has been proven to be crucial for the success of a security system, as they are responsible for channelling the needed resources for it (Wolden et al. 2015). In regards to lower-level managers, Hale et al. (2004) describe a number of responsibilities that they could be charged with, when it comes to the tactical implementation of a security strategy for information assets. In some countries, legal requirements in this regard may exist. In Canada, companies need to have implemented structural mechanisms, like an executive risk board, in order to be able to list on the Toronto Stock Exchange (Boyson 2014).

Khan & Estay (2015), however, argued for distributed accountability, instead of a centralised authority controlling cyber-risks. They defend this need stems from arising complexity in supply chain arrangements, as this complexity creates the conditions for malevolent actors to infiltrate and harm whole networks (WEF 2017). In this line, assigning responsibilities to different individuals adds layers of defence, reducing the possibilities of success for a malicious insider (Miyamoto et al. 2017). Both Khan & Estay (2015) and Yoshifu et al. (2018) suggest the creation of cyber-crisis teams, or emergency response teams, within each organisation, whom should be empowered to work across organisational boundaries.

In support for working across inter-organisational boundaries for the sake of dealing with cyber risks, Patnayakuni & Patnayakuni (2014) and Caldwell (2015) argue for allowing auditing and assessments of business partners to make sure the compliance with defined security criteria, as this "should preserve the integrity of the supply chain" (Caldwell 2015).

Although it is generally accepted that it will be difficult to stop all attacks, considering resilience in the design of the network would "make attacks less likely to succeed", "minimise the consequences when they do succeed", and "act as a deterrent against future attacks" due to increased adversary cost and uncertainty (Goldman et al. 2011).

A key factor on the design of a supply chain structure is that it is a highly strategical component, with a long-term view. According to Ali et al. (2017), supply chain design is the main practice in building a *robust* supply chain. Ali et al. (2017) refer to "robustness" as the ability of the supply chain to resist change and it implies proactively anticipating change before it occurs. In this context it entails the design of a network structure that sustains the creation of value during and after a disruptive event. Herrera & Janczewski (2016) use the term *architectural mechanisms* in a similar way, to refer to the coordination mechanisms across the supply chain that "establish a clear baseline structure", trying to minimise the exposure to sources of disruption.

Ab Rahman et al. (2016) ultimately use the concept of Forensic by Design, proposing to integrate forensic systems and structures into the design and development phases of cyber-physical cloud systems. The value of considering forensics early is that it could allow for attribution during the investigation after a security incident, as for example identifying the attack source, or assisting in reducing the complexity of a forensic investigation and minimising the investigation time.

Finally, Osborn & Simpson (2017) research the effects that the size of an organisation has on the technology they employ and the impact that it has on their cyber-security decision making, highlighting the differences in their infrastructure and vulnerabilities stemming from their smaller scale and resources available.

3.6.3 Relational component

From a governance perspective, relational capabilities are differentiated from structural capabilities in that they lead to the "voluntary and collaborative behaviour of different stakeholders to clarify differences and solve problems, in order to find integrative solutions" (Peterson 2004). In other words, they enhance the collaboration of stakeholders working with different mental models and their shared learning, which could result in improved coordination of the decision making process, as well as more collaborative relationships (Peterson 2004).

Mechanisms that facilitate the development of the relational component are often not regulated, because they are usually regarded as tacit, like the informal role of leadership. The willingness and support of the leaders of an organisation for an information security program, both at top and middle management level, has a direct influence over the effectiveness of implementation of

an information security framework (Wolden et al. 2015). However, leadership is not the only mechanism. In this regard, Hale et al. (2004) show several subjective KPIs (Key Performance Indicators) to assess the success of a security program, which can be relevant to the relational governance perspective like: measuring the motivation of employees playing key roles in supporting the program, the frequency of messages exchanged in the topic, or the proactive contributions made by employees to improve the system.

On a different note, Patnayakuni & Patnayakuni (2014) relate trust to relational capabilities, and defend that it is possible to choose developing relational trust-based organisational processes for information security, over the previously discussed processes and structural integration, depending on three variables which are the *complexity of decisions*, the *ability to standardise decisions*, and the *capabilities of the business partner*. Nonetheless, the three forms of governance are complementary to each other in most cases (Patnayakuni & Patnayakuni 2014).

Häyhtiö & Zaerens (2017) describe the existence of two different approaches towards the management of contracts. The first one is focused on the structural design of the transaction, referring to the *written contracts* between the participating parties, which are legally binding by nature. For example, some companies put clauses into vendor contracts that oblige them to address certain risks (Boyson 2014). The second approach places its focus on the relationships between the parties involved in the co-operation. In this last case, the parties involved rely on trust, "which works as a safeguard for coordination and control functions".

In the e-maritime context, Polemi & Papastergiou (2016) point at the lack of trust chains of maritime entities at different national and international levels as one of the most important obstacles "in the way they they manage security processes".

However, Häyhtiö & Zaerens (2017) warn about the inherent risks added to the system by placing trust and assumptions on supply chain partners, especially in regards to the implementation of measures against known and unknown threats. Windelberg (2016) analyses the rationale behind this problem more extensively, treating trust assumptions as *tradeoffs*, which on one hand could bring beneficial features to the system, more efficiency, preserve performance or facilitate system utilisation, while on the other hand increase risk in the way that they introduce defects or vulnerabilities. Additionally, Windelberg also modelled typical tradeoffs and trust assumptions, where the tradeoffs are labelled as *addition*, *omission* and *sub-optimisation*.

3.7 Pre-Event Knowledge Management

Knowledge management can be understood as making the best use of the knowledge available to achieve organisational objectives. According to Ali et al. (2017), supply chain resilience can be improved by cultivating knowledge management in a situation previous to a risk-event, due to bringing a better general understanding of the supply chain and the human resources. In this regard, the practices recommended are related to education and training in regards to cyber risks, and the creation of a resilience / risk management culture.

Safa et al. (2017*b*) look into education for information security, and describe six approaches that can be used for raising knowledge and awareness of users in this area, as well as the advantages and disadvantages of their use. As they define them, those delivery methods can be: *Conventional*, *Instructor-led*, *Online*, *Game-based*, *Video-based*, and *Simulation-based*.

Indeed, employees should understand the information security framework in their company, and the importance of it. However, employee awareness of the information security programs is not a perfect indicator for this, as their own beliefs and assumptions also play an important role when they handle security programs, and those beliefs must be understood in order to effectively implement those programs (Wolden et al. 2015). Furthermore, employees do not always comply to the information security policies and procedures stated by their companies (Safa et al. 2017*b*).

On the other hand, companies tend to rely on IT staff and department to be protected from cybercrimes, but research has also shown that in some cases the high level positions lacked an understanding about cybercrimes. Therefore, training senior management "is as important as educating the end users about security" (Almadhoob & Valverde 2014).

It is understood that a strong information security culture could also be effective in order to protect information assets (Alhogail 2015, Safa et al. 2017*b*). To implement security programs and root them into a company's culture, Alhogail (2015) approaches the problem from a change management perspective. According to Safa et al. (2017*b*), there are three external factors that affect information security culture: *regulatory requirements*, *customer preferences and expectations*, and *geographical distribution*.

3.8 Cyber Security

Here, the term cybersecurity refers to the protection of the assets and systems (physical or digital) involved with the storing and processing of information in digital format. The terms "IT security" and "Information security" may be used in a similar way, and interchangeably with cybersecurity when it refers to the protection of either IT systems or information in digital format.

Once the risks have been identified and assessed, then countermeasures must be put in place. In this section, we cover proactive measures and techniques found in the literature, used to prevent previously identified cyber risks, before the risk event takes place.

In general, information security measures tend to focus on the protection of the *confidentiality*, *integrity* and *availability* of information (Almadhoob & Valverde 2014, Boyes 2015, Miyamoto et al. 2017), which is also the baseline of the CIA triad mentioned earlier in this document. In regards to creating cyber resilience, Goldman et al. (2011) describe a number of *proactive techniques*, which they define as "architectural or inherent and exist prior to attack". Those proactive techniques, as defined by them are:

- *Segmentation, Isolation, Containment*: this requires modification of the system architecture, ideally reducing the attack surface, limiting the damage of exploits when they occur, and allowing better monitoring of critical functions.
- *Diversity & Randomness*: adding elements of surprise or confusing a potential attacker may thwart an exploit. This technique is aimed at increasing the attacker's risk of getting exposed, buying time to the defenders and minimising the impact of technology-specific attacks. Examples are the use of multiple operating systems, or different versions of the same software on different machines, which could minimise attacks based on a specific technology.
- *Moving Target and distributedness*: distributing critical processing through different locations, at the same time and/or over time has become increasingly feasible due to virtualised and cloud-based services. This type of defence aims at decreasing the motivation of the attacker to proceed with an attack, by increasing their uncertainty "that the IT environment is still the same as when he did reconnaissance" (Alexander 2012).
- *Non-persistence*: when continuous access is not essential, this type of technique restricts access to certain data, applications and connectivity over time. This way, access to them is given only when needed, which restricts attacker's opportunities to identify and exploit vulnerabilities, as well as maintaining a presence. An example could be the use of virtualised browsers. In a similar way, Alexander (2012) talks about *isolation mechanisms*, which can help prevent exposure, contamination and collusion.
- *Data & System Integrity & Availability*: integrity mechanisms attempt to prevent attacks causing resource modification. When the integrity of a component or of a system gets compromised, then the situation may be worsened by traditional resilience techniques, which may propagate corrupted services or data.

Bodeau et al. (2010) define different levels of cyber threat, based on the threat actors involved, while characterising their capabilities and techniques, and provide examples of security measures for each level of cyber threat. Those security measures are divided in five levels:

1. Perimeter Defence
2. Critical Information Protection

3. Responsive Awareness
4. Architectural Resilience
5. Pervasive Agility

In recent years, it has been found that even some of the most "basic" security measures like antivirus and firewalls are still not being always correctly implemented by companies, while measures like integrity checkers are among the least implemented (Almadhoob & Valverde 2014). Nonetheless, all security measures are not only technical in nature. The social aspect of information security is also looked at in the literature, and a strong information security culture is pointed at as an effective mean of mitigating vulnerabilities stemming from individual behaviour (Mensah et al. 2015, Safa et al. 2017*a*). Some examples of risky behaviour are the infrequent back-up of information or the use of email accounts to send sensitive and confidential information, as well as carrying sensitive and confidential information on unencrypted devices (Safa et al. 2017*a*).

Moreover, security systems may also be the subject of a cyber attack, which also threatens the information and/or information systems they protect. Therefore, protection systems must as well be protected, as for example intrusion detection systems (Miyamoto et al. 2017).

As mentioned in previous sections, Industry 4.0 brings the possibility of increasing efficiency through the integration of industry with new technologies and the Internet. This includes examples like IoT, the Cloud and the use of RFIDs in the supply chain. Nonetheless, while they can make a system more efficient and secure, they also introduce new vulnerabilities that must be secured.

This way, RFID (radio frequency identification) tags are regarded as a relatively new way of tracking and tracing the movement of physical material and products along the supply chain (Barreto et al. 2017). However, several authors have look into the new risks derived from the use of this technology and propose ways of countering them. One of the most mentioned issues relates to confidentiality. On RFIDs used in the healthcare sector, attackers could obtain unauthorised access to medical data stored in the RFID tag, as well as track the movement of objects and people in real time. For this, some solutions are proposed such as encryption or allowing patients to opt-out from using the RFID systems (Hawrylak & Hale 2015). Qi et al. (2016) look into RFID-enabled Third-party Supply chain systems, and identify ways of securing it through the use of crypto-IDs. On the other hand, Kim (2012) mentions authentication and availability issues of their use in the supply chain, and proposes an enhanced hash-based RFID mutual authentication protocol.

The Industrial Internet of Things (IIoT) and Cloud services do also add vulnerabilities to the system, when linking production facilities to the Internet, potentially allowing attackers to sabotage critical infrastructure from the outside, access sensitive customer data and espionage (Preuveneers et al. 2017). Because of this, Alam et al. (2017) discuss the use of data transfer protocols involving sensors in the IoT era, which should include "confidentiality, message integrity, and end-point authentication" properties. Mustafa et al. (2015) address privacy issues in the charging protocol of EV (electric vehicles), supporting privacy in the identification and location of the EV's user from the host supplier.

Most recently, blockchain technology has been proposed for addressing some of the aspects of security and privacy in IT-enabled supply chains. Kshetri (2017*a*), for example, compares the cloud and blockchain from a security and privacy perspective. According to Kshetri (2017*b*), blockchain can address some of the challenges that IIoT pose, like architectural constraints, cloud server downtime and unavailability of services, susceptibility to manipulation, and capacity constraints to manage rapidly growing needs. In general, blockchain technology can also address challenges related to transparency, security provision, and accountability (Kshetri 2017*a*, Preuveneers et al. 2017, Meng et al. 2018). This way, Preuveneers et al. (2017) propose the use of private blockchains on a production network, and they argue that their solution is able to "mitigate identity spoofing, information disclosure and escalation of privilege threats". However, the same transparency and accountability that could be considered beneficial on one side, could translate on privacy issues in other cases (Preuveneers et al. 2017).

Securing electronic products, like integrated circuits (ICs), has also attracted significant research efforts, due to supply chain risks like reverse-engineering, the insertion of Trojans, counterfeits and

IP piracy (Ali et al. 2016). Nonetheless, when it comes to implementing risk-avoiding techniques, they mostly involve integrating security measures in the design of the ICs, like *watermarking*, *metering*, *side-channel fingerprinting*, *obfuscation*, and *locking* (Liu et al. 2015, Ali et al. 2016, Dofe & Yu 2018).

In summary, as Goldman et al. (2011) put it, there is no single solution that fits all contexts. Therefore, they recommend a balanced combination of mechanisms and capabilities for protection, detection, and adaptive response based on the needs of the mission, environment and risk tolerance, some of which are discussed next.

3.9 Supply Chain Agility

Supply chain agility is defined by Christopher & Peck (2004) as "the ability to respond rapidly to unpredictable changes in demand or supply". They identify two main components to it, which are *agility* and *velocity*.

As mentioned in section 3.3, agility is understood here with a "pre-event" connotation, while velocity would form part of the "during-event" phase, in a similar way as Ali et al. (2017) propose. In the context of Cloud supply chain resilience, Herrera & Janczewski (2015) also follow a similar approach than Ali et al. (2017) and defined visibility as a protective mechanism (proactive), while velocity forms part of a response mechanism (reactive). Both elements are further described and discussed in the next subsections.

3.9.1 Visibility

Visibility refers to generating knowledge and awareness on the current status of supply chain operating assets and the environment (Pettit et al. 2013, Ali et al. 2017). It involves being able to detect risk events on the supply chain (i.e. affecting supply chain partners) which have the potential of also impacting the focal company, giving valuable time for the focal company to prepare for them, aligning capabilities and minimising the impact of the cyber event on them and the supply chain.

Boyson (2014) hails the existence of strategies ensuring continuous visibility of software and hardware production and delivery cycles as a "hallmark of a proficient, mature IT supply chain risk management practitioner". Finding issues as soon in the lifecycle as possible provide for time and better availability of resources to deal with them.

Put in the context of cyber risks, supply chain visibility would translate into being able to detect cyber events suffered by SC partners (upstream or downstream) or the whole supply chain (Christopher & Peck 2004), like (and not restricted to) a cyberattack that results in the leak of confidential and sensitive customer data affecting the focal company, the introduction of counterfeit products in the supply chain, or the loss of IT capabilities affecting the supply of services to the focal company and/or the focal company's services themselves.

Visibility can be enabled in the supply chain through proper IT governance mechanisms like structures and processes, such as compliance to standards and policies with the disclosure of cyber-breaches, as described in section 3.6. Different practices related to the increase of visibility between supply chain partners are: the collective monitoring of performance through KPIs, the sharing of information, and increased connectivity and transparency through integrated systems and sensor networks (Ali et al. 2017, Boyson 2014).

Nonetheless, the use of IT systems to increase general supply chain visibility can also increase the vulnerabilities inherent in the system. Cloud solutions and big data, for example, have been proposed for supply chain management, but Radke & Tseng (2015) warn that "a critical mass among suppliers and customers" is needed for the use of such technologies in order to "reap their benefits", otherwise risking the extrapolation of unreliable information. (Bandyopadhyay et al. 2010), on the other hand, argue that an increase of IT integration in the supply chain should be preceded by consequent investments in security measures to account for an increase in risks.

Blockchain technology is proposed in the literature as a novel way of solving some of the security issues posed by the integration of IT systems in industries and their supply chains, as seen in section 3.8, mitigating information security risks related to "identity spoofing, information disclosure and escalation of privilege threats" (Preuveneers et al. 2017).

Counterfeits and tampered IT products inserted into the supply chain have also attracted significant interest, due to the risks they pose. Several authors propose different approaches to verify the authenticity of both hardware and software coming from different parts of the supply chain. As a result of the literature review, it is believed that those approaches tend to focus on the following areas:

- The detection of counterfeit hardware, like ICs (Panko 2011, Meraglia & Miller 2014, Liu et al. 2015, Ali et al. 2016, Frazier et al. 2017, Babun et al. 2017)
- The detection of tampered hardware, as for example via hardware Trojan horses (McFadden & Arnold 2010, Liu & Sandhu 2015, Ali et al. 2016)
- The detection of malicious software inserted on IT systems via cyber-vulnerability exploitation (Mattsson 2004, Forbes et al. 2014, Lee & Kwon 2016, Rrushi 2016)

The detection methods proposed by the authors in the list above include different testing techniques on hardware and software, the implementation of different design techniques that make tampered circuitry more obvious to spot (as also mentioned in section 3.8), the use of cryptography, deception, and machine learning to observe behavioural anomalies on IT systems and products.

Still, despite all the available techniques to detect unwanted IT elements in the supply chain, inspections also carry a cost and a "100% test coverage" may not be possible (Goertzel 2013). Therefore, tradeoffs existing between the coverage of quality inspections and the costs involved in them must be considered (Pan et al. 2017), and a balance must be found in accordance to the risk appetite of the organisation.

Finally, supply chain monitoring of relevant metrics (KPIs) must also be put in place, allowing for the detection of any supply chain issues as early as possible. For Estay & Khan (2015), the concept of *detectability* (or its counterpart, *un-detectability*) gains special relevance in this context, as the risks that relate to a disruption event that is more relevant tend to be, in fact, less detectable. To illustrate this, they propose the use of a tool to dynamically respond to disruptions through detectability, based on the monitoring of the performance of KPIs over time.

