Cyber Supply-Chain Security Challenges in the Context of Interorganizational Collaboration

Author: Johannes Henriksson (971227)

Semester: VT 2021

Course: IK442A – Master Thesis, Advanced, 30 credits

Subject: Informatics

Örebro University School of Business

Supervisor: M. Sirajul Islam

Examiner: Åke Grönlund

Abstract

Purpose: *A Cyber Supply-Chain (CSC) is defined as the linkages of multiple organizations working together exchanging (digital) products or services. Cyber Supply-Chain Security (CSCS) is the protection of this linkage encompassing the entire chain and all the components both physical and digital. The aim was to identify CSCS challenges when working with multiple organizations in an interorganizational collaboration context and to see specific CSCS challenges in Swedish organizations.*

Research methods: *The research design was as follows: literature reviews and interviews for data collection and qualitative inductive approach was used to develop a conceptual framework. The literature reviews were used to get an understanding of the topic and to identify CSCS challenges. The interview's aim was to investigate Swedish CSCS challenges and get additional information on CSCS challenges. The qualitative inductive approach was used to map up these challenges found in the literature reviews and to understand their relations.*

Findings: *The CSCS challenges found in both the literature reviews and interviews were multidisciplinary. Including but not limited to information security, IT security, cyber security, information system management, Supply-Chain Security, and Cyber Supply-Chain Risk Management. These multidisciplinary challenges can be seen as puzzle pieces to CSCS. The CSCS challenges were categorized via the qualitative inductive approach into five categories: communication; life cycle; points of penetration; cyber security objectives; multiple vendors. There were two main differences in the interviewee's challenges and the challenges seen in the conceptual framework. This was: all vendor organizational sizes have their unique challenges, and a Supply-Chain cannot strictly be looked at in the context of "the weakest link" if other security measures are in place.*

Conclusion: *CSCS can lead to devastating consequences not just for one organization but for every organization in the CSC. Thus, concluding the results are of benefit to the young field of CSCS and are significant in demonstrating the multidisciplinary nature of CSCS and its challenges.*

Keywords: Supply-Chain Security, Cyber Supply-Chain Security, Cyber Security, Cyber Supply-Chain Security Framework, Cyber Supply-Chain Security Challenges, Collaboration, Third Party, Interorganizational

Abbreviations, Acronyms, and Initialisms

Anon. 1 anonymous participant 1 7, 22–24, 29

Anon. 2 anonymous participant 2 7, 22–24

Anon. 3 anonymous participant 3 7, 22–24, 26

Anon. 4 anonymous participant 4 7, 22–24, 29

CIA Confidentiality, Integrity, and Availability 11, 20, 23, 25, 27, 42

CISA Cybersecurity & Infrastructure Security Agency 13, 17–21, 33

CPS Cyber-Physical Systems 1, 9, 11, 20

CSC Cyber Supply-Chain 1, 2, 7–12, 19–21, 26–28, 30, 31, 41, 42, A

CSCRM Cyber Supply-Chain Risk Management 8, 13, 16, A

CSCS Cyber Supply-Chain Security 1–14, 16–32, 38, 41–43, A

CyberSec Cyber Security 2, 6–13, 16, 17, 20, 22, 23, 25–31, 41–43

ENISA European Union Agency for Cybersecurity 15, 16, 26, 34

ICT Information and Communications Technology 8, 13–15, 17–21, 33

IEC International Electrotechnical Commission 12, 13, 17–21, 27, 34

IoT Internet of Things 1, 9, 15, 16

ISO International Organization for Standardization 12, 13, 17–21, 27, 34

IT Information Technology 1, 9, 11, 14, 22, 27, 41, A

NDIA National Defense Industrial Association 12, 17, 19, 20, 26, 35

NIST National Institute of Standards and Technology 12, 13, 16–21, 27, 35, 36

NISTIR NIST Interagency Report 12, 13, 35, 36

SC Supply-Chain 1, 2, 5, 8–16, 18, 19, 21–24, 26–28, 38, 41, A

SCRM Supply-Chain Risk Management 8, 12, 13, 17–21, 33

SCS Supply-Chain Security 1–3, 5, 7, 8, 10–16, 18, 19, 27, 30, 32, 41, A

Table of Contents

Listings

List of Figures

List of Tables

1 Introduction

There have been a lot of cyber-attacks and compromises to the Cyber Supply-Chain (CSC) in recent times, some examples are: the SolarWinds incident which significantly affected the Supply-Chain (SC) of 18000 customers Information Technology (IT) systems which included large organizations such as Microsoft and U.S. department of Justice (Krebs, 2021a; Lakshmanan, 2020a, 2020b, 2021b; Volz & McMillan, 2021). Another CSC cyber-attack was done against the American retail corporation Target in 2014, which originated from Target's third-party HVAC (Heating, Ventilation, and Air Conditioning) supplier. In the end, attackers had access to all of Target's internal network. (Hassija, Chamola, Gupta, Jain, & Guizani, 2020; Lu, Koufteros, Talluri, & Hult, 2019; Wilding & Wheatley, 2015; Zheng & Albert, 2019) Then finally, a software bug in the OpenSSL platform named Heartbleed compromised all OpenSSL web traffic, thus if an organization used OpenSSL as its web security, information could leak out ("CVE-2014-0160", 2014; Fruhlinger, 2017; Synopsys, 2020).

So, what is a SC and a CSC? According to Prokop (2017, p. 1) a broad definition of a SC is, "*the linkages of two or more organizations managed in such a way so as the whole is more valuable than the sum of its individual parts*". Hassija et al. (2020) stated that the definition of SC encompasses more than just the flow of materials, it encompasses the flow of information, services, and finances. Thus, this is the definition and scope of SC being used in this thesis, two or more organizations working together exchanging products, services, and or information. CSC is working on this definition and includes digital products or services, such as software updates of a product, digital controls, interfaces, and Cyber-Physical Systems (CPS) in the SC.

The devastating consequences a bad CSC could result, as the European Union has recommended more collaboration between private, public, and military (e.g., NATO) sectors. This is to utilize each other's services and avoid duplication of efforts. (Portesi et al., 2017) According to Santos (2020) many organizations are moving services and infrastructure to the cloud, as this changes capital expenditure to operational expenditure. Boiko, Shendryk, and Boiko (2019) wrote consumers expect more and more services to be interconnected. For example, airports, airlines, passengers, cargo, public transport, and fleets of cars; all connected, sharing information and making the user experience seamless from a mobile device (Boiko et al., 2019). The industry direction seems to be heading towards more collaboration and more use of other organizations' technologies.