3.9.2 Velocity

Supply chain velocity is defined as "distance over time" (Christopher & Peck 2004), making reference to the time that it takes to respond to risks. Similarly, Herrera & Janczewski (2015) use the term in the context of Cloud supply chain resilience, asserting that supply chain velocity mechanisms assess how rapidly the supply chain reacts to disruptive events.

In the context of managing supply chain cyber risks and cyber resilience, very few direct references have been found to the velocity component of agility. However, it is an important concept in the general context of supply chain resilience (Christopher & Peck 2004, Ali et al. 2017).

According to Christopher & Peck (2004) "there are three basic foundations for improved supply chain velocity", which are: *streamlined processes*, *reduced inbound lead-times* and *non-value added time reduction*.

When it comes to supply chain cyber risks, those foundations could refer to having mechanisms in place that ensure a streamlined response to cyber-events. Real-time monitoring is one of those mechanisms mentioned in the literature (Herrera & Janczewski 2016). Moreover, as seen before in section 3.6, supply chain IT governance could also provide such benefits, through the establishment of mechanisms like inter-organisational emergency response teams and action protocols.

Although it has not been directly linked to the concept of velocity, the integration of forensic capabilities within the IT systems in the supply chain can definitely minimise investigation time in a security incident (Ab Rahman et al. 2016, Miyamoto et al. 2017, Meng et al. 2018). The use of blockchain solutions in the supply chain has also been proposed to deal more efficiently with crisis situations where it is necessary to track "the sources of insecurity" (Kshetri 2017*a*), because their public availability makes it suitable to trace products back to their origins.

3.10 Ability to adapt

The *ability to adapt* can be understood as being able to manage critical resources and operations in the supply chain, and adjust them in response to challenges and opportunities (Pettit et al. 2013, Ali et al. 2017). According to Ali et al. (2017), this ability is also covered in the supply chain resilience literature through two elements: *flexibility* and *redundancy*. In this case, flexibility refers to flexibly use of processes, supply and/or demand management. This definition contrasts with the one from Pettit et al. (2010) in that for the latter the ability to modify processes forms part of the general adaptability. Redundancy, on the other hand, builds on maintaining excess capacity as a mechanism to adapt to disruptive events (Ali et al. 2017).

Even though Ali et al. (2017) sustain that flexibility and redundancy are two of the three most discussed element of SCRES, in the reviewed literature it has been observed that these concepts held a much lesser presence among the topics of discussion, being able to point at very few examples of research where flexibility, redundancy and even adaptability are clearly addressed in the context of managing cyber risks.

Herrera & Janczewski (2015) define "flexibility mechanisms" as those that "provide alternatives to meet the CSC (Cloud Supply Chain) expected level of resilience", while Goldman et al. (2011) describe a number of reactive techniques used to thwart cyber-attacks, which in a way make use of flexible IT processes or resources, namely: *dynamic reconfiguration*, *deception*, *dynamic reconstitution*, *dynamic composition*, and *alternative operations*. Regarding building redundancy, Boyes (2015) discusses about investing in adequate capacity to handle surges in demand, mostly for online traffic and services.

3.11 Recovery

In the context of supply chain resilience, recovery is understood as the "ability to return to the normal state rapidly" (Pettit et al. 2010), and in this section we describe a number of elements in the literature that were found to be relevant to allow for a return to normal from a cyber risk event.

According to Ali et al. (2017), there are two main elements in this regard, which are the existence and actuation of contingency plans, and the market position of the firm. A similar approach will be used here, with slight modifications. On one hand, the term *recovery planning* is preferred over contingency, more in line with the terminology used by Pettit et al. (2010). On the other hand, the relevance of *financial strength* is also argued, and included together with *market position*.

3.11.1 Recovery Management

Recovery plans allow for a faster enactment of the best suited actions to effectively counter certain disruption events. Ali et al. (2017) refer to them as "contingency plans", which could allow for the scenario analysis, as well as for dealing with the reconfiguration and mobilisation of supply chain processes and resources. For Pettit et al. (2010), some factors that are also associated to the recovery are the crisis management, the communications strategy, and the mitigation of consequences.

We understand that recovery management in this context involves the identification of critical vulnerabilities and risks that the firm should prepare for, the development of contingency plans for recovery and mission assurance after a risk event, planning for the availability of resources needed for the execution of post-disruption plans, and the effective and efficient execution of those plans when needed.

Please note, Recovery Management is placed in the post-risk event phase because we emphasise its value in the management of cyber risks after they have been realised. Nonetheless, the planning process itself should take place before the realisation of the risk event, and it makes use of outputs from some of the elements in the preparation phase previously described in this thesis, like compliance, situation awareness and governance.

As it can be observed, several concepts and tools that fit under recovery management may overlap in some way with others, previously discussed in the pre-event phase, like vulnerability identification and risk assessment (described in section 3.5), although the focus of their application is now centred in mitigation and recovery rather than prevention. For example, some approaches used to prepare for risk events through the detection of supply chain vulnerabilities, like simulation and modelling techniques, have also been proposed for the elaboration of recovery plans (Axelrod 2013, Filippini & Silva 2015).

Torabi et al. (2016) propose a risk assessment framework for business continuity management, which considers different supply chain elements, as well as risks stemmed from cyber-attacks. They also discuss the issue of resource allocation, and propose the use of benefit-cost analysis for the prioritisation of resources for key functions in the face of certain risks, as well as metrics like minimum required resources to continue key functions and time required to prepare those resources.

Another relevant point is that the formulation of recovery plans should contain KPIs and objectives that are understood by the members of the supply chain (Radke & Tseng 2015, Windelberg 2016). This is expected to lead to a more efficient coordination between supply chain members, together with proper governance through well understood processes and structures, as well as relationship management (Patnayakuni & Patnayakuni 2014).

However, Gaudenzi & Siciliano (2018) recently warned that there is still a general lack of implementation of systematic plans in the field of cyber risks "for disaster recovery, business continuity, or the backup of sensitive data".

3.11.2 Market Position and Financial Strength

In the context of supply chain resilience, market position refers to the status of an organisation and/or its products in specific markets, while financial strength reflects its capacity to absorb variations in cash flow (Pettit et al. 2010). Both concepts are instrumental in increasing a firm's chance of recovering from supply chain disruptions (Ali et al. 2017).

This way, market share, product differentiation and customer loyalty are some sub-factors understood to form part of the market position, while financial reserves, liquidity, portfolio diversification and insurance are elements under the broader concept of financial strength (Pettit et al. 2010).

As mentioned in section 3.5.2, financial indicators are often recommended for measuring the impacts of risks. In fact, the use of units of currency is the main way used to reflect the losses caused by cyber-attacks (McAfee 2014, PWC 2017).

This could lead to the reasoning that, in an organisation where none of the mechanisms previously discussed in this thesis has been applied (e.g. measures for prevention and mitigation of any cyber risks), the company would either have to rely on financial resources alone in order to survive the impact of any cyber event and allow for a timely recovery from lost income (financial strength), or else enjoy a level of market share, portfolio diversification or customer retention that does not completely severe their sources of income before a complete recovery (market position).

The smaller the size of the organisation and the availability of financial resources is, on the other side, also limits the ability to invest in cybersecurity and the amount of suitable security solutions, which leads to the general observation of less advanced security mechanisms in smaller organisations when compared to bigger ones (Osborn & Simpson 2017).

The use of insurance policies to mitigate the economic impact of cyber risks has also been proposed in the literature (Boyson 2014), but in practice their use seems to have been limited. Normal insurance policies do not cover cyber-attacks (Meyer-larsen & Müller 2018). Even though there are insurance companies that provide insurance policies covering cyber risks, several authors warn that there is a general lack of actuarial data, causing insurers to charge "too high premiums for first party policies" (Dedeke 2017). Moreover, there is the general fear that a single IT failure by a widespread vendor could impact "a large part of the economy and that the risk will be borne by the insurance industry" (Keegan 2014), further limiting such insurance policies. Furthermore, Dedeke (2017) argued that the quantification and clarification of covered cyber-related losses is difficult, as well as the assignment of liability.

3.12 Growth

Learning as a supply chain resilience concept refers to seeking improvement through the opportunities that emerge in the post-disruption phase and thrive in the long-term, well beyond the recovery from a risk event, learning from the past and making improvements (Herrera & Janczewski 2015, Ali et al. 2017).

In the literature, it has also been referred to as "growth", which seems to have started being generally considered as a relevant part of supply chain resilience only since the beginning of this decade, being consistently reckoned as important since then (Ali et al. 2017).

We identify two important elements relative to learning, which are consistent with the division proposed by Ali et al. (2017): *post-event knowledge management* and *building social capital*.

3.12.1 Post-Event Knowledge Management

Post-event knowledge management focuses on enhancing the ability of the supply chain to learn from past events, through elements like post-event feedback, improvement through education and training, and gathering of cost/benefit knowledge (Ali et al. 2017), which can be used for updating contingency plans and innovating by improving or changing resilience mechanisms (Herrera & Janczewski 2015).

Therefore, some elements proposed for pre-event knowledge management, like those described in section 3.7 are also useful in post-event knowledge management, like education and training in regards to information security, and the embeddedness of key learnings in the organisational security culture.

In the context of supply chain cyber risk management, digital forensics are also proposed as a way to learn from past incidents after the return to normal operations (Miyamoto et al. 2017), easing the possibility to answer key questions of an incident like "what, why, how, who, when and where" (Ab Rahman et al. 2016).

In Estay & Khan (2015) and Estay & Khan (2017), a framework was developed to represent the resilient response to a cyber-attack, considering system dynamics theory to it, which can be used to depict the cross-disciplinary processes that occurred in an organisation when it managed past disruptions. Estay & Khan (2017) defend that this tool is suitable for "undertaking a medium to long-term timeframe analysis of the problems related to the effects of cyber risks in operations", as well as when there is "limited information available about past events of resilient response to cyber-attacks".

Another tool that could be used for the quantification of the dynamic effects of a past cyber-attack is the representation of KPI performance over time, as also proposed in another tool by Estay & Khan (2015).

3.12.2 Social Capital

Social capital can be seen as the network of relationships formed with suppliers, which can also be seen as a valuable asset, and an enduring source of advantage (Carey et al. 2011). The existence of social capital in the context of supply chain resilience can lead to an strengthened ability among the supply chain partners to learn from each other, as a result of inter-organisational relationships and relational competence (Ali et al. 2017).

Johnson et al. (2013) discuss about the role of social capital in facilitating supply chain resilience by defining the term as "the information, trust and norms of reciprocity inhering within social networks" and linking it to the resilient concepts of absorbing shock and adapting to change. To explain the links between both areas (social capital and resilience), they define three social capital dimensions: *structural mechanisms*, *cognitive processes* and *relational*. Examples of structural mechanisms are network ties and network configuration; cognitive processes refer to shared codes, language and narratives, and the relational component to the development of trust, expectations and obligations.

However, this taxonomy shares many similarities with the three IT governance dimensions described by Peterson (2004) - structural, process and relational governance capabilities -, which gives room to argue that building social capital has at least some correlation to good governance mechanisms. In fact, it has been proved that under certain conditions (like supply uncertainty), relational governance can lead to the formation of social capital (Carey et al. 2011, Carey & Lawson 2011).

Moreover, it is possible to nurture social capital deliberately or without design (Johnson et al. 2013). Therefore, in this thesis the concept of supply chain IT governance is defined in the pre-event phase, where social capital is created and made available to use in the post-event phase, while it is argued that the social capital left in the aftermath of a cyber-disruption is used as a building block in the process of supply chain learning and improvement.

The reviewed literature in the topic of managing supply chain cyber risks was found to seldom directly discuss this concept of building improvements from social capital, although different elements linked to it through relational governance (like trust, strong communication and sense of understanding) are regarded as important by several authors (for example Boyson (2014), Sabbagh & Kowalski (2015), Polemi & Papastergiou (2016)).

4 Analysis

The results of the literature review were presented in section 3, in an attempt answering the research questions RQ1.1 and RQ1.2.

Now, the purpose of this section is to analyse the results obtained, explicitly addressing the research sub-question RQ1.3, by arguing for a way in which the found constructs from the literature can be put together, improving conceptual clarity over the area of supply chain cyber risk management.

4.1 Linking the Constructs: a Dynamic SCCRM Framework

Throughout the collection and presentation of the review results, it was observed that the proposed dynamic view turned out to be a good fit for structuring the information provided by the different identified themes.

First, taking a hypothetical risk event as a point of reference in time leads to the identification of elements belonging to at least one of three different stages (pre, during and post, a seen in figure 13). They basically differ from each other on how far they are from the moment in time in which a risk event occurs, and whether they take place before or after said risk event.

Figure 13: Pre, during and post risk event

Then, this dynamic approach allows to position all the previously discussed themes in a sort of timeline which gives a sense of how each element interacts in time, both with the prevention of, response to, and recovery from cyber risk events, as well as with the long-term view associated to them.

Following this time perspective, the main elements from section 3 are now represented against the line time, in figure 14. In section 3, it was discussed how *Compliance* can be regarded as the precedent for the management of cyber risks, where the risks and security standards to conform to exert influence into the risk assessment process (Gaudenzi & Siciliano 2018), which forms part of *Situation Awareness*. According to Ali et al. (2017), good situation awareness in the context of supply chain resilience leads to the understanding of the vulnerabilities of the supply chain and the planning for such events, such as the elaboration of early warning strategies or continuity planning, and the identification of supporting elements needed for them like information sharing, coordination and the availability of knowledge. Therefore, it is understood that situation awareness is also needed early in the process of SCCRM.

As also argued before, IT *Governance* feeds on the outcomes from compliance and situation awareness (Gaudenzi & Siciliano 2018), defining how IT-related decisions should be made across the organisation and the supply chain to manage cyber risks. The previous elements define what knowledge should be created and nurtured among the members of the organisation and the supply chain when it comes to managing cyber risks, which is achieved through proper *Knowledge Management* previous to the realisation of the risk event (Ali et al. 2017).

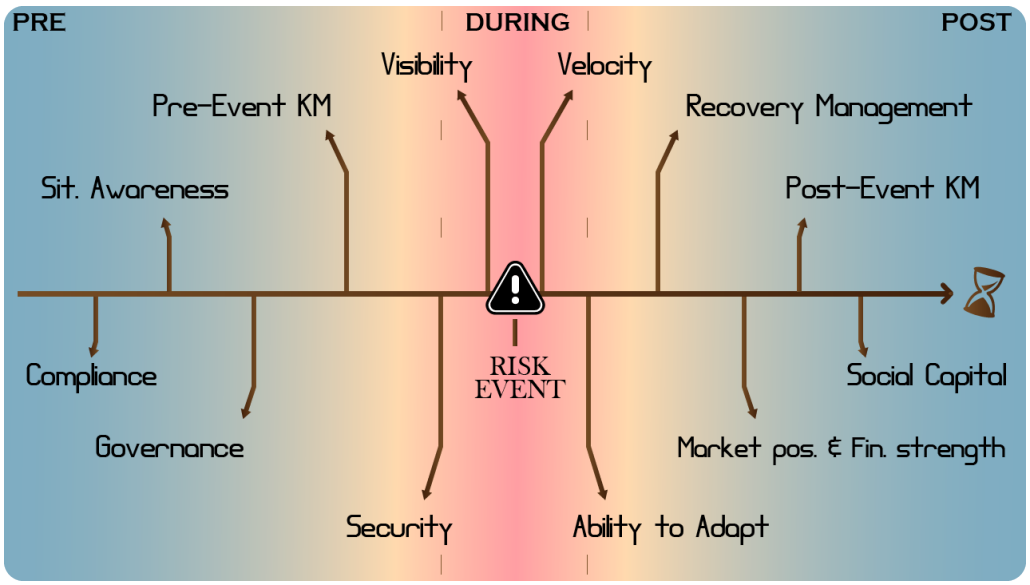

Figure 14: SCCRM themes from a chronological perspective

Cyber *Security* mechanisms must be in place to prevent the exploitation of vulnerabilities from adversaries, and protect the goals of the supply chain from incoming threats (Goldman et al. 2011). However, if the security in place is not enough to stop the cyber-threat, then enough supply chain *Visibility* is needed to ensure that a cyberattack is discovered, (hopefully) before it has caused significant damage (Pettit et al. 2010).

If the cyber event is spotted, then *Velocity* mechanisms are needed to allow for a fast response (Christopher & Peck 2004). In the chaos of a disruption, the *Ability to Adapt* is instrumental to allow continuity of operations, through for example a flexible redistribution of resources through different processes and use of previously redundant capacity (Ali et al. 2017).

The existence of *Recovery Management* programs helps in prioritising the resources and coordinated actions needed throughout the supply chain to recover from a cyber-disruption, by providing valid contingency plans and ensuring the availability of resources needed to return the enterprise to the normal state (Torabi et al. 2016). If it turns out that there are no contingencies available, or they are not enough, then the company will rely solely on absorbing the damage through its *Market Position and Financial Strength* (Pettit et al. 2010).

When (and if) the mission recovers from the disruption, it is important to use the very valuable learnings gained through the experience to update and improve the practices across the different SCCRM mechanisms previously described, through proper *Post-Event Knowledge Management* (Ali et al. 2017). Finally, the *Social Capital* that is formed in turbulent times is also a valuable asset, that can enhance collaborative attitudes across different levels in the supply chain, towards a better management of the common risks faced and the exploitation of new opportunities (Johnson et al. 2013).

On top of this, this sense of distance in time can allow for other ways of approaching the problem, with the introduction of concepts like strategic and tactical elements, as depicted in figure 15.

In a way, if we understand strategic elements as those that look at the problem from a more long-termed point of view, and tactical mechanisms as those that approach it from a shorter time span, then this division allows to identify mechanisms that are more relevant in either the short (tactical) or the long (strategical) term, before and/or after the realisation of a risk event, and how they can complement each other in carrying out a holistic approach towards the management of cyber risks in the supply chain.

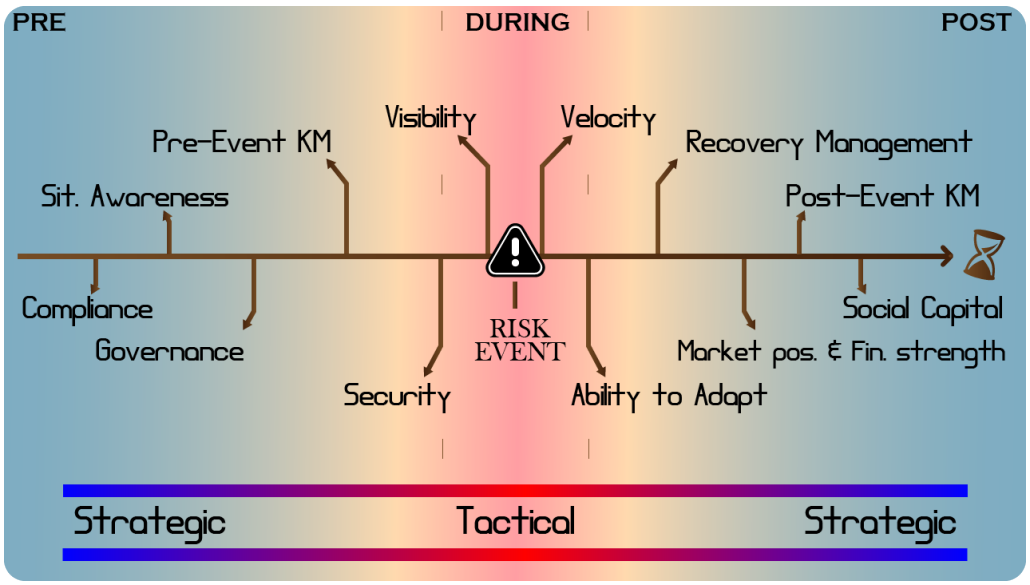

Figure 15: Strategic vs Tactical SCCRM themes

4.2 Understanding the Framework: the Impact-Wave Analogy

As it has been mentioned before, the findings presented throughout this work draw knowledge from areas like supply chain risk and resilience management, and cybersecurity. A number of concepts that are important to those fields are the prevention of risks, the protection against them, and the mitigation of their impact when they occur.

From the perspective of the proposed framework, those concepts have found a place in it and we believe that their interaction can be better presented through the use of an analogy, which considers the ripple or wave created by an impact against a surface (e.g. water), as in figure 16.

Figure 16: Ripples from a drop on water. Taken from Pexels (2018)

As part of this analogy, the problem is looked at from the perspective of an organisation (namely the *focal organisation*) which forms part of a supply chain, and represented through the previous framework. The point of reference in time is in this case understood as the "*point of impact*" in which a cyber-event "*hits*" the organisation. See figure 17.

Looking at the time variable, in order for a risk to successfully impact the organisation, it has to cut across a number of defensive mechanisms on the left side, which can be relatively far in time (strategic mechanisms) or close (tactic/operational mechanisms). They can also be understood as *lines of defence*. See figure 18.

When the lines of defence are not able to stop the occurrence of a cyber-event, an *impact* occurs. This impact then creates a "shock wave", or a "ripple", that can expand in time as shown in figure 19. The magnitude of those waves and their reach will depend on a number of factors. On the left side of the framework, there are the elements that can reduce the strength of (or even stop) the impact (i.e., in this analogy the speed at which the cyber-bullet impacts the system), which will directly affect the magnitude of the shock wave on impact. However, the function of the elements

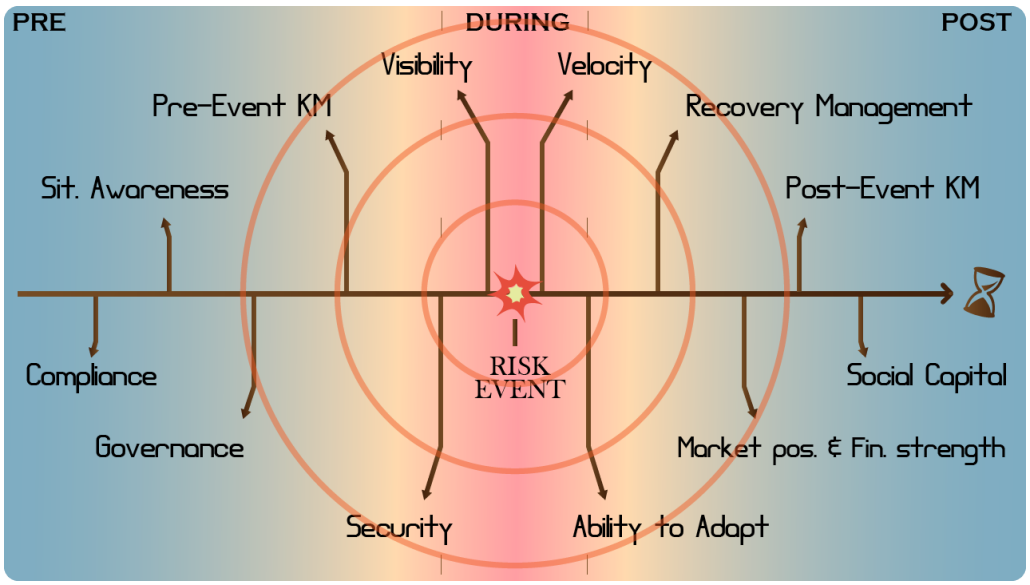

Figure 17: The impact of a successful cyber attack can be "felt" over a period of time

placed on the right side of the framework is to mitigate the "disastrous" effects of those waves, absorbing them. For the sake of this analogy, it can be understood that these waves are able to reach as far as the next absorption mechanism in place is able to absorb a shock wave of equal or bigger magnitude. If a wave is stronger than what a certain mechanism is able to absorb, then its effects will continue to spread and the next mechanism in time will have to actuate, until the shock wave is stopped.

On the left side, it could be that the regulatory requirements are not enough to adequately address a certain cyber-threat. If this threat is not made aware of as part of the risk identification and assessment process, then different governing processes and structures may not be in place to correctly address them, and the knowledge (KM) needed to treat it will not be there either. It could also happen that this cyber-attacker, making use of an inherent vulnerability in the system, is able to avoid the cyber security in place. Then, needless to say, if the Visibility mechanisms are not designed to detect the actions of a cyber-attack that whose possibility has not been identified before, the organisation might have been hit by a cyber-event without (maybe) being able to notice it.

For example, if a cyber-breach occurs and the Visibility and Velocity mechanisms in place are not able to detect and react to the attack fast enough, then Adaptive mechanisms could also be not enough to contain and stop it from spreading and/or allowing the attackers to take a foothold into the IT systems of the organisation. If such a breach escalates, then the organisation starts relying on the existence of contingency plans to recover from the disruption, together with facing a test on its financial and market strength. A chain of events with similar narrative after the cyber-attack to this one was also shown in the case study presented by Estay & Khan (2017), where IP theft stemming from a previously unnoticed cyber-attack led to the company facing technical and financial challenges.

Coming back to the analogy, if an organisation is not able to stop this "wave", then the "disaster" could become comparable to that of a "cyber-tsunami", in which the continuity of the company's mission is at stake. Maybe the effects of a cyber-tsunami (figure 20) are not the same as a real one but, even though an organisation's physical assets might still be there for some more time, their business model could have been left ineffective, due to financial unsustainability as a consequence of, for example, loss of competitive advantage (from IP theft), reputation, increased costs or technical impossibility of continuing critical operations within a reasonable timeframe.

At this point, the only things left for the organisation might be their social capital (like the personal and collective knowledge contained in the organisation, and the value of the network of personal relations formed within the value chain), and learning from past experiences, which could be used to innovate and build a new start for the organisation, if so.

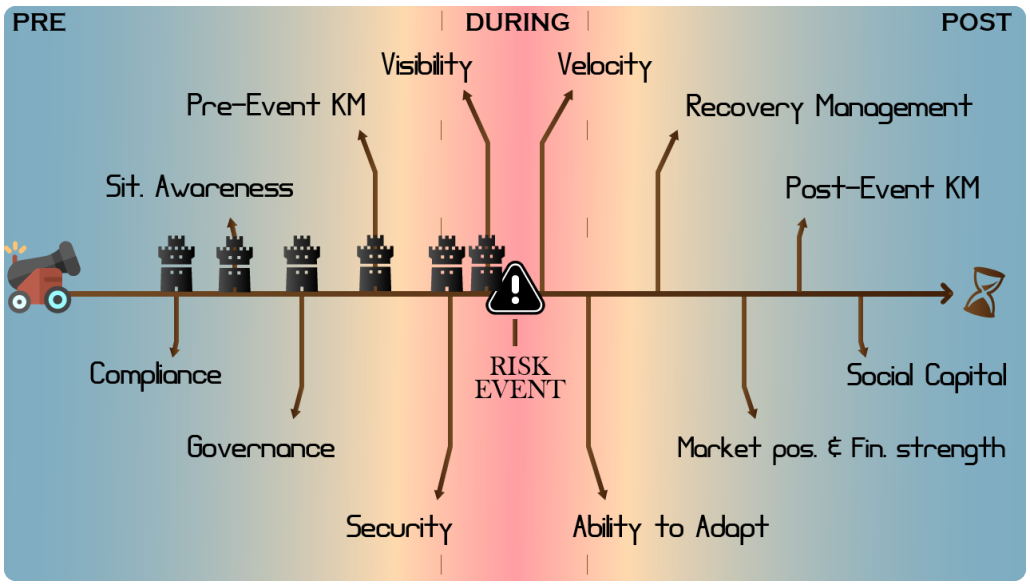

Figure 18: A cyber attack, understood as a cannon ball that will try to penetrate the different lines of defence in place

4.3 Closing the Loop: Organisational Learning and Resilience

As described in section 3.12, it seems that it has only been since this decade that the idea of considering disruptive events as learning and growth opportunities took a consistent hold in the supply chain resilience literature (Ali et al. 2017).

Nonetheless, learning from cyber-events can also be represented in the proposed framework. For this, further organisational learning theory has to be brought to the scene, being applied in the context of supply chain cyber resilience in a way that, to the best of our knowledge, has not been done yet.

This will be done through the introduction of the concepts of single-loop learning and double-loop learning, firstly described by Argyris & Schön (1978).

Both concepts attempt to represent the way experience is used to learn and modify future behaviour, and therefore improve performance. A depiction of both models can be seen on figure 21. On one side, single-loop learning relates to using the feedback collected from the detection and correction of errors to collectively refine the rules under which the organisation operates and finding ways of "doing things better", but "without challenging the governing variables" (Hayes 2014). Double-loop learning, on the other side, can lead to the development of a new shared mental model, challenging the "accepted ways of thinking", and doing things differently or even doing better things (Hayes 2014).

According to Hayes (2014), double-loop collective learning tends to occur when some type of crisis or incongruous events "that violate conceptual frameworks" take place. In those cases, feedback points at the need to re-examine the fitness of the shared mental model.

Applied to the management of cyber risk in the supply chain, it makes sense that those risk events that cause minimal damage, will have smaller effects in the change of the system, meaning that the feedback collected from them will tend to be used for improving the different resilience mechanisms in place in a more incremental way - for example, through in creases in the cybersecurity mechanisms, to prevent the system from some vulnerabilities, or the implementation of agility mechanisms to detect the event faster, or the development of contingency plans for that specific risk. Moreover, in practice it has been seen that recovering from the "crisis situation" created by a cyber-breach can lead to the collective realising the need to make more profound changes in the way cyber-risks are handled (Social-engineer 2015). In the proposed framework, these single- and double-learning loops could be conceptually represented as depicted in figure 22.

The way figure 22 should be understood is that, depending on how deeply a cyber-event impacts

an organisation, the deeper will tend to be the learning and changes derived from the recovery process. Feedback loops do not travel back in time -as the figure could seem to suggest-, but they affect elements in the pre-event phase of a future hypothetical cyber-risk event, which will have a more strategic impact the stronger the realisation for a need of change on how things are done is.

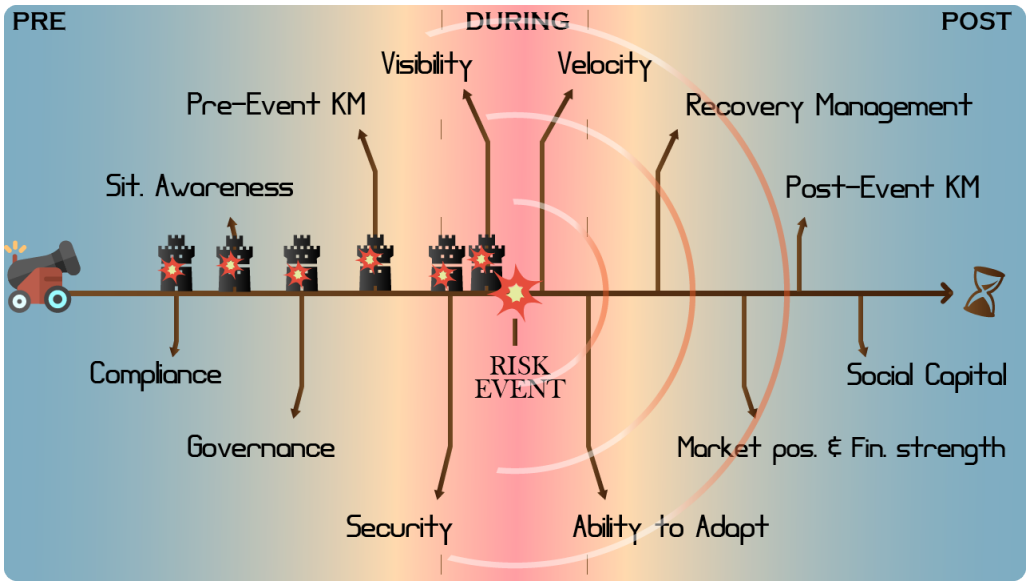

Figure 19: Analogy of a successful cyber attack

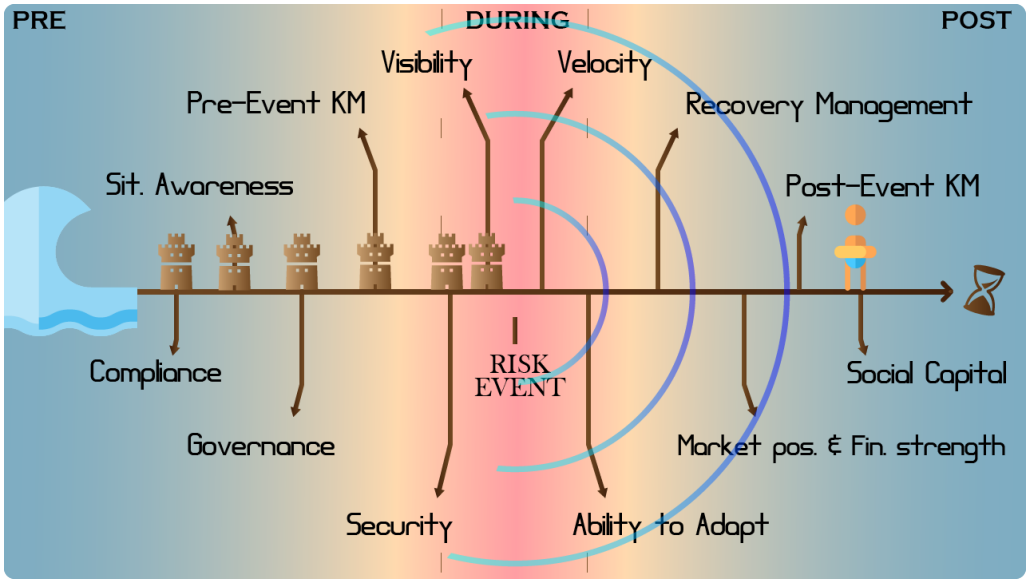

Figure 20: The analogy of a cyber-tsunami

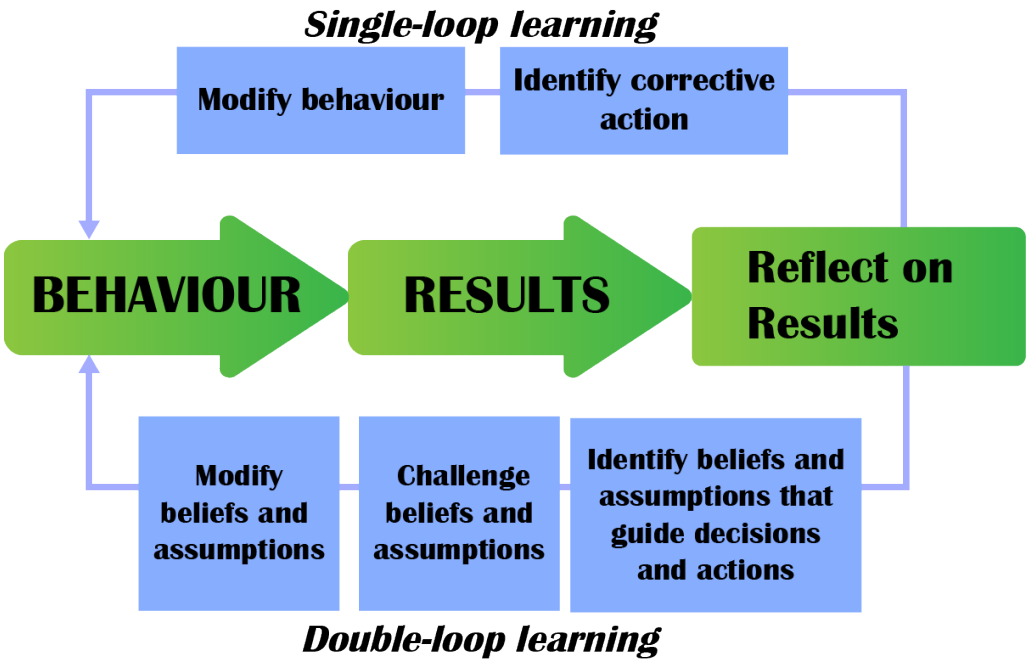

Figure 21: Single- and double-loops of learning. Adapted from Hayes (2014)

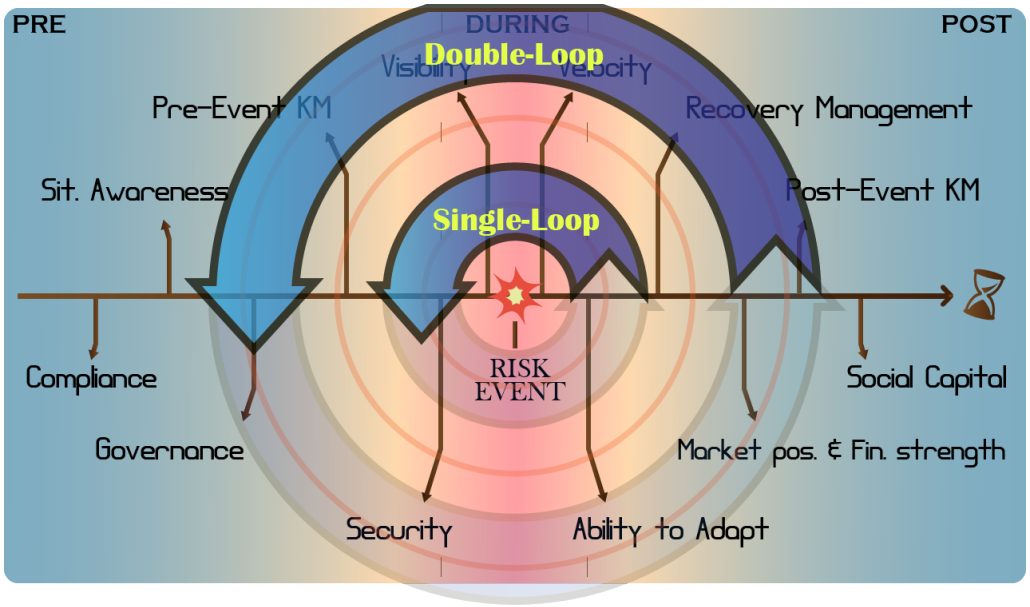

Figure 22: Single- and double-loop learning on the SCCRM framework

5 Discussion and Improvement Suggestions

In this section a discussion is presented regarding the validity of the methodology and the results obtained. In parallel, recommendations for improvement are suggested.