With how devastating attacks against the SC can be to the organization, reputation, profit, safety, and more comes an important and interesting research area. How to secure a CSC and what challenges there are in Supply-Chain Security (SCS). The move to more use of technology, third-party vendors, and Internet of Things (IoT) in newer CSC just increases this importance (Ogbuke, Yusuf, Dharma, & Mercangoz, 2020; Sobb, Turnbull, & Moustafa, 2020). The SC has also become more global. Thus, SCS should account for multiple jurisdictions and vendors to get the products and services to the intended customer. (Zage, Glass, & Colbaugh, 2013) We have already seen more development in SCS for freight and container shipping after the 9/11 terrorist attack. There have been major improvements in how to mitigate attacks on the SC. (Li & Ye, 2008) However, the same cannot be said for Cyber Supply-Chain Security (CSCS). An ever-growing need for more academic research on CSCS to mitigate against cyber-attacks is needed (Linton, Boyson, & Aje, 2014; Sawik, 2020; Singh, Gunasekaran, Kaushik, & Pandey, 2020; Weiss et al., 2019).

1.1 Problem Formulation

Insecurities or weaknesses in the CSC can affect every organization in the chain. Therefore, CSCS is of utmost importance. CSCS is like any other form of Cyber Security (CyberSec) it is constantly evolving, and new vulnerabilities are discovered. Thus, there needs to be a systematic and agreed upon ways to communicate and maintain a good CSCS. To do this, both parties need to understand what CSCS challenges exist.

Having a good CSCS is not just one organization's responsibility as all third-parties involved can affect the entire CSCS. As Hassija et al. (2020) wrote, there are a lot of security risks and challenges when working with third-parties. We have seen that even when we have stopped working with a third-party supplier attacks against third-parties can still affect organizations that have worked with supplier (Hassija et al., 2020). This point stresses the importance of maintaining good CSCS and addressing potential CSCS challenges.

The academic research on SCS has increased as Blackhurst, Ekwall, and Martens (2015) and Hassija et al. (2020) found. However, Linton et al. (2014), Sawik (2020), Singh et al. (2020), and Weiss et al. (2019) concluded that there is a lack of academic research in the addition of information security and CyberSec in SCS research. Weiss et al. (2019) found a lack of inter-firm CyberSec research on SCS and collaboration of organization and the impact on the CSCS. In addition, the academic research on frameworks and practices handling interorganizational collaboration in the SC is also lacking. During the literature review we found some research such as Hou, Such, and Rashid (2019) who included the number of suppliers in their SCS framework aimed at information control systems. We saw this area of developing a conceptual framework for what challenges two separate organizations might encounter and thus, knowing what areas need protection would help to fill these research gaps. Obviously, not one single framework or method can secure a CSC or organization 100%, due to the ever-changing nature of CyberSec (Boyes, 2015; Sawik, 2020). However, this does not mean CSCS is futile. A framework of common CSCS challenges can be used as an intermediate language. This intermediate language can help reduce CSCS risk when introducing new or existing organizations into the CSC.

Therefore, based on the above problem formulation of the thesis, the thesis aims were to find challenges in CSCS when collaborating with multiple parties and vendors and understand their correlation with each other. This addressed multiple research gaps in CSCS research. Where this thesis was covering the addition of cyber, collaboration and inter-firm relationship with CSCS, and information security and CyberSec in the CSC. In addition, as Weiss et al. (2019) found that no SCS research was done in Sweden, this thesis also contributes to that aspect of CSCS research. The research aims and research gaps covered in this thesis is reflected in the research question and research objectives:

RQ1 What are the challenges in the management of CSCS in the context of interorganizational collaboration?

RObj1 To develop a conceptual framework in order to understand and map-up challenges related to CSCS management.

RObj2 To investigate the issues and challenges in the management of CSCS in the context of interorganizational collaboration in Sweden.

The research question (**RQ1**) was answered through multiple literature reviews and interviews to understand the CSCS challenges. The interviews focused on exploring Swedish CSCS challenges thus, helped to address **RObj2**. In order to operationalize **RObj1** a qualitative inductive approach was used to map-up the relationship of the identified CSCS challenges.

However, the interviews were with a limited number (4) of participants in a few (2) organizations. The development of the conceptual framework only used second order sources in the form of literature reviews. This was due to time constraints, however, we find the results are still beneficial and will help fill research gaps presented above in the young field of CSCS research.

1.2 Structure

The thesis is structured as follows, Section 2 presents the three-step research method used in the thesis. Section 3 presents the literature review and data collection towards developing the conceptual framework (see Subsection 3.4 for the framework). Section 4 presents the results from the interviews. Section 5 presents the discussion which was where the conceptual framework was also discussed. Section 6 presents some concluding remarks for the thesis. Subsection 6.1 presents the limitations of the thesis. Finally, Subsection 6.2 discusses future research based on this thesis and its limitations.

1.3 Target Group

This thesis is aimed at researchers in the field of SCS and CSCS, information security managers, and SCS and CSCS managers. One suggestion for information security managers and SCS/CSCS managers is to read Section 1, 3.4, 4, 5, and 6. This presents what the thesis is about as well as to see the developed conceptual framework and the challenges the Swedish organization perceived.

2 Research Methods

The approach of this thesis is based on a qualitative research approach. The two data collection methods used in the thesis were literature reviews and qualitative interviews. A conceptual framework was developed to operationalize **RObj1**, to understand the relationship of CSCS challenges found in the data collection methods. As the research question (**RQ1**) is aimed at identifying CSCS challenges, thus the method needed to be a form of data collection. Due to the interdisciplinary and young field and our time constraint, we choose the data collection to be qualitative (Bartol, 2014; Linton et al., 2014). The thesis data collection method is systematic literature reviews. These systematic literature reviews followed the methods of Webster and Watson (2002). This enabled a systematic way to understand a topic while also gathering information from trusted academic sources. This is a benefit seen in De Veaux, Velleman, and Bock (2016) to minimize sample biases that can arise from gathering first order sources. To augment the literature review and to help address **RObj2**, interviews of Swedish organizations were conducted to get a different perspective on CSCS challenges that was not present in the literature reviews (Weiss et al., 2019). To be able to address **RObj1** of understanding the relationships of the identified CSCS challenges there are multiple methods that can be used: design science, grounded theory, and qualitative inductive approach. **RObj1** aimed at producing a conceptual framework we saw the validation required of design science not to be able to fit within the timeframe of the thesis. In addition, the length to develop and evaluate the framework in grounded theory within the timeframe was not possible. Thus, we choose a qualitative inductive approach.

This method flow is depicted in Figure 2.1, the diagram depicts the main steps of the thesis in the rectangle boxes with the start depicted as an ellipse. The parallelograms depict the methods of each step. The triangles depict the research question and research objective each step tries to answer or address. The relationship of these aspects is shown with either solid or dashed lines representing either source relationship or linkage between two aspects. These methods are then explained more in depth in the following subsection.