5.1 Regarding the methodology

The validity of the methodology is measured by how suitable it is to answer the research question and sub-questions. On one hand, the choice of using a structured literature review process seemed to fit very well with the research question and the context of the area of knowledge to be researched. The reasons for this are related to the fact that the field of supply chain cyber risk management is relatively new and growing at an increased pace. Its body of knowledge and terminology do not seem to be unified yet, and continuous advancements in the field make difficult to keep track of it, tied to the lack of journals of reference in the area.

Therefore, venturing into the effort of unifying the knowledge encompassed in this field requires an approach like the SLR, which can lead to validation of the results in terms of its replicability, through a clearly defined and transparent process. These aspects were particularly emphasised both in the description of the methodology used and in the presentation of the results of the process.

On the other hand, one of the points in which the validity of the methodology employed could be argued is in the existence of biases. In this regard, Durach et al. (2017) mention a number of four potential biases as part of the SLR process, which are now debated.

The first one is the sampling bias. According to Durach et al. (2017), it could come from a base sample that is inadequate or incomplete due to the search. The way this was dealt with in this thesis was by doing a preliminary search and reading a few publications in the field, with the aim of identifying the most common terminology in the area, apart from using multiple (eight) combinations of key terms. Another potential bias mentioned by Durach et al. (2017) could come from choosing only publications from leading journals, as those tend to be groundbreaking and not representative of the field. However, as it was mentioned, this field is relatively new and its body of research growing more each year (doubling every 2-3 years), so there is a lack of general literature associated to it, and "ground-breaking" publications are the normal in this situation.

Secondly, there is the bias inherent in the coding of the findings. In our case, this could mean that a relevant finding gets identified under the wrong theme, potentially leading to an incorrect outcome of the review. There is only one reviewer doing this task, it was not possible to involve more people in this process because of its high requirements in the workload. The only way to mitigate this bias was through carrying out different iterations: the findings under each theme were checked at least three times before the final writing of the thesis, reducing the risk of being coded wrongly by mistake (though not mitigating the reviewer's bias).

Third, there is the risk of synthesising the data wrongly due to biases in the expectation of the reviewer, who is influence by conscious and unconscious expectations about the final results. To mitigate this risk, it was considered that a key in this process would be the identification of the "right" themes under which the findings would represent better the reality of the field. Because of this, the identification of themes was thought of early in the process (when reading titles and abstracts), and allowed to identify more than were needed, which then were dynamically modified along the review process, to better encompass the different bodies of relevant findings.

Fourth, another bias comes from the selection process. On one side, there is the risk of inaccurately designing the selection criteria, therefore not including relevant literature. Another risk is the inclusion of articles that lead to incorrect results, due to the subjectivity of the inclusion process and bias in the selector (Durach et al. 2017). Transparency was integrated in the process to allow for the discovery of this bias, if existing, through a description of the methodology that was as thorough as possible, while providing detailed accounts (to the best of our capabilities) on the results obtained, which should also enable others to assert on the appropriateness of the criteria and results.

Another step taken in this direction, as to minimise the existing bias, was to devise two stages for the selection of the relevant literature, which theoretically should lead to a better judgement of the reviewer which comes from learning through the process. However, the final number of publications which met the inclusion criteria turned out to be too big, and almost half of it could not be analysed due to constraints from the time-resource available.

One of the ways of having avoided this could have been the design of more restrictive inclusion criteria, or search results. Nonetheless, according to the defined research question, the non-read 103 publications that were identified as valid do also answer it, and redefining the search results to reduce the sample size would actually rule out valid publications.

Therefore, it is argued that the size of the sample considered to meet the inclusion criteria (284 publications) is still valid and relevant for answering the research question, and it should be the amount reviewed to fully answer it, but it was not possible to fully approach it with the available resources. This way, a better solution would have been to either develop this work with two reviewers (e.g. two thesis writers) instead of just one, or to scale down the ambition of the research question to better fit and represent the amount of work needed for the completion of the thesis.

Apart from this, a few observations can be made on the use of two stages in differentiating between publications to include and exclude from the initial sample. Firstly, a great difference was noticed in the efficiency of the labelling process between the first and the second round of labelling, meaning that the second time it happened at a noticeably faster pace. Secondly, the increase in experience and knowledge of the topic by the reviewer also made a big difference in the review process, where the number of publications labelled as "Maybe" meeting the inclusion criteria was reduced from 304 to 12, from only reading their titles and abstracts, leaving 103 more articles as "meeting the criteria". Because of this, it is believed that this process actually would save time towards the overall SLR process, only that this time there were too many valid articles in the initial sample as to possibly review them all with the time available.

5.2 Regarding the Results

The validity and value of the results obtained must be measured against how well they answer the research question and sub-questions. Certainly, the amount of publications reviewed already provides a valuable insight into how cyber risks should be managed in the supply chain, by giving answers into what the risks related to the use of IT systems in the supply chain are; what tools, practices and constructs could be used to manage them, and how they can be linked to make sense of the body of knowledge created.

Unfortunately, due to the impossibility of reviewing the whole lot of selected publications, it should be discussed whether the literature reviewed is actually representative enough of the field and whether this has led to reach valid results.

Here, it is conceded that the existence of other valuable approaches and constructs in the literature not-reviewed (103 publications) cannot be confirmed or discarded unless they are also reviewed. The completeness of the results can be, indeed, argued. However, it can also be said that, if a certain theme or construct is not mentioned in any of the 123 publications reviewed, then it could be either not regarded as important in the general body of knowledge, or the awareness of its existence and relevance has not reached the wider public yet, in which case it would not form part of the main current or past trends of the field, either. Therefore, the results obtained from the 123 publications reviewed do provide valuable answers and insights to the research question.

Finally, regarding the validity of the framework proposed, it seen that the findings from the literature reviewed fit fairly well within the proposed themes. In other words, to proposed tool seems to internally correlate with the findings of this thesis. Furthermore, to enhance the understanding and potential applicability of the proposed framework, an analogy and a narrative that links the different concepts discussed throughout this thesis are also proposed. However, some work needs to be done in order to prove the external validity of the results, which means, how much it can be, in fact, generalised. This could be done, for example, through the use of cases, which outreaches the scope of this thesis.

6 Contributions to Theory and Practice

The contributions of this thesis are various. Firstly, this thesis provides a detailed methodology for conducting Structured Literature Reviews in the area of SCCRM, based on the one described by Durach et al. (2017), but with a few modifications that on themselves can be considered as one of the contributions made to this field. To the best of our knowledge, this methodology innovates in a few points of the process, such as dynamically structuring information into themes to better fit the findings from the literature review, or the use of two stages to better identify publications that meet the inclusion criteria.

Moreover, the metrics that the use of structured spreadsheets allow to obtain provided the following insights into the field of SCCRM:

- The two search engines DTU Findit and Scopus are complementary to each other in the field of SCCRM, each of them providing unique results that vary between a 24-32% of the total for each of them, on average, with the key terms proposed. These results have an added value in the context of setting some boundaries to the replicability of this process in other contexts: the use of different search engines may indeed affect the baseline sample to analyse, despite of using of the exact same search terms.
- The "success ratio" is used to measure how effective different combinations of key terms are at returning relevant publications in the field of SCRM. Knowing what combinations of key terms produce better results may also help in a better selection of those key terms in the future, and improve efficiency later in the process due to a reduced presence of publications not meeting the inclusion criteria.
- The academic interest for the field of SCCRM seems to be growing exponentially, with the total number of existing publications in this area being doubled every 2-3 years since the year 2000.
- There is no current journal of reference for the publication of scientific articles in this field.

On the other side, a list of publications that can be directly related to the field of SCCRM has been created, which can be seen on appendix A, encompassing all the publications found to relate to this area from 2000 to February 2018. This should ease future research carried out on this field.

Moreover, from an academic perspective, this work has contributed to the area of SCCRM by analysing an important part of the literature available on this topic, providing a comprehensive overview of the current state of development of the field, and proposing to structure all the knowledge of the SCCRM into different main themes, following a taxonomy that seems to correlate well with the findings obtained from each publication.

This thesis contributes to the practice in the area of supply chain cyber risk management by providing a framework that is able to link the most important themes from this field of knowledge, plus further incorporating other features that are not often observed in this area, like single- and double-learning loops to explain some behaviours and change of the system over time, after suffering a cyber-disruption. To the best of our knowledge, this is the first time a result of this characteristics has been shown in the area of SCCRM.

This framework makes use of a dynamic perspective, in which all the themes belong to a moment in time that is either pre-, during-, or post- risk event. Said elements, which can be seen in figure 23, can also be understood as strategic or tactical when it comes to managing a cyber risk event, depending on their position and distance in time to a hypothetical cyber-risk event.

Finally, it is also assumed that the terminology used, the themes shown on the framework, and they way in which they are laid, may change if this research is to be repeated in the future, because of new knowledge added to the field. Nonetheless, this framework has didactic value, as it has been shown its flexibility towards illustrating several concepts that are relevant to SCCRM. Through analogies like the shock-wave, as shown in figure 24 it allows for the representation of the defined SCCRM field in a way that is very graphic and at some extent intuitive, when permitting the use of a narrative that makes easier the description of the different elements involved in the management of a cyber-risk event, and their interrelationships.

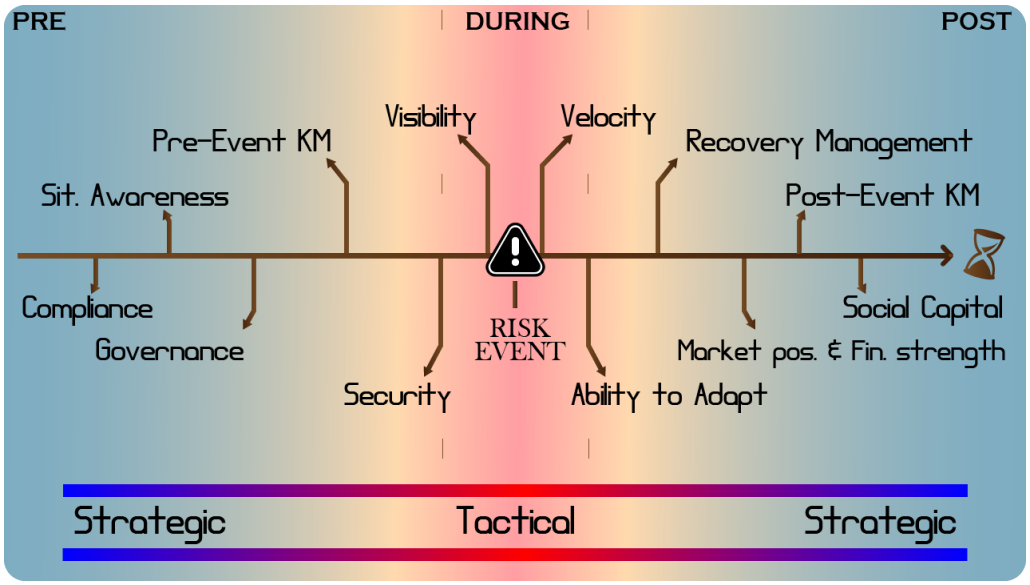

Figure 23: Strategic vs Tactical SCCRM themes

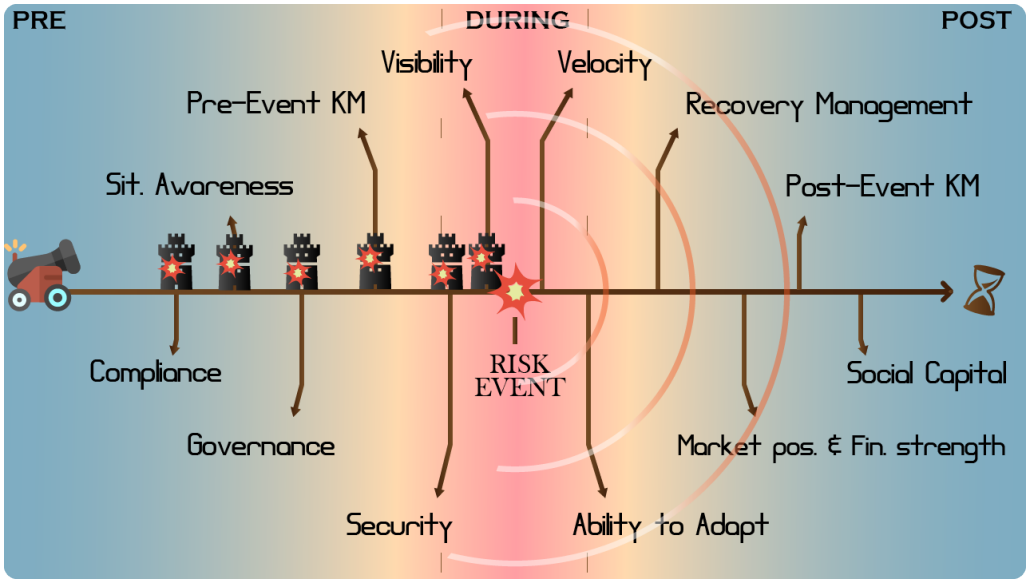

Figure 24: A successful cyber attack

7 Conclusions

Nowadays, the presence of IT systems and the cyberspace within industries and supply chains has become more relevant than ever before, driven by technological movements like the "fourth industrial revolution" (Industry 4.0), the Internet of Things and Big Data. However, as it is shown throughout this document, the integration of any such elements comes inherent with new vulnerabilities and risks, opening the doors of not only single organisations, but also their supply chain partners, to a different type of risks for which traditional risk management approaches seem not to be enough.

In fact, it has been seen that in recent years the field of supply chain cyber risk management has seen an exponential growth in the interest it attracts. Nonetheless, it is still a very young field and its body of knowledge is also scattered all around the research community.

To answer the research question, "*How should the risks derived from the use of IT systems be managed along the supply chain?*", a literature review on the field of supply chain cyber risk management (SCCRM) is conducted, gathering a significant amount of knowledge applied in this area. Then this knowledge is structured in a way that tries to best reflect the most relevant findings. For this, different themes are identified with the purpose of providing a taxonomy that gives a better overview of the existing tools, practices and constructs proposed in the scientific literature to manage supply chain cyber risks. To provide conceptual clarity, those constructs are linked through the proposition of a SCCRM framework, where all the previously identified themes can be analysed from a time-dynamic perspective.

Although some potential improvement points are discussed, we believe that the methodology, results and analysis presented here contribute to the field of Supply Chain Cyber Risk Management, bringing its currently disperse knowledge a bit closer together.

References

Ab Rahman, N. H., Glisson, W. B., Yang, Y. & Choo, K.-K. R. (2016), 'Forensic-by-Design Framework for Cyber- Physical Cloud Systems', *IEEE Cloud Computing* **3**(1), 50–59.
URL: *https://www-computer-org.ezproxy.umuc.edu/csdl/mags/cd/2016/01/mcd2016010050.pdf*

Alam, M., Tehranipoor, M. M. & Guin, U. (2017), 'TSensors Vision, Infrastructure and Security Challenges in Trillion Sensor Era', *Journal of Hardware and Systems Security* **1**(4), 311–327.

Alexander, S. D. (2012), 'Trust engineering - Rejecting the tyranny of the weakest link', *ACM International Conference Proceeding Series* pp. 145–148.

Alhogail, A. (2015), 'Design and validation of information security culture framework', *Computers in Human Behavior* **49**, 567–575.
URL: *http://dx.doi.org/10.1016/j.chb.2015.03.054*

Ali, A., Mahfouz, A. & Arisha, A. (2017), 'Analysing supply chain resilience: integrating the constructs in a concept mapping framework via a systematic literature review', *Supply Chain Management: An International Journal* **22**(1), 16–39.
URL: *http://www.emeraldinsight.com/doi/10.1108/SCM-06-2016-0197*

Ali, S., Ibrahim, M., Rajendran, J., Sinanoglu, O. & Chakrabarty, K. (2016), 'Supply-Chain Security of Digital Microfluidic Biochips', *Computer* **49**(8), 36–43.

Almadhoob, A. & Valverde, R. (2014), 'Cybercrime Prevention in the Kingdom of Bahrain Via It Security Audit Plans', *Journal of Theoretical and Applied Information Technology* **10**(651), 274–292.

Argyris, C. & Schön, D. a. (1978), 'Organizational Learning: A Theory of Action Perspective', *The Journal of Applied Behavioral Science* **15**(4), 542–548.

Axelrod, C. W. (2013), 'Using transaction-level simulation to prepare for and recover from supply-chain disasters', *2013 IEEE International Conference on Technologies for Homeland Security, HST 2013* pp. 338–343.

Axelrod, C. W. (2014), 'Malware, "weakware," and the security of software supply chains', *CrossTalk* **27**(2), 20–24.

Babun, L., Aksu, H. & Uluagac, A. S. (2017), 'Identifying counterfeit smart grid devices: A lightweight system level framework', *IEEE International Conference on Communications* .