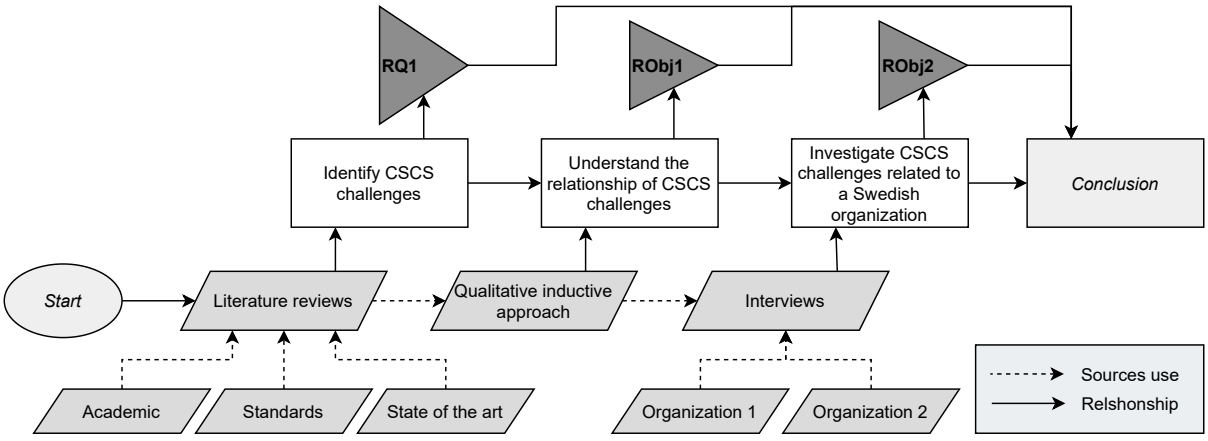

Figure 2.1: *Method diagram*

2.1 Literature Review

To be able to understand the CSCS challenges as well as to help answer **RQ1** literature reviews was used. Systematic concept centric literature reviews were conducted which followed the method of Webster and Watson (2002). To help answer **RQ1** three separate literature reviews

were conducted, (1) academic and scientific sources, (2) public and private standards, and (3) state of the art in organizations CSCS approach. This was done to help see a wider view into what challenges there are in CSCS. The systematic concept centric literature review began with a wide collection of information and articles about SCS and CSCS (Webster & Watson, 2002). All searches gave a low number of articles (less than 200 per database). We looked at the title and abstract of all of these and selected only the ones that seem relevant towards answering **RQ1**. For those more general search terms we only looked at the top 50 results to find relevant articles and refine our search term.

The collection of academic and scientific articles was used to see the state of the art is in academic research on CSCS as well as to investigate the CSCS challenges brought up in the academic literature. The academic literature review used the following databases: Örebro University's Primo, Web of Science, and IEEE Xplore. As the research area internally where SCS that was the first search term and keyword used. However, this yielded more results on physical SC on both maritime and containers, which was not the final aim of the study. Thus, the addition of cyber was used to focus on the research area of CSCS as this was the final aim of the study. The search terms used can be seen in Listing 2.1. The research field (CSCS) is young, thus, we did not specify a search restriction on the age of the article. However, the oldest article we found was from 2008, so our search window was from January 2008 to March 2021.

```
supply chain security
"supply chain security"
cyber supply chain security
"cyber" "supply-chain" "security"
```

Listing 2.1: *Search terms used in the literature review on academic and standards. Exact search- and keywords used on databases in the literature review for Cyber Supply-Chain Security. Quotation marks used to search to find content with those words in that specific order.*

The collection of public and private CSCS standards was used to see the current good practice in mitigating CSCS challenges as well as to see what common CSCS challenges are presented in standard documents. During the academic literature review standards and standard organization (both public and private) were noted down and were the standards and standard organizations used in this literature review. These standard organizations identified (see Appendix B) in the academic literature was then searched with the keywords seen in Listing 2.1 to find more standards that might not have been mentioned in the academic field of CSCS. This was done as the academic field of CSCS was young, and thus we assumed that not all relevant standards might not have been mentioned in the literature. However, we did not investigate standards that were decrepit according to the standard organization even if mentioned by academic literature.

The collection of organizational practices in CSCS was to get a current state of the art in CSCS challenges and good practices. During both the literature review on standards and academics, we noted down the public and private organizations which were used in this part of the literature review. An additional discussion of potential organizations that might have adopted CSCS practices was carried out with the supervisor which was also used. These organizations can be seen in Appendix C. This part of the literature review used the following databases: Örebro University's Primo, Web of Science, IEEE Xplore, and Google search. With the search terms seen in Listing 2.2 where the organization was appended to get their approach to CSCS mitigation, challenges, and state of the art.

```
[ORGANIZATION NAME] supply chain security
[ORGANIZATION NAME] cyber supply chain security
[ORGANIZATION NAME] supply chain security best practices
[ORGANIZATION NAME] Cyber supply chain security best practices
```

Listing 2.2: *Search terms used in literature review on the state of the art*
Exact search- and keywords used on databases in the literature review for the state of the art in Cyber Supply-Chain Security. The [ORGANIZATION NAME] where substituted with the organizations found in Appendix C

2.2 Qualitative Inductive Approach

To understand the relationship of the CSCS challenges (which was **RObj1**), a qualitative inductive approach was used to develop a conceptual framework of the CSCS challenges. The qualitative inductive approach followed the method of Thomas (2006). With the data collection of the literature reviews presented above. The main literature reviews used were on academic sources and public and private standards. The data from the data collection was then sorted into themes and key concepts in line with the research question (**RQ1**). This followed the coding process presented by Thomas (2006). Then the data had been sorted into first-order themes and key concepts, these first-order concepts were then grouped and categorized into second-order key concepts and themes. Then finally, the second-order concepts were analyzed and how they interacted with each other to find how all key concepts and themes relate and interact with each other. This was done iteratively until a conceptual framework of CSCS challenges had been developed and **RObj1** was addressed. (Thomas, 2006)

To demonstrate the coding process of Thomas (2006) in practice here how one node and category were constructed. For example these authors Singh et al. (2020) and Weiss et al. (2019) discussed the weakest link keyword of working with third-parties, Fukuda, Kawamura, Kubota, and Wataguchi (2019) and Singh et al. (2020) discussed challenges seen with weakened CSCS on smaller businesses. Thus, first-order concepts seem to be third-parties or multiple vendors, and a second-order concept seems to be the weakest link and the size of an organization. This is how all the first-order and second-order concepts were constructed then once all of them were made, similar concepts (such as multiple vendors and third-parties) were combined iteratively until a conceptual framework had been constructed.

2.3 Interviews and the Interviewed Organizations

Interviews were used to help address **RObj2** as all the interviewees were from Swedish organizations. The interviews followed the method of Brinkmann and Kvaled (2018) and semi-structured open-ended questions were used in the individual interviews. The interview questions were directly developed from the challenges in the conceptual framework. This means all the categories and nodes seen in the conceptual framework in Appendix A was used as a questions. Thus, the same motivation for why it is a challenge as the conceptual framework was used. The aim of the interview was twofold, (1) to get more information on CSCS challenges that might not be seen in the literature and (2) to find what CSCS challenges a Swedish organization may encounter. However, one could argue CyberSec is the same everywhere, so why would Sweden be different from let say the United States. Well, CyberSec is related to the maturity of CSCS practice in that country. This is one point in **RObj2** we wanted to analyze as this might bring out some unique challenges to Swedish organizations in the form of example: governing challenges or cultural challenges. With that, additional questions were made to probe what they saw as the main CSCS challenge and if they were challenges missing from our conceptual framework.

We also wanted to know if knowing these challenges before acquiring new CSC relationships would help mitigate security risks. These questions can be seen in Appendix D. The interviews were transcribed via notes then handed to the interviewee for confirmation that the transcribed information was correct. The interviewee had a chance then to alter answers to reflect their opinions better.

The interviewees were selected due to their expertise in SCS and CSCS and a total of four interviews were conducted from two government organizations.

Due to the anonymity, we cannot state what organization they work at. However, we can explain some general non-decrepit information about the organization. The interviewed participants were from two Swedish government organizations. These two organizations were both of hierarchical organizational structure. A hierarchical organizational structure, according to Saiti and Stefou (2020) is structured as a pyramid where the point delegates duties down the hierarchical levels. This organizational structure allows for great scalability and a clear form of leadership can be presented (Saiti & Stefou, 2020). These two Swedish government organizations work directly or indirectly with security and CyberSec as their aim. The two organizations procure software and hardware related to CyberSec from multiple vendors in an interorganizational context. Thus, CSCS is of importance to their operation. All the participants worked directly with CSCS either at a managerial level with security or in a specific security department. Table 2.1 presents the job titles of the four participants. This got us a wide range of different professions that dealt with CSCS with different viewpoints.

Table 2.1: *Job titles of the interviewees*

	Anon. 1	**Anon. 2**	**Anon. 3**	**Anon. 4**
Job title	Supplier manager	Chief information security officer	Agreement's manager	Information security manager

2.4 Ethical Considerations for the Research Methods

The two first steps; the literature review, and the development of the conceptual framework. Both use publicly available information; thus, no specific ethical consideration has been taken. However, for the interviews we have taken some ethical consideration, where we have informed all interviewees of the following (Brinkmann & Kvaled, 2018, p. 31-38):

- State the purpose of the interview and research as well as the interviewer's role in the research.
- Get the consent of the interviewee for participating in the interview and research.
- Inform the participant that they have the right to withdraw their consent and be withdrawn from the research.
- Inform the participant that they have the right to anonymity and confidentiality.
- The intent of the research and that anything in the research was made public.

We have decided not to collect any personal information from the participant as this was not necessary. As SCS and CSCS was a subject of security not to expose any vulnerabilities of the interviewee, a transcript of the interview was sent for approval where they had a chance to alter the information so that it can be used in the research and published publicly.

3 Related Research: Towards Developing a Conceptual Framework

This section helps to build the foundation of the conceptual framework. In Subsection 3.1 a literature review of scientific and academic articles, on the topic of SCS and CSCS is presented. In Subsection 3.2 a literature review of public and private standards in CSCS was conducted. These two were the foundation of the conceptual framework presented in Subsection 3.4.

Then finally, Subsection 3.3 investigates the state of the art in CSCS on a small selection of available public and private organizations. These three Subsections (3.1, 3.2, and 3.3) helped find the CSCS challenges in the context of interorganizational collaboration.

3.1 Literature Review

Due to the interdisciplinary nature of CSCS, different industries have started to work in CSCS. Due to this, multiple coined terms have been made for essentially the same thing. (Bartol, 2014) According to Bartol (2014) the following list are all essentially interchangeable:

- Information and Communications Technology Supply-Chain Risk Management (ICT SCRM)
- Information and Communications Technology Supply-Chain Security (ICT SCS)
- Supply-Chain Risk Management (SCRM)
- Cyber Supply-Chain (CSC)
- Cyber Supply-Chain Security (CSCS)
- Cyber Supply-Chain Risk Management (CSCRM)

Even though Bartol (2014) claims these are interchangeable, we do not fully agree as these terms focus on different areas within CSCS, thus, we will use the terms used in the respective literature.

According to Weiss et al. (2019) the addition of cyber in the SC does not necessarily make the CSC easier, it makes it more complex. Thus, we have seen as Annarelli, Nonino, and Palombi (2020) and Hassija et al. (2020) wrote, that the most critical asset an organization has is information and thus, information security becomes more important in CSCS. Lu et al. (2019) stated one of the most important factors was information security management realizing that information security was a corporate responsibility. Lu et al. (2019) concluded that top management affects the organizational culture which in turn affects SCS practices.

Barron et al. (2016) stressed the global importance of CyberSec in the success of SCS in the global economy and for safety critical systems. Fukuda et al. (2019) discussed the globalization of the CSC, how it becomes difficult in complying with all standards, laws, and regulations. Thus, we could see that CyberSec is important to the CSCS and as Weiss et al. (2019) stated that data breaches are a regular occurrence. C. Williams (2014, p. 382) wrote "*A deep-rooted sense of denial prevents many of us from acknowledging just how vulnerable the cyber supply chain really is*". Urciuoli, Männistö, Hintsa, and Khan (2013) wrote that cyber-crime is huge and costly and that cyber-attacks can facilitate traditional crimes such as cargo theft, smuggling, counterfeiting, and sabotage. Thus, in line with Linton et al. (2014), Lu and Koufteros (2019), and Sobb et al. (2020) that the topic of CSCS was important to national security performance

and vulnerabilities to the CSC could have devastating consequences. Fukuda et al. (2019) said cyber-attacks against organizations with insufficient CSCS had increased in recent years. We have also seen actual cases where information was leaked through the third parties CSC (Fukuda et al., 2019).

Ogbuke et al. (2020), Sobb et al. (2020), and Urciuoli (2015) discussed SC 4.0, Industry 4.0, and the globalization of the CSC, this adds more technology and IT services and systems to the CSC in the form of blockchain, artificial intelligence, CPS, IoT, and big data. Still, according to C. Williams (2014) the lack of understating in the CSCS is scary. Yet there is not much time until manufacturing of computers will happen at homes around the world in the same ease that we print airline tickets today. C. Williams (2014) expressed this concern about CyberSec and CSCS so elegantly:

> *At the root of our fears about the vulnerabilities of the supply chain specifically, and of cyber more generally, is the apprehension that our adversaries have proven better able to exploit the true form of cyber than we have, and even less comfortably, the darker fear that deep down, our failure to counter the success of our adversaries is our own fault.* (C. Williams, 2014, p. 384)

3.1.1 Threats, Challenges, and Vulnerabilities in the Cyber Supply-Chain

Kim and Im (2014) found several CSC challenges which are: CSC management including complete integration of CSC modules and continued improvement, responsibility management and integration of CSCS both technical and human resources, general information security and CyberSec challenges. Kim and Im (2014) presented two future challenges to CSCS is to take advantage of new technologies and as the CSC moves down the SC to primary, secondary, and tertiary vendors security measures must be in place.