Baldwin, K., Miller, J. F., Popick, P. R. & Goodnight, J. (2012), 'The United States Department of Defense revitalization of system security engineering through program protection', *Systems Conference (SysCon), 2012 IEEE International* pp. 1–7.

Bandyopadhyay, T., Jacob, V. & 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* **11**(1), 7–23.

Barreto, L., Amaral, A. & Pereira, T. (2017), 'Industry 4.0 implications in logistics: an overview', *Procedia Manufacturing* **13**, 1245–1252.
URL: *https://doi.org/10.1016/j.promfg.2017.09.045*

Bartol, N. (2014), 'Cyber supply chain security practices DNA - Filling in the puzzle using a diverse set of disciplines', *Technovation* **34**(7), 354–361.
URL: *http://dx.doi.org/10.1016/j.technovation.2014.01.005*

Bodeau, D. J., Graubart, R. & Fabius-Greene, J. (2010), 'Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels', *Proceedings - SocialCom 2010: 2nd IEEE International Conference on Social Computing, PASSAT 2010: 2nd IEEE International Conference on Privacy, Security, Risk and Trust* pp. 1147–1152.

Boyes, H. (2015), 'Cybersecurity and Cyber-Resilient Supply Chains', *Technology Innovation Management Review* **5**(4), 28–34.

Boyson, S. (2014), 'Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems', *Technovation* **34**(7), 342–353.
URL: *http://dx.doi.org/10.1016/j.technovation.2014.02.001*

Caldwell, T. (2015), 'Securing small businesses - The weakest link in a supply chain?', *Computer Fraud and Security* **2015**(9), 5–10.
URL: *http://dx.doi.org/10.1016/S1361-3723(15)30083-X*

Cambridge-Dictionary (2018), 'Definition of 'risk' in the online cambridge dictionary'. Accessed on 20.04.2018.
URL: *https://dictionary.cambridge.org/dictionary/english/risk*

Carey, S. & Lawson, B. (2011), 'Governance and social capital formation in buyer-supplier relationships', *Journal of Manufacturing Technology Management* **22**(2), 152–170.
URL: *http://www.emeraldinsight.com/doi/10.1108/17410381111102199*

Carey, S., Lawson, B. & Krause, D. R. (2011), 'Social capital configuration, legal bonds and performance in buyer-supplier relationships', *Journal of Operations Management* **29**(4), 277–288.

Chabinsky, S. (2014), 'Cybersecurity Risk Management', *Security* **51**(2), 38.

Christopher, M. & Peck, H. (2004), 'BUILDING THE RESILIENT SUPPLY CHAIN', *International Journal of Logistics Management* **15**(2), 1–13.

Couce-Vieira, A. & Houmb, S. H. (2016), Computer Safety, Reliability, and Security, *in* A. Skavhaug, J. Guiochet, E. Schoitsch & F. Bitsch, eds, 'Computer Safety, Reliability, and Security', Springer International Publishing, pp. 246–255.
URL: *http://link.springer.com/10.1007/978-3-319-45480-1*

Croll, P. R. & George, K. (2007), 'Engineering for Systems Assurance - a State of the Practice Report', *IEEE Systems Conference* pp. 1–7.

Daniele, P., Maugeri, A. & Nagurney, A. (2017), Operations Research, Engineering, and Cyber Security, *in* 'Operations Research, Engineering, and Cyber Security', Vol. 113, Springer Optimization and Its Applications, pp. 117–134.
URL: *http://link.springer.com/10.1007/978-3-319-51500-7*

Dedeke, A. (2017), 'Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles', *IEEE Security and Privacy* **15**(5), 47–54.

Demchak, C. C. (2012), 'Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)', *Journal of Comparative Policy Analysis: Research and Practice* **14**(3), 254–269.

DHS (2018), 'Critical infrastructure sectors: Department of homeland security'. Accessed on 20.04.2018.
URL: *https://www.dhs.gov/critical-infrastructure-sectors*

Dofe, J. & Yu, Q. (2018), 'Novel dynamic state-deflection method for gate-level design obfuscation', *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* **37**(2), 273–285.

Durach, C. F., Kembro, J. & Wieland, A. (2017), 'A New Paradigm for Systematic Literature Reviews in Supply Chain Management', *Journal of Supply Chain Management* **53**(4), 67–85.

Durowoju, O. A., Chan, H. K. & Wang, X. (2012), 'Entropy assessment of supply chain disruption', *Journal of Manufacturing Technology Management* **23**(8), 998–1014.
URL: *http://www.emeraldinsight.com/doi/10.1108/17410381211276844*

Dutcher, D. (2013), 'How do cyber threats affect petrochemical risk models ?', *Hydrocarbon Processing* **92**(11), 51–55.

Duzha, A., Gouvas, P. & Canepa, M. (2017), 'MITIGATE: An innovative cyber-security maritime supply chain risk management system', *CEUR Workshop Proceedings* **1816**(653212), 248–252.

Dynes, S. (2006), Information Security Investment Case Study : The Manufacturing Sector, Technical report, Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover, New Hampshire.

EC (2018), 'Critical infrastructure: European commission'. Accessed on 20.04.2018.
URL: *https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en*

Estay, D. A. S. & Khan, O. (2015), 'Extending supply chain risk and resilience frameworks to manage cyber risk', *Paper presented at 22nd EurOMA Conference, Neuchâtel, Switzerland* (July), 0–10.

Estay, D. A. S. & Khan, O. (2016), 'Control structures in supply chains as a way to manage unpredictable cyber-risks', *Paper presented at 5th World Production and Operations Management Conference, Havana, Cuba* .

Estay, D. A. S. & Khan, O. Q. (2017), A System Dynamics Case Study of Resilient Response to IP Theft from a Cyber- Attack, *in* '2017 International Conference on Industrial Engineering and Engineering Management (IEEM)', Suntec City, Singapore.

Farag, M. M., Lerner, L. W. & Patterson, C. D. (2012), 'Interacting with Hardware Trojans over a network', *Proceedings of the 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2012* pp. 69–74.

Filippini, R. & Silva, A. (2015), 'I-ML: An Infrastructure Resilience-Oriented Modeling Language.', *IEEE Transactions on Systems, Man & Cybernetics. Systems* **45**(1), 157–169.

Finnegan, A. & McCaffery, F. (2014), 'A security argument pattern for medical device assurance cases', *Proceedings - IEEE 25th International Symposium on Software Reliability Engineering Workshops, ISSREW 2014* pp. 220–225.

Forbes, L., Vu, H., Udrea, B., Hagar, H., Koutsoukos, X. D. & Yampolskiy, M. (2014), 'SecureCPS: Defending a nanosatellite cyber-physical system', *Proceedings of SPIE* **9085**(June 2014), 90850I.
URL: *http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2054162*

Frazier, P. D., Gilmore, E. T., Collins, I. J. & Chouikha, M. F. (2017), 'Novel counterfeit detection of integrated circuits via infrared analysis: A case study based on the Intel Cyclone II FPGAS', *Proceedings - International Conference on Machine Learning and Cybernetics* **1**, 404–409.

Gaudenzi, B. & Siciliano, G. (2017), 'Just do it: Managing it and cyber risks to protect the value creation', *Journal of Promotion Management* **23**(3), 372–385.

Gaudenzi, B. & Siciliano, G. (2018), Managing IT and Cyber Risks in Supply Chains, *in* 'Supply Chain Risk Management: Advanced Tools, Models, and Developments', Springer Singapore, Singapore, pp. 85–96.
URL: *http://link.springer.com/10.1007/978-981-10-4106-8*

Goertzel, K. M. (2013), 'Integrated Circuit Security Threats and Hardware Assurance Countermeasures', *CrossTalk* pp. 33–38.
URL: *http://www.crosstalkonline.org/storage/issue-archives/2013/201311/201311-Goertzel.pdf*

Goff, E., Glantz, C. & Massello, R. (2014), 'Cybersecurity procurement language for energy delivery systems', *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14* pp. 77–79.
URL: *http://dl.acm.org/citation.cfm?doid=2602087.2602097*

Goldman, H., McQuaid, R. & Picciotto, J. (2011), 'Cyber resilience for mission assurance', *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011* (April), 236–241.

Hale, J. C., Landry, T. D. & Wood, C. M. (2004), 'Susceptibility audits: A tool for safeguarding information assets', *Business Horizons* **47**(3), 59–66.

Hawrylak, P. J. & Hale, J. (2015), Medical Data Privacy Handbook, *in* 'Challenges in Synthesizing Surrogate PHI in Narrative EMRs', pp. 549–567.
URL: *http://link.springer.com/10.1007/978-3-319-23633-9*

Hayes, J. (2014), *The theory and practice of change management*, fourth edn, Palgrave Macmillan.

Häyhtiö, M. & Zaerens, K. (2017), 'A Comprehensive Assessment Model for Critical Infrastructure Protection', *Management and Production Engineering Review* **8**(4), 42–53.

He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y. & Gabrys, B. (2016), 'The security challenges in the iot enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence', *2016 IEEE Congress on Evolutionary Computation* pp. 1015–1021.

Herrera, A. & Janczewski, L. (2015), 'Cloud Supply Chain Resilience: A Coordination Approach', *2015 Information Security for South Africa (ISSA)* pp. 1–9.

Herrera, A. & Janczewski, L. (2016), 'Cloud supply chain resilience model: Development and validation', *Proceedings of the Annual Hawaii International Conference on System Sciences* **2016-March**, 3938–3947.

Hosseini, S. & Barker, K. (2016), 'A Bayesian network model for resilience-based supplier selection', *International Journal of Production Economics* **180**, 68–87.
URL: *http://dx.doi.org/10.1016/j.ijpe.2016.07.007*

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W. & Dornfeld, D. (2015), 'Framework for Identifying Cybersecurity Risks in Manufacturing', *Procedia Manufacturing* **1**, 47–63.

Infracritical (2018), 'Critical infrastructure sector map'. Accessed on 20.04.2018.
URL: *https://web.archive.org/web/20100213054539/http://www.infracritical.com/images/cip-sectors5.jpg*

ISO/IEC (2011), 'Iso/iec 27000 family – information security management systems. geneva, switzerland: Iso/iec'. Accessed on 01.05.2018.
URL: *https://www.iso.org/isoiec-27001-information-security.html*

Jarvelainen, J. (2013), 'It incidents and business impacts: Validating a framework for continuity management in information systems', *International Journal of Information Management* **33**, 583–590.

Jayaram, A. (2016), 'Lean six sigma approach for global supply chain management using industry 4.0 and iiot', *Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics* pp. 89–94.

Jilcott, S. (2015), 'Securing the supply chain for commodity IT devices by automated scenario generation', *2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015* pp. 0–5.

Johnson, C. (2015), 'The role of cyber-insurance, market forces, tort and regulation in the cybersecurity of safety-critical industries', *10th IET System Safety and Cyber-Security Conference 2015* pp. 7 .–7 .
URL: *http://digital-library.theiet.org/content/conferences/10.1049/cp.2015.0288*

Johnson, N., Elliott, D. & Drake, P. (2013), 'Exploring the role of social capital in facilitating supply chain resilience', *Supply Chain Management: An International Journal* **18**(3), 324–336.
URL: *http://www.emeraldinsight.com/doi/10.1108/SCM-06-2012-0203*

Kammerstetter, M., Langer, L., Skopik, F. & Kupzog, F. (2014), 'Practical Risk Assessment Using a Cumulative Smart Grid Model', *3rd International Conference on Smart Grids and Green IT Systems (SMARTGREENS)* pp. pages 31–42.
URL: *http://old.iseclab.org/papers/mk_smartgreens_2014.pdf*

Keegan, C. (2014), 'Cyber security in the supply chain: A perspective from the insurance industry', *Technovation* **34**(7), 380–381.
URL: *http://dx.doi.org/10.1016/j.technovation.2014.02.002*

Kelic, A., Collier, Z. A., Brown, C., Beyeler, W. E., Outkin, A. V., Vargas, V. N., Ehlen, M. A., Judson, C., Zaidi, A., Leung, B. & Linkov, I. (2013), 'Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks', *Environment Systems and Decisions* **33**(4), 544–560.

Khan, O. & Estay, D. A. S. (2015), 'Supply Chain Cyber-Resilience: Creating an Agenda for Future Research', *Technology Innovation Management Review* (April), 6–12.

Kim, H. (2012), 'Enhanced hash-based RFID mutual authentication protocol', *Communications in Computer and Information Science* **339 CCIS**, 70–77.

Kshetri, N. (2017*a*), 'Blockchain's roles in strengthening cybersecurity and protecting privacy', *Telecommunications Policy* **41**(10), 1027–1038.
URL: *https://doi.org/10.1016/j.telpol.2017.09.003*

Kshetri, N. (2017*b*), 'Can Blockchain Strengthen the Internet of Things?', *IT Professional* (August), 68–72.

Lee, J. H. & Kwon, T. (2016), 'Secure dissemination of software updates for intelligent mobility in future wireless networks', *Eurasip Journal on Wireless Communications and Networking* **2016**(1).
URL: *http://dx.doi.org/10.1186/s13638-016-0746-6*

Liu, B., Jin, Y. & Qu, G. (2015), 'Hardware Design and Verification Techniques for Supply Chain Risk Mitigation', *2015 14th International Conference on Computer-Aided Design and Computer Graphics (CAD/Graphics)* pp. 238–239.

Liu, B. & Sandhu, R. (2015), 'Fingerprint-Based Detection and Diagnosis of Malicious Programs in Hardware', *IEEE Transactions on Reliability* **64**(3), 1068–1077.

Manners-Bell, J. (2014), *Supply chain risk: understanding emerging threats to global supply chains*, Kogan Page.

Martin, R. A. M. C. (2014), 'Non-Malicious Taint Bad Hygiene is as Dangerous to the Mission as Malicious Intent', *CrossTalk* (2), 4–9.

Mattsson, U. T. (2004), 'A real-time intrusion prevention system for commercial enterprise databases and file systems', *Proceedings of the Third IASTED International Conference on Communications, Internet, and Information Technology* pp. 189–194.

McAfee, I. (2014), 'Net losses: Estimating the global cost of cybercrime', *Santa Clara, CA; Intel Security* .

McFadden, F. E. & Arnold, R. D. (2010), 'Supply chain risk mitigation for IT electronics', *2010 IEEE International Conference on Technologies for Homeland Security (HST)* pp. 49–55.
URL: *http://ieeexplore.ieee.org/document/5655094/*

McGraw, R. M., Fowler, M. J., Umphress, D. & MacDonald, R. A. (2014), 'Cyber threat impact assessment and analysis for space vehicle architectures', *Proceedings of SPIE* **9085**(June 2014).
URL: *http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2055242*

Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y. & Han, J. (2018), 'When Intrusion Detection Meets Blockchain Technology: A Review', *IEEE Access* **6**, 10179–10188.

Mensah, P., Merkuryev, Y. & Longo, F. (2015), 'Using ICT in developing a resilient supply chain strategy', *Procedia Computer Science* **43**(C), 101–108.
URL: *http://dx.doi.org/10.1016/j.procs.2014.12.014*

Meraglia, J. & Miller, M. (2014), 'Counterfeiting , Supply Chain Security , and the Cyber Threat : Why Defending Against Counterfeit Electronics Is No Longer Enough', *SAE Technical Paper 2014-01-2125* .

Meyer-larsen, N. & Müller, R. (2018), 'Enhancing the Cybersecurity of Port Community Systems', *Dynamics in Logistics* pp. 318–323.

MITRE (2018*a*), 'Common weakness enumeration (cwe) – the mitre corporation'. Accessed on 20.04.2018.
URL: *https://cwe.mitre.org/about/index.html*

MITRE (2018*b*), 'Common weakness enumeration (cwe): enumeration of technical impacts – the mitre corporation'. Accessed on 20.04.2018.
URL: *https://cwe.mitre.org/cwraf/enum_of_ti.html*

Miyamoto, I., Holzer, T. H. & Sarkani, S. (2017), 'Why a counterfeit risk avoidance strategy fails', *Computers and Security* **66**, 81–96.
URL: *http://dx.doi.org/10.1016/j.cose.2016.12.015*

Murphy, D. R. & Murphy, R. H. (2013), 'Teaching Cybersecurity: Protecting the Business Environment', *Proceedings of the 2013 on InfoSecCD '13 Information Security Curriculum Development Conference - InfoSecCD '13* pp. 88–93.
URL: *http://dl.acm.org/citation.cfm?id=2528908.2528913*

Mustafa, M. A., Zhang, N., Kalogridis, G. & Fan, Z. (2015), 'Roaming electric vehicle charging and billing: An anonymous multi-user protocol', *2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014* pp. 939–945.

Nagurney, A., Daniele, P. & Shukla, S. (2017), 'A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints', *Annals of Operations Research* **248**(1-2), 405–427.

Nasir, M. A., Sultan, S., Nefti-Meziani, S. & Manzoor, U. (2015), 'Potential cyber-attacks against global oil supply chain', *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* pp. 1–7.
URL: *http://ieeexplore.ieee.org/document/7166137/*

NIST (2012), 'Nist sp 800-30 rev.1 – guide for conducting risk assessments. maryland, usa: Nist'. Accessed on 01.05.2018.
URL: *https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final*

NIST (2018), 'Cybersecurity framework – the national institute of standards and technology (nist)'. Accessed on 20.04.2018.
URL: *https://www.nist.gov/cyberframework*

Olson, D. L. & Wu, D. D. (2010), 'A review of enterprise risk management in supply chain', *Kybernetes* **39**(5), 694–706.

Osborn, E. & Simpson, A. (2017), 'On small-scale IT users' system architectures and cyber security: A UK case study', *Computers and Security* **70**, 27–50.
URL: *https://doi.org/10.1016/j.cose.2017.05.001*

Pan, Y., White, J., Schmidt, D., Elhabashy, A., Sturm, L., Camelio, J. & Williams, C. (2017), 'Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems', *International Journal of Interactive Multimedia and Artificial Intelligence* **4**(3), 45.
URL: *http://www.ijimai.org/journal/node/1344*

Panko, R. R. (2011), 'Identity Content Assurance and Tracking Systems (ICATSs) for military supply chain risk management: A preliminary design', *Proceedings of the Annual Hawaii International Conference on System Sciences* pp. 1–6.

Papastergiou, S. & Polemi, N. (2018), 'MITIGATE : A Dynamic Supply Chain Cyber Risk Assessment Methodology', *Smart Trends in Systems, Security and Sustainability* pp. 1–9.