According to Linton et al. (2014) we have seen more collaboration between public and private sectors. As Keegan (2014) argued for the strategies of promoting the domestic IT and infrastructure industry, which in turn does not promote good international collaboration in CyberSec to protect the SC and mitigate risk. This might be due to a lack of common understanding and approaches to CyberSec between countries (Keegan, 2014). Weiss et al. (2019) stated that partners should work together and be more transparent with their security to leverage each other's know-how to help mitigate and deal with the CSCS risks. Lu, Koufteros, and Lucianetti (2017) and Zage et al. (2013) said it is difficult to protect and maintain a CSC, as this spans over goods, factories, partners, fright, people, and information on numerous suppliers across multiple tires. However, Windelberg (2016) wrote that organizations typically only have visibility up- and downstream of one to two tiers and the complex and dynamic nature of the SC can make assessing risk and protecting the CSC difficult.

According to Lu et al. (2017), Singh et al. (2020), Wang and Franke (2020), Weiss et al. (2019), Yeboah-Ofori and Islam (2019), and Zage et al. (2013) a breach or disruption at any point or node in the SC can affect the entire global CSC. Thus, the CSC is only as secure as the weakest link. Wang and Franke (2020) gave an example of where a business bought payment processing from a third-party whose services goes down. Now the business cannot process payments and concludes that any third-party services the business relies on whose services could go down could cause business interruptions. (Wang & Franke, 2020)

According to Hou et al. (2019) and Weiss et al. (2019) the risk to the CSCS amplifies when working with multiple vendors and parties. Singh et al. (2020) presented an argument from industry experts, which stated that most real vulnerabilities to the CSC occur due to compromises in tier two and three suppliers. The authors continued that most of the risk in

CSCS was due to working with third-party suppliers (Singh et al., 2020). This might have been linked to a survey of Fortune 1000 companies (as cited in Keegan, 2014) where only 14% of companies mention SCS or outsourcing as major risks even after being asked if they perceive these as major risks. Fukuda et al. (2019) stated that small to medium-sized businesses tend not to have adopted adequate SCS measures. Singh et al. (2020) wrote that most attacks on the SC happened on small organizations. Thus, this puts an interesting risk on larger organizations who have these smaller organizations in their CSC (Singh et al., 2020).

According to Blackhurst et al. (2015) as the CSC becomes more global the need for CSCS becomes necessary. Fukuda et al. (2019) stated that more concern regarding SCS have increased. This is reflected that SCS threats were ranked 4th in Information-Technology Promotion Agency's 10 major security threats of 2019 (Information-Technology Promotion Agency, 2019). This concluded that more organizations need to taken CSCS more seriously and a deeper understanding of the threats to the CSC as well as how to mitigate and recover from said threats (Blackhurst et al., 2015). As Boyes (2015) wrote a cyber resilient system and CSC is not only a technical issue and challenge it also encompasses the human element. Lu and Koufteros (2019) claimed that most SCS breaches happened due to intentional acts which tends to be due to illicit activities. Kim and Im (2014) claimed that most CSCS problems can be traced to human error and not a technological vulnerability.

Hassija et al. (2020) found three main threats to the CSC, tampering and fraudulent substitution, not having the same security standard across the SC (especially with third-parties), and CyberSec. Hassija et al. (2020, p. 5) continued with third-party security risk with a survey result where 50% of the respondents perceive that the reason behind the increase in cyber-attacks was due to third-parties. These third-party challenges have been seen in the Target corporation breach as well as JP Morgan which both fell victim to data breaches due to their third-party supplier (Hassija et al., 2020). Hassija et al. (2020) also stated that there are incidents where data is leaked from third-parties even after relationships with the third-party have terminated.

Boyes (2015) presented some examples of what issues a bad CSCS could have, they presented cases of Dell shipping malware infected computers, HP shipping malware infected switches, Microsoft discovered new PCs shipped with pre-installed malware. Boyes (2015) also presented an interesting CSC risk where a cloud provider (2e2) went into liquidation and all the clients lost access to their data and services without paying an extra fee. Both Urciuoli et al. (2013) and Weiss et al. (2019) saw huge consequences of attacks against the CSC for the society. Urciuoli et al. (2013) and Weiss et al. (2019) speculated what a devastating consequence a Stuxnet like attack on the pharmaceutical SC or food SC would have on society.

3.1.2 Cost and Investment in Supply-Chain Security

Kim and Im (2014) said that with more security incidents makes it difficult for organizations to trust their CSC. According to Linton et al. (2014) involvement in CSCS could result in large gains and large losses. Z. Williams, Lueg, and LeMay (2008) wrote that one issue and challenge with SCS is that an organization may not know how well it is implemented until it is tested and thus, this fact significantly increases the difficulty in assessing SCS. According to Ni, Melnyk, Ritchie, and Flynn (2016) if the SC members do not see a monetary gain from investing in CSCS they may view it as an expenditure without benefit. Lu and Koufteros (2019) and Lu et al. (2017) both presented a theory where the cost of prevention and detection of attacks on the SC is often undervalued and it is hard to estimate the cost of prevented attacks. This theory is backed up by Lu et al. (2019) who wrote, SCS may not yield visible return on security investment. In agreement with Lu et al. (2017), Lu et al. (2019) the large cost of investing in SCS coupled with the low probability of a major SCS breach and that there are multiple parties

that needs to invest at the same time to secure the entire SC, have motivated some organization not to invest accordingly on SCS and Cyber Supply-Chain Security (CSCS).

Z. Williams et al. (2008) stated that some firms speculate that their SC would not be breached, thus justifying not investing in SCS. Z. Williams et al. (2008) continued that a few leading global shipping and carriers have invested in SCS and they assume that if a breach to the SC happened, it would affect all partners equally. Thus, with this view one could assume investment in the SCS was futile (Z. Williams et al., 2008).

3.1.3 Existing Frameworks, Models and Methods for Supply-Chain Security

Hou et al. (2019) developed a framework that takes into consideration the number of suppliers and their tiers for addressing security requirements in the SC. They also found that none of the existing frameworks and methods for securing information control systems have taken into consideration CSCS (Hou et al., 2019).

Li and Ye (2008) suggested a six-step process to improve SCS, making the total supply network visible, establishing comprehensive tracking and monitoring, preventing attacks at the source, inspection and process control, hiring and screening process control, and building a strong SCS team.

Annarelli et al. (2020) discussed the concept of a cyber resilient system, where a system is cyber resilient if it has two main features (1) robustness against potential predictable attacks, and (2) the ability to come back to a safe state without compromised system behavior and functionality when a successful attack has happened.

Yeboah-Ofori, Islam, and Yeboah-Boateng (2019) presented the concept of Cyber Threat Intelligence which is a proactive measure. Yeboah-Ofori et al. (2019) wrote that without Cyber Threat Intelligence it would be very difficult to effectively mitigate attacks, risk, and vulnerabilities against the CSC.

Roy, Gupta, and Deshmukh (2012) broke down the SCS into hard and soft security. Where hard security is about physical theft, damage to supply and so on, and soft security is about data security, technology, and management. This soft security included the flow of information, information sharing, IT systems, human error and risk, and third-parties and vendors. (Roy et al., 2012) Weiss et al. (2019) classified points of penetration to the CSC as technical, human, and physical. Lu and Koufteros (2019) and Lu et al. (2017) categorized the SCS practice in four classes, detection, prevention, response, and mitigation. Lu and Koufteros (2019) also stated that they believed prevention was the most important class.

Fukuda et al. (2019) suggested the outcome-based approach to SCS, where both parties agree on an outcome of security, for example, we need encryption of data in storage, however, they would not agree on exact encryption specifications. According to Fukuda et al. (2019) this outcome-based approach lightened the burden on security for both buyer and supplier. With an outcome-based approach both parties' security systems can be discussed and comply with each other's agreement via an intermediary language and at the same time does not expose any security vulnerabilities (Fukuda et al., 2019).

According to Boyes (2015) and Sawik (2020) with these complex and sophisticated CPS in the SC the traditional Confidentiality, Integrity, and Availability (CIA)-triad is not enough, and a better suited method would be the Parkerian hexad. The authors continued to state that the objective of CyberSec is to protect the six areas in the Parkerian hexad. The Parkerian hexad consists of the CIA-triad and includes the addition of utility, authenticity, and possession (Boyes, 2015; Sawik, 2020). Boyes (2015) points out that Parkerian hexad does not include trustworthiness. Thus, Boyes (2015) suggested the Parkerian hexad should be augmented

with safety and resilience to encompass trustworthiness. Windelberg (2016) listed the five objectives in Supply-Chain Risk Management (SCRM) as, security, reliability, safety, quality, and trustworthiness.

3.2 Public and Private Standards and Frameworks for Cyber Supply-Chain Security

Bartol (2014) argued that public, private, and academic stakeholders need to come together to help secure and maintain a good CSCS. Weiss et al. (2019) stated that the lack of accepted unified standards and guidelines for cyber defense to the CSC was hindering the development of a good cyber defense. Bartol (2014) continued that there are a number of standards for CSCS, however most of them originate from the National Defense Industrial Association (NDIA) Guidebook. Bartol (2014) explained that you can see an influence of the NDIA Guidebook in the following standards International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27036, National Institute of Standards and Technology (NIST) SP 800-53, and NIST Interagency Report (NISTIR) 7622. However, from the litterateur review (see Subsection 3.1) we could see that these standards brought up by Bartol (2014) seem to be the most prominent standards within CSCS. There were also additional standards seen in maritime and container SCS (such as ISO/IEC 28000, C-TPAT, and AEO) which were not presented here as this study was focused on general CSCS.

Weiss et al. (2019) said that many companies believe once they have achieved certification or accreditation of a standard in security, that they would always maintain the certification or accreditation. Thus, many companies believe that they do not have to improve their CyberSec measurements (Weiss et al., 2019). However, even how sophisticated and advanced your CyberSec measures are, it will still not be 100% secure due to the ever-changing nature of CyberSec (Boyes, 2015; Sawik, 2020).

3.2.1 NDIA Guidebook

NDIA (2008) discussed the vulnerabilities of SC and that no system was free of all vulnerabilities and that failure to a system may have greater consequences than just system functionality. NDIA (2008) presented the following vulnerabilities related to SCS: information sharing (sharing confidential information may lead to counterfeiters), change of supplier in the SC could introduce new vulnerabilities, and intentional undocumented addition to the product during development like insertion of Trojans, malware, and viruses.

3.2.2 ISO/IEC 27036

ISO/IEC (2014a) stated that a large significant of organizations had relationships with other vendors. Thus, most of these suppliers needed some information or access to the information system to provide their service. This introduced an information security risk to all members in the SC. All members both supplier and acquirer needed to take equal responsibility to uphold good information security, while also having to trust that the other party upholds their information security. Examples of these risks are software vulnerabilities and intentional or unintentional release of sensitive information. When acquiring a product or services it could be difficult to enforce your information security requirements on tier two and three suppliers as visibility upstream is limited. (ISO/IEC, 2014a)

ISO/IEC (2014a) presented some vulnerabilities and inherent information security risk when working with suppliers: weakness in governance which may lead to loss of information, or supplier

outsourcing part of the service thus reduction in control for the acquirer, miscommunication and misunderstanding in the supplier relationship, and geographical, social and cultural differences between supplier and acquirer. ISO/IEC (2014a) continued with specific examples of information security risk in the SC as: software or services with pre-existing vulnerabilities introduced in the SC; poor quality of product and services; counterfeited products or services; physical access to onsite systems; access, processing, and storage of information by supplier; and use of application and services not controlled and monitored by acquires of their information on the supplier's systems. (ISO/IEC, 2014a) ISO/IEC (2014b) specified how the life cycle of a supplier should be managed, including, planning, selection, agreement, management, and termination of a supplier relationship.

3.2.3 NIST

There are many NIST standards that dealt with directly or indirectly in SCS and CSCS. Thus, this subsection covered only the following NIST standards:

- NIST SP 800-53r5 (NIST, 2020c)
- NIST SP 800-161 (NIST, 2015)
- NISTIR 7622 (NIST, 2012)
- NIST cyber security framework v1.1 (NIST, 2018)

NIST (2020c) introduced the concept of outcome-based security controls and more about SCS and SCRM. NIST (2020c) provided security controls through SCRM, which was divided into 12 control categories, these categories provided mitigation for third-party vulnerabilities, counterfeited and altered products and services, information sharing risk and vulnerabilities, vulnerability disclosure and patch management, and more (NIST, 2020c).

The focus of NIST (2015) was to provide a guideline on identifying, assessing, selecting and implementing SCRM for Information and Communications Technology (ICT) SC. NIST (2015) disused some vulnerabilities in the ICT SC such as malicious modification of products and services, counterfeit products and services, and vulnerabilities due to poor manufacturing or development. NIST (2015) was an extension of NIST (2020c) to include more security controls specific for ICT SC and was an updated version of NIST (2012). One additional noteworthy addition in the NIST (2015) was that all security controls are marked at what tier level (first, second, and third) they needed to be implemented at.

The CyberSec framework was a risk-based approach to minimize CyberSec risk (NIST, 2018). NIST (2018) has been updated to include information for Cyber Supply-Chain Risk Management (CSCRM). NIST (2018) provided a use case of the framework as a common language when acquiring products and services into the SC with third-party vendors.