Patnayakuni, R. & Patnayakuni, N. (2014), 'Information Security in Value Chains : A Governance Perspective', *Twentieth Americas Conference on Information Systems* pp. 1–10.

Peterson, R. (2004), 'Crafting information technology governance', *Information Systems Management* **21**(4), 7–22.

Pettit, T., Croxton, K. & Fiksel, J. (2013), 'Ensuring supply chain resilience: Development and implementation of an assessment tool', *Journal of Business Logistics* **34**(1), 46–76.

Pettit, T. J., Fiksel, J. & Croxton, K. L. (2010), 'Ensuring Supply Chain Resilience: Development of a Conceptual Framework', *Journal of Business Logistics* **31**(1), 1–21.
URL: *http://doi.wiley.com/10.1002/j.2158-1592.2010.tb00125.x*

Pexels (2018), 'Water drop photo'. Accessed on 20.04.2018.
URL: *https://www.pexels.com/photo/water-drop-photo-220213/*

PITAC (2005), 'Cyber security: A crisis of prioritization', *National Coordination Office for Information Technology Research and Development, Arlington, VA* .

Polatidis, N., Pavlidis, M. & Mouratidis, H. (2018), 'Cyber-attack path discovery in a dynamic supply chain maritime risk management system', *Computer Standards and Interfaces* **56**(September 2017), 74–82.

Polatidis, N., Pimenidis, E., Pavlidis, M. & Mouratidis, H. (2017), Recommender Systems Meeting Security: From Product Recommendation to Cyber-Attack Prediction, *in* 'Engineering Applications of Neural Networks', Vol. 744, Springer International Publishing, pp. 508–519.
URL: *http://link.springer.com/10.1007/978-3-319-65172-9*

Polemi, N. & Papastergiou, S. (2016), Current efforts in ports and supply chains risk assessment, *in* '2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015', pp. 349–354.

Preuveneers, D., Joosen, W. & Ilie-Zudor, E. (2017), 'Trustworthy data-driven networked production for customer-centric plants', *Industrial Management & Data Systems* **117**(10), 2305–2324.
URL: *http://www.emeraldinsight.com/doi/10.1108/IMDS-10-2016-0419*

PWC (2017), 'Strengthening digital society against cyber shocks - key findings from the global state of information security® survey 2018'. Accessed on 20.12.2017.
URL: *https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf*

Qi, S., Zheng, Y., Li, M., Lu, L. & Liu, Y. (2016), 'Secure and Private RFID-Enabled Third-Party Supply Chain Systems', *IEEE Transactions on Computers* **65**(11), 3413–3426.

Radke, A. M. & Tseng, M. M. (2015), 'Design Considerations for Building Distributed Supply Chain Management Systems Based on Cloud Computing', *Journal of Manufacturing Science and Engineering* **137**(4), 040906.

Reddy, D. (2014), 'Criticality analysis and the supply chain: Leveraging representational assurance', *Technovation* **34**(7), 362–379.
URL: *http://dx.doi.org/10.1016/j.technovation.2014.01.009*

Rovito, S. M. & Rhodes, D. H. (2016), 'Enabling better supply chain decisions through a generic model utilizing cause-effect mapping', *10th Annual International Systems Conference, SysCon 2016 - Proceedings* .

Roy, A. & Kundu, A. (2012), 'Management of information security in supply chains - A process framework', *Proceedings of International Conference on Computers and Industrial Engineering, CIE* **2**, 1129–1139.

Rrushi, J. L. (2016), 'NIC displays to thwart malware attacks mounted from within the OS', *Computers and Security* **61**, 59–71.
URL: *http://dx.doi.org/10.1016/j.cose.2016.05.002*

Sabbagh, B. A. & Kowalski, S. (2015), 'A Socio-technical Framework for Threat Modeling a Software Supply Chain', *IEEE Security & Privacy* **13**(4), 30–39.
URL: *http://ieeexplore.ieee.org/document/7180277/*

Safa, N. S., Maple, C. & Watson, T. (2017*a*), 'An Information Security Risk Management Model for Smart Industries', *Advances in Transdisciplinary Engineering* **6**, 257–262.

Safa, N. S., Maple, C. & Watson, T. (2017*b*), 'The information security landscape in the supply chain', *Computer Fraud and Security* **2017**(6), 16–20.
URL: *http://dx.doi.org/10.1016/S1361-3723(17)30053-2*

Shankles, S., Moss, M., Pickel, J. & Bartol, N. (2013), 'How international standard efforts help address challenges in today's global ICT marketplace', *CrossTalk* **26**(2), 10–15.

Siciliano, G. G. & Gaudenzi, B. (2018), The Role of Supply Chain Resilience on IT and cyber Disruptions, *in* 'Network, Smart and Open', Vol. 24, Springer International Publishing, pp. 57–69.
URL: *http://link.springer.com/10.1007/978-3-319-62636-9*

Smith, G. E., Watson, K. J., Baker, W. H. & Pokorski, J. A. (2007), 'A critical balance: Collaboration and security in the IT-enabled supply chain', *International Journal of Production Research* **45**(11), 2595–2613.

Social-engineer (2015), 'The social-engineer podcast: Podcast ep. 066 – into the breach'. Retrieved from https://www.social-engineer.org on 10.05.2018.

Tjahjono, B., Esplugues, C., Ares, E. & Pelaez, G. (2017), 'What does industry 4.0 mean to supply chain?', *Procedia Manufacturing* **13**, 1175–1182.

Torabi, S. A., Giahi, R. & Sahebjamnia, N. (2016), 'An enhanced risk assessment framework for business continuity management systems', *Safety Science* **89**, 201–218.
URL: *http://dx.doi.org/10.1016/j.ssci.2016.06.015*

Tranfield, D., Denyer, D. & Smart, P. (2003), 'Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review', *British Journal of Management* **14**(3), 207–222.
URL: *http://doi.wiley.com/10.1111/1467-8551.00375*

Urciuoli, L. & Hintsa, J. (2017), 'Adapting supply chain management strategies to security???an analysis of existing gaps and recommendations for improvement', *International Journal of Logistics Research and Applications* **20**(3), 276–295.

Urciuoli, L., Männistö, T., Hintsa, J. & Khan, T. (2013), 'SUPPLY CHAIN CYBER SECURITY – POTENTIAL THREATS', *Information & Security: An International Journal* **29**(1), 51–68.
URL: *http://dx.doi.org/10.11610/isij.2904*

Venkatachary, S., Prasad, J. & Samikannu, R. (2017), 'Economic impacts of cyber security in energy sector: A review', *International Journal of Energy Economics and Policy* **7**(5), 250–262.

WEF (2017), 'World economic forum - global risks report 2017'. Accessed on 20.12.2017.
URL: *http://reports.weforum.org/global-risks-2017/shareable-infographics/*

Windelberg, M. (2016), 'Objectives for managing cyber supply chain risk', *International Journal of Critical Infrastructure Protection* **12**, 4–11.
URL: *http://dx.doi.org/10.1016/j.ijcip.2015.11.003*

Wolden, M., Valverde, R. & Talla, M. (2015), 'The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system', *IFAC-PapersOnLine* **28**(3), 1846–1852.
URL: *http://dx.doi.org/10.1016/j.ifacol.2015.06.355*

Yoshifu, K., Itoh, M. & Yamada, T. (2018), 'Cybersecurity Consulting Services in the World of IoT', *NEC Technical Journal* **12**(2), 64–69.

A Appendix - Publications relevant to the field of SCCRM

In this appendix section, three tables are shown. On one side, the first set of publications that were labelled as meeting the inclusion criteria and that were not excluded later in the process are listed. A column will indicate whether the article was read ("Yes") or not ("Not accessible"). Then, the publications that were believed to meet the inclusion criteria but were not reviewed are listed. Finally, the publications found from cross-references and then reviewed to add to the results of this thesis are shown on the third table.

Please note, the data shown on columns "Title", "Authors", "Year" and "Source of publication" are the ones originally provided by the search engines, and they need to be verified if this data is to be used for referencing purposes. The purpose of showing this data is to enable the reader to find relevant publications on areas related to SCCRM.

Table 6: Publications from the first group meeting the inclusion criteria.

#	Read	Title	Authors	Year	Source of publication
1	Yes	Cyber-attack path discovery in a dynamic supply chain maritime risk management system	Polatidis N., Pavlidis M., Mouratidis H.	2018	Computer Standards and Interfaces
2	Yes	Cybersecurity consulting services in the world of IoT	Yoshifu K., Itoh M., Yamada T.	2018	NEC Technical Journal
3	Yes	Enhancing the Cybersecurity of Port Community Systems	Meyer-Larsen, Nils and Müller, Rainer	2018	Dynamics in Logistics
4	Yes	Novel dynamic state-deflection method for gate-level design obfuscation	Dofe J., Yu Q.	2018	IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems
5	Yes	The Role of Supply Chain Resilience on IT and cyber Disruptions	Siciliano, Giorgia, Giusi and Gaudenzi, Barbara	2018	Network, Smart and Open
6	Yes	When Intrusion Detection Meets Blockchain Technology: A Review	Meng W., Tischhauser E., Wang Q., Wang Y., Han J.	2018	IEEE Access
7	Yes	A Comprehensive Assessment Model for Critical Infrastructure Protection	Häyhtiö M., Zaerens K.	2017	Management and Production Engineering Review
8	Yes	A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints	Nagurney A., Daniele P., Shukla S.	2017	Annals of Operations Research
9	Yes	A system dynamics case study of resilient response to IP theft from a cyber- attack	Sepúlveda Estay, Daniel Alberto and Khan, Omera	2017	0

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
10	Yes	Adapting supply chain management strategies to security–an analysis of existing gaps and recommendations for improvement	Urciuoli L., Hintsa J.	2017	International Journal of Logistics Research and Applications
11	Yes	An information security risk management model for smart industries	Sohrabi Safa N., Maple C., Watson T.	2017	Advances in Transdisciplinary Engineering
12	Yes	Analysing supply chain resilience: integrating the constructs in a concept mapping framework via a systematic literature review	Ali A., Mahfouz A., Arisha A.	2017	Supply Chain Management
13	Yes	Blockchain's roles in strengthening cybersecurity and protecting privacy	Kshetri N.	2017	Telecommunications Policy
14	Yes	Can Blockchain Strengthen the Internet of Things?	Kshetri N.	2017	IT Professional
15	Yes	Control structures in supply chains as a way to manage unpredictable cyber-risks	Sepúlveda Estay, Daniel Alberto and Khan, Omera Qayyum	2017	0
16	Not accessible	Cyber resilient flight software for spacecraft	Wheeler, Wayne and Betser, Joseph and Cohen, Nicholas and Meyers, Craig and Snavely, William and Chaki, Sagar and Riley, Michael and Runyon, Brad	2017	Aiaa Space and Astronautics Forum and Exposition
17	Yes	Cybersecurity Framework Adoption: Using Capability Levels for Implementation Tiers and Profiles	Dedeke, Adenekan	2017	Ieee Security and Privacy
18	Yes	Cybersecurity investments with nonlinear budget constraints: Analysis of the marginal expected utilities	Daniele P., Maugeri A., Nagurney A.	2017	Springer Optimization and Its Applications
19	Yes	Economic impacts of cyber security in energy sector: A review	Venkatachary S.K., Prasad J., Samikannu R.	2017	International Journal of Energy Economics and Policy

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
20	Yes	Identifying counterfeit smart grid devices: a lightweight system level framework	Babun, Leonardo and Aksu, Hidayet and Uluagac, A. Selcuk	2017	2017 Ieee International Conference on Communications (icc). Proceedings
21	Yes	Identifying multiple authors in a binary program	Meng X., Miller B.P., Jun K.-S.	2017	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
22	Yes	Industry 4.0 implications in logistics: an overview	Barreto L., Amaral A., Pereira T.	2017	Procedia Manufacturing
23	Yes	Managing IT and Cyber Risks in Supply Chains	Gaudenzi, Barbara and Siciliano, Giorgia	2017	Supply Chain Risk Management
24	Yes	MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology	Papastergiou, Spyridon and Polemi, Nineta	2017	Smart Trends in Systems, Security and Sustainability
25	Yes	MITIGATE: An innovative cybersecurity maritime supply chain risk management system	Duzha A., Gouvas P., Canepa M.	2017	CEUR Workshop Proceedings
26	Not accessible	Mitigating synchronized hardware trojan attacks in smart grids	Jin C., Ren L., Liu X., Zhang P., Van Dijk M.	2017	Proceedings - 2017 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017 (part of CPS Week)
27	Yes	Modeling SCADA Attacks	Kalogeraki, Eleni-Maria and Polemi, Nineta and Papastergiou, Spyridon and Panayiotopoulos, Themis	2017	Smart Trends in Systems, Security and Sustainability
28	Yes	Novel counterfeit detection of integrated circuits via infrared analysis: A case study based on the Intel Cyclone II FPGAS	Frazier P.D., Gilmore E.T., Collins I.J., Chouikha M.F.	2017	Proceedings - International Conference on Machine Learning and Cybernetics
29	Yes	On small-scale IT users' system architectures and cyber security: A UK case study	Osborn E., Simpson A.	2017	Computers and Security

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
30	Yes	Recommender systems meeting security: From product recommendation to cyber-attack prediction	Polatidis N., Pimenidis E., Pavlidis M., Mouratidis H.	2017	Communications in Computer and Information Science
31	Not accessible	Supply chain uncertainties linked to information systems: A case study approach	Ruel S., Ouabouch L., Shaaban S.	2017	Industrial Management and Data Systems
32	Yes	Taxonomies for Reasoning About Cyber-physical Attacks in IoT-based Manufacturing Systems	Pan, Yao and White, Jules and Schmidt, Douglas C. and Elhabashy, Ahmad and Sturm, Logan and Camelio, Jaime and Williams, Christopher	2017	International Journal of Interactive Multimedia and Artificial Intelligence
33	Yes	The information security landscape in the supply chain	Safa N.S.	2017	Computer Fraud and Security
34	Yes	Trustworthy data-driven networked production for customer-centric plants	Preuveneers, Davy and Joosen, Wouter and Ilie-Zudor, Elisabeth	2017	Industrial Management and Data Systems
35	Yes	TSensors Vision, Infrastructure and Security Challenges in Trillion Sensor Era	Alam, Mahabubul and Tehranipoor, Mark M. and Guin, Ujjwal	2017	Journal of Hardware and Systems Security
36	Yes	Why a counterfeit risk avoidance strategy fails	Miyamoto I., Holzer T.H., Sarkani S.	2017	Computers and Security
37	Not accessible	Advances in software engineering and software assurance	Shoemaker D., Woody C., Mead N.R.	2016	Advances in Computers
38	Yes	An enhanced risk assessment framework for business continuity management systems	Torabi, S. Ali and Giahi, Ramin and Sahebjamnia, Navid	2016	Safety Science
39	Yes	Cloud Supply Chain Resilience Model: Development and Validation	Herrera, Andrea and Janczewski, Lech	2016	Proceedings of the ... Annual Hawaii International Conference on System Sciences
40	Yes	Current efforts in ports and supply chains risk assessment	Polemi N., Papastergiou S.	2016	2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
41	Yes	Cybersecurity and Cyber-Resilient Supply Chains	Boyes, Hugh	2016	0
42	Not accessible	Designing security policies for complex SCADA systems management and protection	Feltus C., Khadraoui D.	2016	International Journal of Information Technology and Management
43	Yes	Enabling better supply chain decisions through a generic model utilizing cause-effect mapping	Rovito S.M., Rhodes D.H.	2016	10th Annual International Systems Conference, SysCon 2016 - Proceedings
44	Yes	Forensic-by-Design Framework for Cyber-Physical Cloud Systems	Ab Rahman N.H., Glisson W.B., Yang Y., Choo K.-K.R.	2016	IEEE Cloud Computing
45	Yes	Hardware Design and Verification Techniques for Supply Chain Risk Mitigation	Liu B., Jin Y., Qu G.	2016	Proceedings - 2015 14th International Conference on Computer-Aided Design and Computer Graphics, CAD/Graphics 2015
46	Yes	NIC displays to thwart malware attacks mounted from within the OS	Rrushi J.L.	2016	Computers and Security
47	Yes	Objectives for managing cyber supply chain risk	Windelberg M.	2016	International Journal of Critical Infrastructure Protection
48	Not accessible	Radio frequency identification and mobile ad-hoc network: Theories and applications	Kasemsap K.	2016	Handbook of Research on Recent Developments in Intelligent Communication Application
49	Not accessible	Redefining network intrusions as threat systems: Towards a socio technical approach to threat analysis	Bertram S.K.	2016	Why Cyber Security is a Socio-Technical Challenge: New Concepts and Practical Measures to Enhance Detection
50	Yes	Resilience of initiatives to shifting management priorities under emergent and future conditions	Collier Z.A., Connelly E.B., Thorisson H., Lambert J.H., Asce F., Sra F.	2016	10th Annual International Systems Conference, SysCon 2016 - Proceedings

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
51	Not accessible	Resilient metro-scale smart structures: Challenges & future directions	Burmester M., Munilla J.	2016	IoTBD 2016 - Proceedings of the International Conference on Internet of Things and Big Data
52	Yes	Secure and Private RFID-Enabled Third-Party Supply Chain Systems	Qi S., Zheng Y., Li M., Lu L., Liu Y.	2016	IEEE Transactions on Computers
53	Yes	Secure dissemination of software updates for intelligent mobility in future wireless networks	Lee J.H., Kwon T.	2016	Eurasip Journal on Wireless Communications and Networking
54	Not accessible	Some Unresolved Concerns & Future Directions for Resilient RFID Smart Structures in the Supply Chain	Fajardo, Jorge Munilla and Burmester, Mike	2016	Aebmr
55	Not accessible	Spacecraft embedded cyber defense-prototypes & experimentation	Cohen, Nicholas and Ewart, Roberta and Wheeler, Wayne and Betser, Joseph	2016	Aiaa Space 2016
56	Yes	Supply-Chain Security of Digital Microfluidic Biochips	Ali S.S., Ibrahim M., Rajendran J., Sinanoglu O., Chakrabarty K.	2016	Computer
57	Yes	The role of the supply chain in cybersecurity incident handling for drilling rigs	Couce-Vieira A., Houmb S.H.	2016	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
58	Not accessible	University research in hardware security	Lee R.B.	2016	2014 IEEE Hot Chips 26 Symposium, HCS 2014
59	Not accessible	Using a standard approach to the design of next generation e-supply chain digital forensic readiness systems	Masvosvere D.J.E., Venter H.S.	2016	SAIEE Africa Research Journal
60	Not accessible	A conceptual model for digital forensic readiness in e-supply chains	Masvosvere D., Venter H.	2015	European Conference on Information Warfare and Security, ECCWS