3.2.4 CISA ICT SCRM Task Force

Cybersecurity & Infrastructure Security Agency (CISA) ICT SCRM Task Force (2021) objective was focused on threat evaluation and not risk assessment; however, this threat evaluation contained the following: produce a set of procedures for conducting threat assessments with a focus on the global ICT SC as well as product assurance, data security, and SC risk. CISA ICT SCRM Task Force (2021) found and consolidated nine SC threats which were: counterfeit parts, external attacks on operation and capabilities, internal security operation and controls, system

development life cycle processes and tools, insider threats, economic risk, inherited risk (from other vendors in the SC), legal risk, and external end-to-end SC risk.

3.2.5 MITRE Supply-Chain Standards

The MITRE SC Attacks and Resiliency Mitigations (Heinbockel, Laderman, & Serrao, 2017) focused on providing mitigation on SCS attacks on ICT through the cyber resiliency engineering framework. Heinbockel et al. (2017) wrote that SC attacks can have a unique delivery method compared to traditional cyber-attacks. Heinbockel et al. (2017) found 41 attacks related to the SC, most of these attacks targeted the ICT systems. These 41 attacks were categorized into three categories: modification, insertion, and substitution of information, hardware, or services in the SC (Heinbockel et al., 2017).

3.3 Public and Private Organization Challenges in Supply-Chain Security

This subsection covers some private and public organization challenges and solutions to CSCS.

3.3.1 Atlantic Council

Herr, Loomis, Scott, and Lee (2020) wrote that software is everywhere and with software comes security flaws and constant software updates and patches from vendors. The constant stream of updates and patches creates a software SC. Organization moves to outsource more and more IT software products and services thus, adding to their software SC. More hardware functions become virtualized in software thus making the software SC even more of a critical component. (Herr et al., 2020)

According to Herr et al. (2020) software SC attacks have become more popular in recent times, as well as state sponsored attacks on the software SC. Thus, Herr et al. (2020) analyzed 115 software SC vulnerabilities in the past 10 years published in public blogs, write-ups, and articles. From the analysis the authors found the following five trends (Herr et al., 2020):

1. deep impact form state actors (such as Egypt, India, Iran, North Korea, Vietnam, Russia, and China)
2. hijacking updates (this was mainly performed by state actors or highly capable actors)
3. undermining code signing
4. open-source compromise (this was mainly performed by criminals)
5. app store attacks (this was mainly performed by criminals with monetary incentive)

3.3.2 Cisco

Cisco has recognized that we need to secure the entire SC and has named this the Cisco Value SC. A need to collaborate and encourage your partners to trust and build better CSCS is needed and have shown great results. CSCS should be applied throughout the entire end-to-end life cycle of a product and service. Cisco has defined these steps in the life cycle as follows: design, plan, source, make, quality, deliver, sustain, and end of life. A layered approach to CSCS was needed of physical-, logical-, information security, and security technology to mitigate against tainted and counterfeit solutions as well as misuse of intellectual propriety and third-party information security breaches. (Cisco, 2015, 2019a, 2019b; Conway, 2015a, 2015b, 2015c)

3.3.3 ENISA

European Union Agency for Cybersecurity (ENISA, 2015) introduced the concept of SC integrity as an abstract float value, where adding more links in the SC of unvetted suppliers lowers the overall SC integrity and vice versa. The authors continued with that there are no standards that have included the concept of SC integrity. ENISA (2015) also found seven challenges with SC integrity related to the ICT SC. These are (ENISA, 2015):

1. complex nature of a globally distributed SC
2. lack of common guidelines for achieving as well as measuring SC integrity
3. lack of tools, processes, and controls to verify SC integrity
4. ineffective tool and techniques for end user verification of products and services
5. lack of accepted tool and techniques to mitigate against counterfeited and tempering within system, products, and services
6. lack of coordinated effort to increase integrity of products and services
7. lack of integrity requirements across the ICT SC

ENISA (2020) researched SCS on IoT where they found several challenges to IoT SC. These challenges are as follows (ENISA, 2020):

- physical deliberate and intentional attacks
  - sabotage
  - gray market
  - inadequate physical enclosure
- intellectual property loss
  - theft of intellectual property
  - reverse engineering
  - overproduction and cloning
- nefarious activity and abuse
  - magnetic field attacks
  - insertion of malware
  - use of debug interface for malicious activities
  - counterfeits and tempering
- legal issues due to non-compliance of standards and regulations
- unintentional loss and or damage to information
  - compromised network
  - use of factory or default credentials
  - undetected additional software present in the SC

- human error
- unpatched or not up to date system being used
- cloud service disruptions
- system not being able to be recovered after an attack

ENISA (2020) provided an in-depth list of security controls and suggestions for good practice of IoT SC given the threats presented above. However, ENISA (2020) concluded their research with, to improve IoT SCS we should establish better relationships within the SC, CyberSec should be taken into consideration at every step as well as seriously, develop with security-by-design principals, and utilize existing standards and good practices in CSCS.

3.3.4 IBM

IBM has discovered from its partners five SCS challenges and issues which were: information protection, information being in multiple places across the SC, information sharing, fraud prevention, third-party vendor risk. To accommodate these challenges IBM have produced a list of SCS best practices which included: security risk management and risk assessment for all suppliers, vulnerability mitigation and scanning, utilizing digitization to get better visibility of the information flow, data identification and classification, data encryption, permission controls for information, trust transparency and provenance of information, and incident response system. (Ramos, 2020)

3.3.5 NIST

NIST (2020b) conducted a multiple case studies where they found eight key practices to help with CSCRM, which were as follows: integrate CSCRM across the organization, establish a formal program, know and manage your critical suppliers, understand your SC, closely collaborate with your key suppliers, include key suppliers in the organization resiliency and important activities, assess and monitor the SC, and plan for the full life cycle of the product and services. (NIST, 2020b)

NIST (2020a) summarized the case studies conducted with six organizations in 2019 as part of the multiple case studies presented in NIST (2020b) to help find these eight key practices. However, NIST (2020a) provided more detailed information used to correlate the key practices found in NIST (2020b). NIST (2020a) found that all the organizations interviewed confirmed the importance of CSCRM and collaboration with third-parties to help train them in CSCS. NIST (2020a) also presented the interviewees general approach to CSCRM which includes: to integrate CSCRM into the organization at all levels, utilize standardized CyberSec frameworks to enable a common language across organizations and streamline incident response communication, top management engagement in CSCRM, and integrate CSCRM into the organizational goals. NIST (2020a) also provided information on how organizations dealt with third-party risk which, was: setting CyberSec requirements on the suppliers and determine supplier criticality, which was done either by organization impact, supplier stability, delivery impact on the organization, if the supplier handles sensitive information, or if the supplier holds long term strategic advantages to the organization.