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
61	Yes	A model for the design of next generation e-supply chain digital forensic readiness tools	Masvosvere D.J.E., Venter H.S.	2015	2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference
62	Yes	A Socio-technical Framework for Threat Modeling a Software Supply Chain	Al Sabbagh, Bilal and Kowalski, Stewart	2015	Ieee Security and Privacy
63	Not accessible	ADAPTIVITY OF COMPLEX NETWORK TOPOLOGIES FOR DESIGNING RESILIENT SUPPLY CHAIN NETWORKS	Mari, Sonia Irshad and Lee, Young Hae and Memon, Muhammad Saad and Park, Young Soo and Kim, Minsun	2015	International Journal of Industrial Engineering-theory Applications and Practice
64	Yes	Cloud supply chain resilience	Herrera A., Janczewski L.	2015	2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference
65	Not accessible	Cyber Risk and Resilience in The Maritime Supply Chain, Cyber Risici og Modstandsdygtighed i den Maritime Forsyningskæde	Mikkelsen, Rune Tind	2015	0
66	Yes	Data privacy issues with RFID in healthcare	Hawrylak P.J., Hale J.	2015	Medical Data Privacy Handbook
67	Yes	Design considerations for building distributed supply chain management systems based on cloud computing	Radke A.M., Tseng M.M.	2015	Journal of Manufacturing Science and Engineering, Transactions of the ASME
68	Yes	Extending supply chain risk and resilience frameworks to manage cyber risk	Sepúlveda Estay, Daniel Alberto and Khan, Omera	2015	0
69	Yes	Fingerprint-Based Detection and Diagnosis of Malicious Programs in Hardware	Liu, Bao and Sandhu, Ravi	2015	Ieee Transactions on Reliability

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
70	Yes	Framework for Identifying Cybersecurity Risks in Manufacturing	Hutchins, Margot J. and Bhinge, Raunak and Micali, Maxwell K. and Robinson, Stefanie L. and Sutherland, John W. and Dornfeld, David	2015	Procedia Manufacturing
71	Yes	Hacking cyber-risks back in their tracks: to identify the right supply chain controls, look at the system	Sepúlveda, Daniel and Khan, Omera	2015	Effektivitet
72	Yes	I®ML: An Infrastructure resilience-oriented modeling language	Filippini R., Silva A.	2015	IEEE Transactions on Systems, Man, and Cybernetics: Systems
73	Not accessible	Improving cybersecurity through the use of the cybersecurity framework	Conkle T., Witte G.	2015	9th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, NPIC and HMIT 2015
74	Yes	MITIGATING RISKS OF COUNTERFEIT AND TAINTED COMPONENTS (Non-Malicious Taint - Bad Hygiene is as Dangerous to the Mission as Malicious Intent)	A. Martin, Robert and Corporation, Mitre	2015	0
75	Yes	Potential cyber-attacks against global oil supply chain	Nasir M.A., Sultan S., Nefti-Meziani S., Manzoor U.	2015	2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2015
76	Yes	Roaming electric vehicle charging and billing: An anonymous multi-user protocol	Mustafa M.A., Zhang N., Kalogridis G., Fan Z.	2015	2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014
77	Yes	Securing small businesses - The weakest link in a supply chain?	Caldwell T.	2015	Computer Fraud and Security

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
78	Yes	Securing the supply chain for commodity IT devices by automated scenario generation	Jilcott S.	2015	2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015
79	Yes	Supply Chain Cyber-Resilience: Creating an Agenda for Future Research	Khan, Omera and Sepúlveda Estay, Daniel Alberto	2015	Technology Innovation Management Review
80	Yes	The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system	Wolden M., Valverde R., Talla M.	2015	IFAC-PapersOnLine
81	Yes	The role of cyber-insurance, market forces, tort and regulation in the cyber-security of safety-critical industries	Johnson C.W.	2015	IET Conference Publications
82	Yes	Topological resilience analysis of supply networks under random disruptions and targeted attacks	Wang W., Street W.N., DeMatta R.E.	2015	Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2015
83	Not accessible	Towards a supply chain cyber-risk and resilience research agenda - a systematic literature review	Sepúlveda Estay, Daniel Alberto and Khan, Omera	2015	0
84	Yes	Using ICT in developing a resilient supply chain strategy	Mensah P., Merkuryev Y., Longo F.	2015	Procedia Computer Science
85	Yes	A security argument pattern for medical device assurance cases	Finnegan A., McCaffery F.	2014	Proceedings - IEEE 25th International Symposium on Software Reliability Engineering Workshops, ISSREW 2014
86	Yes	Counterfeiting, supply chain security, and the cyber threat; Why defending against counterfeit electronics is no longer enough	Meraglia J., Miller M.	2014	SAE Technical Papers

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
87	Yes	Criticality analysis and the supply chain: Leveraging representational assurance	Reddy D.	2014	Technovation
88	Not accessible	CUIAS - A user identity authentication service for discovery service	Liu P., Kong N., Tian Y., Lee X., Yan B.	2014	Proceedings - 2014 IEEE International Conference on Internet of Things, iThings 2014, 2014 IEEE International Conference on Green Computing and Communications, GreenCom 2014 and 2014 IEEE International Conference on Cyber-Physical-Social Computing, CPS 2014
89	Yes	Cyber security in the supply chain: A perspective from the insurance industry	Keegan C.	2014	Technovation
90	Not accessible	Cyber security: The risk of supply chain vulnerabilities in an enterprise firewall	Kuypers M.A., Heon G., Martin P., Smith J., Ward K., Paté-Cornell E.	2014	PSAM 2014 - Probabilistic Safety Assessment and Management
91	Yes	Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems	Boyson S.	2014	Technovation
92	Yes	Cyber supply chain security practices DNA - Filling in the puzzle using a diverse set of disciplines	Bartol N.	2014	Technovation
93	Yes	Cyber Threat Impact Assessment and Analysis for Space Vehicle Architectures	McGraw, Robert M. and Fowler, Mark J. and Umphress, David and MacDonald, Richard A.	2014	Proceedings of Spie–the International Society for Optical Engineering
94	Yes	Cybercrime prevention in the kingdom of Bahrain via IT security audit plans	Almadhoob, Amna and Valverde, Raul	2014	Journal of Theoretical and Applied Information Technology

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
95	Not accessible	Cybersecurity information sharing: A framework for information security management in UK SME supply chains	Lewis R., Louvieris P., Abbott P., Clewley N., Jones K.	2014	ECIS 2014 Proceedings - 22nd European Conference on Information Systems
96	Yes	Cybersecurity procurement language for energy delivery systems	Goff E., Glantz C., Massello R.	2014	ACM International Conference Proceeding Series
97	Yes	Cybersecurity Risk Management	Chabinsky, Steven	2014	Security
98	Yes	Data supply chain management: supply chain management for incentive and risk-based assured information sharing, UTD	Thuraisingham, Bhavani and Thuraisingham, Bhavani	2014	0
99	Not accessible	Disaster and risk conference IDRC davos 2014: Insurability of high impact low probability events in the context of BCM	Regenass J.A.	2014	Proceedings of the 5th International Disaster and Risk Conference: Integrative Risk Management - The Role of Science, Technology and Practice, IDRC Davos 2014
100	Yes	Embedded reconfigurable logic for ASIC design obfuscation against supply chain attacks	Liu B., Wang B.	2014	Proceedings - Design, Automation and Test in Europe, DATE
101	Yes	Information security in value chains: A governance perspective	Patnayakuni R., Patnayakuni N.	2014	20th Americas Conference on Information Systems, AMCIS 2014
102	Yes	Malware, "weakware," and the security of software supply chains	Axelrod C.W.	2014	CrossTalk
103	Not accessible	Open industry standards for mitigating risks to global supply chains	Szakal A.R., Pearsall K.J.	2014	IBM Journal of Research and Development
104	Yes	Practical risk assessment using a cumulative smart grid model	Kammerstetter M., Langer L., Skopik F., Kupzog F., Kastner W.	2014	SMARTGREENS 2014 - Proceedings of the 3rd International Conference on Smart Grids and Green IT Systems

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
105	Yes	Research letter: Issues of cyber supply chain security in Korea	Kim K.-C., Im I.	2014	Technovation
106	Yes	SecureCPS: Defending a Nanosatellite Cyber-Physical System	Forbes, Lance and Vu, H and Udrea, Bogdan and Hagar, Hamilton and Koutsoukos, Xenofon D. and Yampolskiy, Mark	2014	Proceedings of Spie–the International Society for Optical Engineering
107	Yes	Supply chain cyber security: A Russian outlook	Sokolov A., Mesropyan V., Chulok A.	2014	Technovation
108	Not accessible	Supply chain risk management: A review	Singh G., Wahid N.A.	2014	International Journal of Supply Chain Management
109	Yes	The challenge of cyber supply chain security to research and practice - An introduction	Linton J.D., Boyson S., Aje J.	2014	Technovation
110	Yes	Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks	Kelic A., Collier Z.A., Brown C., Beyeler W.E., Outkin A.V., Vargas V.N., Ehlen M.A., Judson C., Zaidi A., Leung B., Linkov I.	2013	Environment Systems and Decisions
111	Not accessible	Ensuring your development processes meet today's cyber challenges	Chrissis M.B., Konrad M., Moss M.	2013	CrossTalk
112	Yes	How do cyber threats affect petrochemical risk models?	Dutcher, D.	2013	Hydrocarbon Processing
113	Yes	How international standard efforts help address challenges in today's global ICT marketplace	Shankles S., Moss M., Pickel J., Bartol N.	2013	CrossTalk
114	Yes	Integrated circuit security threats and hardware assurance countermeasures	Goertzel K.M.	2013	CrossTalk
115	Yes	Next big thing in big data: The security of the ICT supply chain	Lu T., Guo X., Xu B., Zhao L., Peng Y., Yang H.	2013	Proceedings - SocialCom/PASSAT/BigData/EconCom/BioMed 2013
116	Not accessible	Next generation information-based infrastructures: New dependencies and threats	Eric L.	2013	Critical Information Infrastructure Protection and Resilience in the ICT Sector

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
117	Not accessible	RFID mutual authentication protocol based on synchronized secret	Kim H.	2013	International Journal of Security and its Applications
118	Not accessible	Security Risks to IT Supply Chains under Economic Stress	Axelrod, C. Warren and Haldar, Sukumar	2013	International Journal of Cyber Warfare and Terrorism
119	Not accessible	Software ID tags support better cyber security	Klos S., Richardson J.	2013	CrossTalk
120	Yes	Supply Chain Cyber Security – Potential Threats	Urciuoli, Luca and Männistö, Toni and Hintsa, Juha and Khan, Tamanna	2013	Information and Security: an International Journal
121	Yes	Teaching cybersecurity: Protecting the business environment	Murphy D.R., Murphy R.H.	2013	Proceedings of the 2013 Information Security Curriculum Development Conference, InfoSec CD 2013
122	Yes	The Most Influential Cyber Security Team [Information Technology Laboratory team at NIST]	Chabinsky, Steven	2013	Security
123	Not accessible	The weakest link-the ICT supply chain and information warfare	Shoemaker D., Wilson C.	2013	8th International Conference on Information Warfare and Security, ICIW 2013
124	Not accessible	Towards an analysis of software supply chain risk management	Du S., Lu T., Zhao L., Xu B., Guo X., Yang H.	2013	Lecture Notes in Engineering and Computer Science
125	Not accessible	We cannot blindly reap the benefits of a globalized ICT supply chain!	Davidson D., Shankles S.	2013	CrossTalk
126	Yes	Enhanced hash-based RFID mutual authentication protocol	Kim H.	2012	Communications in Computer and Information Science
127	Yes	Entropy assessment of supply chain disruption	Durowoju O.A., Chan H.K., Wang X.	2012	Journal of Manufacturing Technology Management
128	Yes	Information security in supply chains - A process framework	Roy A., Gupta A.D., Deshmukh S.G.	2012	IEEE International Conference on Industrial Engineering and Engineering Management

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
129	Yes	Information Security Investment Case Study: The Manufacturing Sector 1 Summary: Cybersecurity in the Extended Enterprise	0	2012	0
130	Yes	Interacting with Hardware Trojans over a network	Farag M.M., Lerner L.W., Patterson C.D.	2012	Proceedings of the 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2012
131	Not accessible	Management of information security in supply chains - A process framework	Roy A., Kundu A.	2012	Proceedings of International Conference on Computers and Industrial Engineering, CIE
132	Yes	Research on software development process assurance models in ICT supply chain risk management	Xie F., Lu T., Xu B., Chen D., Peng Y.	2012	Proceedings - 2012 IEEE Asia-Pacific Services Computing Conference, APSCC 2012
133	Yes	Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)	Demchak C.C.	2012	Journal of Comparative Policy Analysis: Research and Practice
134	Yes	The United States Department of Defense revitalization of system security engineering through program protection	Baldwin K., Popick P.R., Miller J.F., Goodnight J.	2012	SysCon 2012 - 2012 IEEE International Systems Conference, Proceedings
135	Yes	Trust engineering - Rejecting the tyranny of the weakest link	Alexander S.D.	2012	ACM International Conference Proceeding Series
136	Not accessible	An Integrative View on Cyber Threat to Global Supply Chain Management Systems	Cho, Sung-woo and Pak, Myong-sop	2011	Journal of Korea Trade
137	Yes	Cyber resilience for mission assurance	Goldman H., McQuaid R., Picciotto J.	2011	2011 IEEE International Conference on Technologies for Homeland Security, HST 2011

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
138	Yes	Cyber terrorism and aviation-national and international responses	Abeyratne, Ruwantissa	2011	Journal of Transportation Security
139	Yes	Identity Content Assurance and Tracking Systems (ICATSs) for military supply chain risk management: A preliminary design	Panko R.R.	2011	Proceedings of the Annual Hawaii International Conference on System Sciences
140	Not accessible	IT security in supply chain: Does a leader-follower structure matter?	Bandyopadhyay T.	2011	17th Americas Conference on Information Systems 2011, AMCIS 2011
141	Not accessible	Development of a supply chain management security risk management method: A conceptual model	Warren M., Leitch S.	2010	9th European Conference on Information Warfare and Security 2010, ECIW 2010
142	Yes	Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels	Bodeau, Deborah J. and Graubart, Richard and Fabius-Greene, Jennifer	2010	Proceedings - Socialcom 2010: 2nd Ieee International Conference on Social Computing, Passat 2010: 2nd Ieee International Conference on Privacy, Security, Risk and Trust
143	Yes	Information security in networked supply chains: Impact of network vulnerability and supply chain integration on incentives to invest	Bandyopadhyay T., Jacob V., Raghunathan S.	2010	Information Technology and Management
144	Yes	Supply chain risk mitigation for IT electronics	McFadden F.E., Arnold R.D.	2010	2010 IEEE International Conference on Technologies for Homeland Security, HST 2010
145	Not accessible	Benchmarking supply chains on risk dimensions	Faisal M.N.	2009	International Journal of Services and Operations Management
146	Not accessible	Industry works to boost security as cyberattacks escalate	Fulghum D.A., Warwick G.	2009	Aviation Week and Space Technology (New York)

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
147	Not accessible	Secure The Cyber Supply Chain [supply chain management and data security]	Hoover, J. Nicholas	2009	Informationweek
148	Yes	Security Challenges of the EPCglobal Network	Fabian, Benjamin and Guenther, Oliver	2009	Communications of the Acm
149	Yes	Security engineering: developments and directions	Thuraisingham, Bhavani	2009	Proceedings of the 2009 Third Ieee International Conference on Secure Software Integration and Reliability Improvement. Ssiri 2009
150	Not accessible	Emergent risks In critical infrastructures	Dynes S.	2008	IFIP International Federation for Information Processing
151	Yes	A critical balance: Collaboration and security in the IT-enabled supply chain	Smith G.E., Watson K.J., Baker W.H., Pokorski II J.A.	2007	International Journal of Production Research
152	Not accessible	Economic costs of firm-level information infrastructure failures: Estimates from field studies in manufacturing supply chains	Dynes S., Eric Johnson M., Andrijcic E., Horowitz B.	2007	The International Journal of Logistics Management
153	Yes	Engineering for systems assurance - A state of the practice report	Croll P.R.	2007	Proceedings of the 1st Annual 2007 IEEE Systems Conference
154	Not accessible	Information security risk in the e-supply chain	Baker W.H., Smith G.E., Watson K.J.	2007	E-Supply Chain Technologies and Management
155	Not accessible	Locking onto cybersecurity	Forcinio, Hallie	2007	Managing Automation
156	Not accessible	Secure information sharing in internet-based supply chain management systems	Zhang C., Li S.	2006	Journal of Computer Information Systems
157	Not accessible	The protection of privacy in Internet banking	Liao Z.	2005	Proceedings of the International Conference on Electronic Business (ICEB)

Continuation of Table 6 - Publications from the first group meeting the inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
158	Yes	A real-time intrusion prevention system for commercial enterprise databases and file systems	Mattsson U.T.	2004	Proceedings of the Third IASTED International Conference on Communications, Internet, and Information Technology
159	Yes	Susceptibility audits: A tool for safeguarding information assets	Hale, John C. and Landry, Timothy D. and Wood, Charles M.	2004	Business Horizons
160	Yes	Cyber attacks against supply chain management systems: A short note	Warren M., Hutchinson W.	2000	International Journal of Physical Distribution and Logistics Management
End of Table					

Table 7: Publications from the second group meeting the inclusion criteria.

#	Read	Title	Authors	Year	Source of publication
1	No	Avoiding the internet of insecure industrial things	Urquhart L., McAuley D.	2018	Computer Law and Security Review
2	No	CloudChain: A novel distribution model for digital products based on supply chain principles	Vazquez-Martinez G.A., Gonzalez-Compean J.L., Sosa-Sosa V.J., Morales-Sandoval M., Perez J.C.	2018	International Journal of Information Management
3	No	System-on-Chip Platform Security Assurance: Architecture and Validation	Ray, Sandip and Peeters, Eric and Tehranipoor, Mark M. and Bhunia, Swarup	2018	Proceedings of the Ieee
4	No	A Framework for Assessing Technology Risks in Transaction-Based Extended Enterprises: U.S. Capital Market Case	Friedhoff J.M., Mansouri M.	2017	IEEE Systems Journal
5	No	A process-based dependency risk analysis methodology for critical infrastructures	Stergiopoulos G., Kouktzoglou V., Theocharidou M., Gritzalis D.	2017	International Journal of Critical Infrastructures

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
6	No	A secure architecture for IoT with supply chain risk management	Hiromoto R.E., Haney M., Vakanski A.	2017	Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017
7	No	Agent based simulation of a payment system for resilience assessments	Larsson, A. and Ibrahim, O. and Olsson, L. and van Laere, J.	2017	2017 Ieee International Conference on Industrial Engineering and Engineering Management (ieem)
8	No	Analyzing drivers of risks in electronic supply chains: a grey-DEMATEL approach	Rajesh, R. and Ravi, V.	2017	International Journal of Advanced Manufacturing Technology
9	No	Assessing Supply Chain Resilience upon Critical Infrastructure Disruptions: A Multilevel Simulation Modelling Approach	Trucco, Paolo and Petrenj, Boris and Birkie, Seyoum, Eshetu	2017	Supply Chain Risk Management
10	No	Cyber-security must be a C-suite priority	Boone A.	2017	Computer Fraud and Security
11	No	Do collaborative relationship and organizational system and information techonology affects supply chain resilience? [O relacionamento colaborativo e os sistemas e tecnologias de informação impactam a resiliência das cadeias de suprimentos?]	Alvarenga M.Z., dos Santos W.R., Pelissari A.S.	2017	Espacios
12	No	Experiences in trusted cloud computing	Oliver I., Holtmanns S., Miche Y., Lal S., Hippeläinen L., Kalliola A., Ravidas S.	2017	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
13	No	Hardware-based anti-counterfeiting techniques for safeguarding supply chain integrity	Arafin M.T., Stanley A., Sharma P.	2017	Proceedings - IEEE International Symposium on Circuits and Systems
14	No	HVACKer: Bridging the Air-Gap by Attacking the Air Conditioning System	Mirsky, Yisroel and Guri, Mordechai and Elovici, Yuval	2017	0
15	No	INVITED: Obfus-CADe: Obfuscating Additive Manufacturing CAD Models Against Counterfeiting	Gupta N., Chen F., Tsoutsos N.G., Maniatakos M.	2017	Proceedings - Design Automation Conference
16	No	Kill switches, remote deletion, and intelligent agents: Framing everyday household cybersecurity in the internet of things, Kill switches, remote deletion, and intelligent agents: Framing everyday household cybersecurity in the internet of things	Oravec, Jo Ann and Oravec, Jo Ann	2017	Technology in Society
17	No	Logistics and cloud computing service providers' cooperation: a resilience perspective	Subramanian N., Abdulrahman M.D.	2017	Production Planning and Control
18	No	Mil/Aero electronics supply chain facing new challenges	Marias S.L.	2017	SMT Surface Mount Technology Magazine
19	No	Organisational resilience in a cloud-based enterprise in a supply chain: a challenge for innovative SMEs	Arsovski S., Arsovski Z., Stefanović M., Tadić D., Aleksić A.	2017	International Journal of Computer Integrated Manufacturing
20	No	Restoration decision making for a supply chain network under cyber attack	Heath E.A., Mitchell J.E., Sharkey T.C.	2017	Simulation Series
21	No	Ring oscillators and hardware Trojan detection	Kitsos P., Sklavos N., Voyiatzis A.G.	2017	Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
22	No	Security assurance of (multi-)cloud application with security SLA composition	Rak M.	2017	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)
23	No	Security framework of Ultralightweight Mutual Authentication Protocols for low cost RFID tags	Khalid M., Mujahid U.	2017	Proceedings of 2017 International Conference on Communication, Computing and Digital Systems, C-CODE 2017
24	No	Supply chain threats	Whyte, Stephen	2017	Food Science and Technology (london)
25	No	Addressing critical industrial control system cyber security concerns via high fidelity simulation	Vaughn R.B., Morris T.	2016	Proceedings of the 11th Annual Cyber and Information Security Research Conference, CISRC 2016
26	No	An approach for assessing consequences of potential supply chain & insider contributed cyber attacks on nuclear power plants	Chu T.-L., Varuttamaseni A., Baek J.-S., Pepper S.	2016	Transactions of the American Nuclear Society
27	No	Comparison of radio frequency based techniques for device discrimination and operation identification	Stone B., Stone S.	2016	Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016
28	No	Cyber security in the ATM supply chain	Mohnl G.	2016	ICNS 2016: Securing an Integrated CNS System to Meet Future Challenges
29	No	Detecting a weakened encryption algorithm in microcontrollers using correlation-based anomaly detection	Wylie J., Stone S., Mullins B.	2016	Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
30	No	Factors that influence interorganizational use of information and communications technology in relationship-based supply chains: evidence from the Macedonian and American wine industries	Mirkovski K., Lowry P.B., Feng B.	2016	Supply Chain Management
31	No	Hardware trojans: Lessons learned after one decade of research	Xiao K., Forte D., Jin Y., Karri R., Bhunia S., Tehranipoor M.	2016	ACM Transactions on Design Automation of Electronic Systems
32	No	How internal integration, information sharing, and training affect supply chain risk management capabilities	Riley, Jason M. and Klein, Richard and Miller, Janis and Sridharan, V.	2016	International Journal of Physical Distribution and Logistics Management
33	No	Manufacturing and Security Challenges in 3D Printing	Zeltmann S.E., Gupta N., Tsoutsos N.G., Maniatakos M., Rajendran J., Karri R.	2016	JOM
34	No	Scalable Industry Data Access Control in RFID-Enabled Supply Chain	Qi S., Zheng Y., Li M., Liu Y., Qiu J.	2016	IEEE/ACM Transactions on Networking
35	No	Security against cyber attacks in food industry	Khursheed A., Kumar M., Sharma M.	2016	International Journal of Control Theory and Applications
36	No	Supply chain communication and operational management in the automotive components supply chains in South Africa using cloud hosted information systems	Tlamelo P.	2016	Proceedings of the European Conference on IS Management and Evaluation, ECIME
37	No	Supply chain decision analytics: Application and case study for critical infrastructure security	Edwards N., Kao G., Hamlet J., Bailon J., Liptak S.	2016	Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016
38	No	Supply chain security and impacts	Whitehouse, Ollie	2016	Iet Cyber Security in Modern Power Systems

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
39	No	Supply-Chain Security for Cyberinfrastructure [Guest editors' introduction]	Forte D., Perez R., Kim Y., Bhunia S.	2016	Computer
40	No	Systems-based cyber security in the supply chain	Barron S., Cho Y.M., Hua A., Norcross W., Voigt J., Haimes Y.	2016	2016 IEEE Systems and Information Engineering Design Symposium, SIEDS 2016
41	No	Targeting key data breach services in underground supply chain	Li W., Yin J., Chen H.	2016	IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016
42	No	The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence	He H., Maple C., Watson T., Tiwari A., Mehnen J., Jin Y., Gabrys B.	2016	2016 IEEE Congress on Evolutionary Computation, CEC 2016
43	No	Vendor Malware: Detection Limits and Mitigation	Lysne O., Hole K.J., Otterstad C., Ytrehus O., Aarseth R., Tellnes J.	2016	Computer
44	No	VLSI supply chain security risks and mitigation techniques: A survey	Liu B., Qu G.	2016	Integration, the VLSI Journal
45	No	Weapons systems and cyber security - a challenging union	Koch, Robert and Golling, Mario	2016	2016 8th International Conference on Cyber-conflict (cycon)

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
46	No	A Mixed and Batching Authentication Protocol for Grouped Tags in Mobile RFID System	Litian D., Fu D., Zizhong W.J.	2015	Proceedings - 2015 IEEE International Conference on Data Science and Data Intensive Systems; 8th IEEE International Conference Cyber, Physical and Social Computing; 11th IEEE International Conference on Green Computing and Communications and 8th IEEE International Conference on Internet of Things, DSDIS/CPSCom/GreenCom/iThings 2015
47	No	A survey on financial botnets threat	Bottazzi G., Me G.	2015	Communications in Computer and Information Science
48	No	An empirical study on the impacts of ERP system, e-business technologies and organizational collaboration on supply chain agility: PLS perspective	Almahamid S., Hourani A.	2015	International Journal of Advanced Operations Management
49	No	Analyzing information security investment in networked supply chains	Jianqiang G., Shue M., Weijun Z.	2015	2015 International Conference on Logistics, Informatics and Service Science, LISS 2015
50	No	Best practices for securing your infrastructure and what will justify the effort	Reynolds, Peter	2015	Isa Automation Conference and Exhibition 2015
51	No	Cloud-Based Global Supply Chain: A Conceptual Model and Multilayer Architecture	Akbaripour H., Houshmand M., Valilai O.F.	2015	Journal of Manufacturing Science and Engineering, Transactions of the ASME

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
52	No	Cybersecurity for product lifecycle management a research roadmap	Bertino E., Hartman N.W.	2015	2015 IEEE International Conference on Intelligence and Security Informatics: Securing the World through an Alignment of Technology, Intelligence, Humans and Organizations, ISI 2015
53	No	Enterprise Risk Management: A Common Framework for the Entire Organization	Green P.E.J.	2015	Enterprise Risk Management: A Common Framework for the Entire Organization
54	No	Future integrated factories: A system of systems engineering perspective	Nahavandi S., Creighton D., Le V.T., Johnstone M., Zhang J.	2015	Integrated Systems: Innovations and Applications
55	No	IPCRESS: Tracking intellectual property through supply chains in clouds	Gillam L., Notley S., Broome S., Garside D.	2015	Enterprise Management Strategies in the Era of Cloud Computing
56	No	Preliminary reflections about the establishment of a cyber-security policy for a sustainable, secure and safe space environment	Del Monte L., Zatti S.	2015	Proceedings of the International Astronautical Congress, IAC
57	No	Reconfiguration-based VLSI design for security	Liu B., Wang B.	2015	IEEE Journal on Emerging and Selected Topics in Circuits and Systems
58	No	Survey on mobile user's data privacy threats and defense mechanisms	Khan J., Abbas H., Al-Muhtadi J.	2015	Procedia Computer Science
59	No	An Agent-Based Socio-Technical Approach to Impact Assessment for Cyber Defense	Charitoudi K., Blyth A.J.C.	2014	Information Security Journal
60	No	Cyber supply chain security: A Concern for the pharmaceutical industry	Oldfield E.	2014	Pharmacy Times

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
61	No	Fabrication attacks: Zero-overhead malicious modifications enabling modern microprocessor privilege escalation	Tsoutsos N.G., Maniatakos M.	2014	IEEE Transactions on Emerging Topics in Computing
62	No	Hacking and protecting IC hardware	Hamdioui S., Danger J.-L., Di Natale G., Smailbegovic F., Van Battum G., Tehranipoor M.	2014	Proceedings - Design, Automation and Test in Europe, DATE
63	No	Non-state cyber power in ONG	Kambic J., Liles S.	2014	9th International Conference on Cyber Warfare and Security 2014, ICCWS 2014
64	No	Rationalising the security concern of cloud enabled e-commerce in the supply chain context	Durowoju O.A.	2014	E-Commerce Platform Acceptance: Suppliers, Retailers, and Consumers
65	No	Safe and secure: re-engineering a software process set for the challenges of the 21st century	Wallace, K. R.	2014	9th Iet International Conference on System Safety and Cyber Security (2014)
66	No	Security at the source: Securing today's critical supply chain networks	Véronneau S., Roy J.	2014	Journal of Transportation Security
67	No	Security in the cyber supply chain: A Chinese perspective	Rongping M., Yonggang F.	2014	Technovation
68	No	Security issues in the security cyber supply chain in South Africa	Venter H.S.	2014	Technovation
69	No	Software and supply chain risk management assurance framework	O'Neill D.	2014	CrossTalk
70	No	Threat analysis in the software development lifecycle	Whitmore J., Türpe S., Triller S., Poller A., Carlson C.	2014	IBM Journal of Research and Development
71	No	Towards cybersecurity protection of critical infrastructures by generating security policy for SCADA systems	Feltus C., Ouedraogo M., Khadraoui D.	2014	2014 1st International Conference on Information and Communication Technologies for Disaster Management, ICT-DM 2014

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
72	No	Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure	Knapp E.D., Samani R.	2013	Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure
73	No	Association rule hiding in risk management for retail supply chain collaboration	Le H.Q., Arch-Int S., Nguyen H.X., Arch-Int N.	2013	Computers in Industry
74	No	Effects of inter-organizational compatibility on supply chain capabilities: Exploring the mediating role of inter-organizational information systems (IOIS) integration	Rajaguru R., Matanda M.J.	2013	Industrial Marketing Management
75	No	Multiscale approach to the security of hardware supply chains for energy systems	Lambert J.H., Keisler J.M., Wheeler W.E., Collier Z.A., Linkov I.	2013	Environment Systems and Decisions
76	No	On security with the new Gen2 RFID security framework	Engels D.W., Kang Y.S., Wang J.	2013	2013 IEEE International Conference on RFID, RFID 2013
77	No	Product Piracy Prevention: Product Counterfeit Detection Without Security Labels	Horn, Christian and Blankenburg, Matthias and Kruger, Jorg	2013	International Journal of Cybersecurity and Digital Forensics
78	No	Trusted computation through biologically inspired processes	Anderson G.W.	2013	Proceedings of SPIE - The International Society for Optical Engineering
79	No	A System-Aware cyber security architecture	Jones R.A., Horowitz B.	2012	Systems Engineering
80	No	Information management and sharing for national cyber situational awareness	Skopik F., Bleier T., Fiedler R.	2012	ISSE 2012 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2012 Conference
81	No	Inserting malware at the source	Bradbury D.	2012	Computer Fraud and Security

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
82	No	Quantifying Cyberinfrastructure Resilience against Multi-Event Attacks	Zobel, Christopher W. and Khansa, Lara	2012	Decision Sciences
83	No	Run-time prediction and preemption of configuration attacks on embedded process controllers	Lerner L.W., Farag M.M., Patterson C.D.	2012	ACM International Conference Proceeding Series
84	No	Supply chain attacks: Basic input output systems (BIOS), mux multiplexers and field programmable gate arrays (FPGA)	Rohret D., Willmann J.	2012	7th International Conference on Information Warfare and Security, ICIW 2012
85	No	Computing randomized security strategies in networked domains	Letchford J., Vorobeychik Y.	2011	AAAI Workshop - Technical Report
86	No	Governing intangible risk the cyber supply chain risk model	Boyson S., Corsi T.M., Rossman H.	2011	X-SCM: The New Science of X-Treme Supply Chain Management
87	No	Key management for substations: Symmetric keys, public keys or no keys?	Fuloria S., Anderson R., Alvarez F., McGrath K.	2011	2011 IEEE/PES Power Systems Conference and Exposition, PSCE 2011
88	No	Risk and gain sharing challenges in interorganisational implementation of RFID technology	Hellström D., Johnsson C., Norrman A.	2011	International Journal of Procurement Management
89	No	Selection of model in developing information security criteria on smart grid security system	Ling A.P.A., Masao M.	2011	Proceedings - 9th IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops, ISPAW 2011 - ICASE 2011, SGH 2011, GSDP 2011
90	No	The impact of security and scalability of cloud service on supply chain performance	Durowoju O.A., Chan H.K., Wang X.	2011	Journal of Electronic Commerce Research
91	No	Assessment and mitigation of cyber exploits in future aircraft surveillance	Sampigethaya, Krishna and Poovendran, Radha and Bushnell, Linda	2010	Ieee Aerospace Conference Proceedings

Continuation of Table 7 - Publications from the second group meeting inclusion criteria					
#	Read	Title	Authors	Year	Source of publication
92	No	Securing online transactions with biometric methods	Pope J.A., Bartmann D.	2010	International Journal of Electronic Marketing and Retailing
93	No	Information risk management and resilience	Dynes S.	2009	IFIP Advances in Information and Communication Technology
94	No	The new supply chain's frontier: Information management	Pereira J.V.	2009	International Journal of Information Management
95	No	Web services-based architecture for RFID applications	Sundaram, David and Zhou, Wei and Pienaar, Schalk and Piramuthu, Selwyn	2009	Proceedings - Ieee International Enterprise Distributed Object Computing Workshop, Edoc
96	No	Information and communications technology and the global marketplace	Komaroff M.	2008	CrossTalk
97	No	Inter-organisational intrusion detection using knowledge grid technology	Pilgermann M., Blyth A., Vidalis S.	2006	Information Management and Computer Security
98	No	Oil and gas supply chain peril	Urso J., Colpo J., Sheble N.	2006	InTech
99	No	Virtual integration costs and the limits of supply chain scalability	Bhimani A., Ncube M.	2006	Journal of Accounting and Public Policy
100	No	Adopting wireless machine to machine	Whitehead, Steve	2005	Elektron
101	No	Directions for security and privacy for Semantic e-business applications	Thuraisingham B.	2005	Communications of the ACM
102	No	Critical success factors of web-based supply-chain management systems: An exploratory study	Ngai E.W.T., Cheng T.C.E., Ho S.S.M.	2004	Production Planning and Control
103	No	e-commerce on the docket	Sharp, Kevin R.	2001	Id Systems
End of Table					

Table 8: Publications added to the reviewed set, from cross-references.

#	Read	Title	Authors	Year	Source of publication
1	Yes	Design and validation of information security culture framework	Alhogail, Areej	2015	Computers in Human Behavior
2	Yes	Ensuring supply chain resilience: Development and implementation of an assessment tool	Pettit, T.J. and Croxton, K.L. and Fiksel, J.	2013	Journal of Business Logistics
3	Yes	Exploring the role of social capital in facilitating supply chain resilience	Johnson, Noel and Elliott, Dominic and Drake, Paul	2013	Supply Chain Management: An International Journal
4	Yes	Social capital configuration, legal bonds and performance in buyer-supplier relationships	Carey, Sinéad and Lawson, Benn and Krause, Daniel R.	2011	Journal of Operations Management
5	Yes	Ensuring Supply Chain Resilience: Development of a Conceptual Framework	Pettit, Timothy J. and Fiksel, Joseph and Croxton, Keely L.	2010	Journal of Business Logistics
6	Yes	BUILDING THE RESILIENT SUPPLY CHAIN	Christopher, Martin and Peck, Helen	2004	International Journal of Logistics Management
7	Yes	Crafting information technology governance	Peterson, Ryan	2004	Information Systems Management
End of Table					