3.4 Development of the Conceptual Framework

Based on the CSCS challenges presented above in the literature reviews, a conceptual framework has been constructed via qualitative inductive approach. A summarized conceptual framework

can be seen in Figure 3.1 and the detailed conceptual framework can be seen in Appendix A. The references used in each category can be seen in Table 3.1 and the references used in all nodes can be seen in Tables 3.2, 3.3, 3.4, 3.5, and 3.6 in their respective subsections, where each category of the conceptual framework was motivated.

The CSCS challenges were categorized into five categories: communication, life cycle, points of penetration, CyberSec objectives, and multiple vendors; this is reflected in Figure 3.1. We found that all challenges discovered in the literature reviews could fit into one or more of these categories.

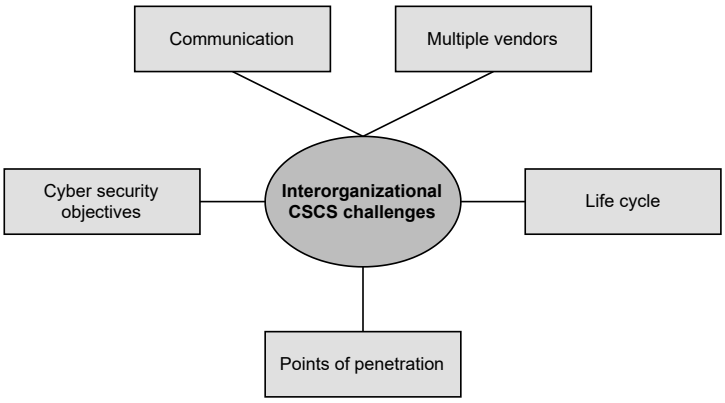

Figure 3.1: *Summary conceptual framework*

Table 3.1: *Summarized conceptual framework references*

Categories	References
Communicating	Annarelli et al., 2020; CISA ICT SCRM Task Force, 2021; Fukuda et al., 2019; ISO/IEC, 2014a; Keegan, 2014; Linton et al., 2014; Lu et al., 2017; Lu et al., 2019; Ni et al., 2016; NIST, 2018; Singh et al., 2020; Weiss et al., 2019; Z. Williams et al., 2008; Windelberg, 2016; Yeboah-Oforiand Islam, 2019
Life cycle	Bartol, 2014; Hassija et al., 2020; Heinbockel et al., 2017; ISO/IEC, 2014a, 2014b; Kim and Im, 2014; Lu and Koufteros, 2019; Lu et al., 2017; Lu et al., 2019; NDIA, 2008; Weiss et al., 2019
Cyber security objectives	Barron et al., 2016; Bartol, 2014; Boyes, 2015; CISA ICT SCRM Task Force, 2021; Hassijaet al., 2020; Heinbockel et al., 2017; ISO/IEC, 2014a; Kim and Im, 2014; NDIA, 2008; NIST 2015, 2020c; Sawik, 2020; Windelberg, 2016
Points of penetration	Boyes, 2015; CISA ICT SCRM Task Force, 2021; Heinbockel et al., 2017; ISO/IEC, 2014a; Lu et al., 2017; NDIA, 2008; NIST 2015; Roy et al., 2012; Weiss et al., 2019
Multiple vendors	CISA ICT SCRM Task Force, 2021; Fukuda et al., 2019; Hassija et al., 2020; ISO/IEC, 2014a; Li and Ye, 2008; Lu et al., 2017; NIST 2015; Singh et al., 2020; Wang and Franke, 2020; Weiss et al., 2019; Windelberg, 2016; Yeboah-Ofori and Islam, 2019; Zage et al., 2013

3.4.1 Communication

All the references for the category of communication in Figure 3.1 and nodes of that category in Appendix A can be seen in Table 3.2.

Table 3.2: *Conceptual framework communication references*

Category	Nodes	References
Communication	Communication issues	Keegan, 2014; Lu et al., 2017; Lu et al., 2019; NIST, 2018; Singh et al., 2020; Windelberg, 2016; Yeboah-Oforiand Islam, 2019
	Miscommunication & misunderstanding	Annarelli et al., 2020; ISO/IEC, 2014a; Windelberg, 2016
	Subject difficulty	Fukuda et al., 2019
	Cost	Linton et al., 2014; Lu et al., 2017; Lu et al., 2019; Ni et al., 2016; Z. Williams et al., 2008
	SCS requirements & responsibilities	Fukuda et al., 2019; ISO/IEC, 2014a
	Governance	CISA ICT SCRM Task Force, 2021; Fukuda et al., 2019; ISO/IEC, 2014a; Keegan, 2014; Weiss et al., 2019

Communication issues: We have seen communication being a major challenge in CSCS practices brought up by Lu et al. (2019), NIST (2018), and Windelberg (2016). The challenge of both communications up- and downstream for the entire SC being difficult was stated by NIST (2018), Singh et al. (2020), Windelberg (2016), and Yeboah-Ofori and Islam (2019).

Miscommunication & misunderstanding: Thus, as communication is of such importance to CSCS practices have ISO/IEC (2014a) borough up one challenge as miscommunication and misunderstanding which according to ISO/IEC (2014a) can be achieved via differences between acquirer and supplier in geographical, social, and or cultural.

Subject difficulty: Fukuda et al. (2019) discussed the challenge of subject difficulty, where one party might not want to disclose their SCS practices in the fear that it might expose some vulnerabilities.

Cost: Cost of CSCS practices was also seen a major challenge due to the difficulty of seeing accurate return on security investment, which was brought up by Linton et al. (2014), Lu et al. (2017), Lu et al. (2019), and Ni et al. (2016), Z. Williams et al. (2008)

SCS requirements & responsibilities: Fukuda et al. (2019) and ISO/IEC (2014a) discussed the challenge of making sure the clear and correct SCS requirements and responsibilities are communicated.

Governance: As the SC becomes more global and spans more and more countries, thus, the SCS must comply with multiple standards, regulations, and laws from different sometimes conflicting countries. This unique legal and governance CSCS challenge have been discussed by CISA ICT SCRM Task Force (2021), Fukuda et al. (2019), ISO/IEC (2014a), Keegan (2014), and Weiss et al. (2019)

3.4.2 Life Cycle

All the references for the category of life cycle in Figure 3.1 and nodes of that category in Appendix A can be seen in Table 3.3.

Table 3.3: *Conceptual framework life cycle references*

Category	Nodes	References
Life cycle	SCS life cycle	Bartol, 2014; Hassija et al., 2020; Heinbockel et al., 2017; ISO/IEC, 2014a, 2014b; Lu and Koufteros, 2019; Lu et al., 2017; NDIA, 2008
	Continued improvement	Bartol, 2014; Kim and Im, 2014; Lu et al., 2019; Weiss et al., 2019

SCS life cycle: Bartol (2014), Hassija et al. (2020), Heinbockel et al. (2017), ISO/IEC (2014a), and NDIA (2008) discussed the importance of maintaining a good CSCS throughout the end-to-end life cycle of the product or service. According to ISO/IEC (2014a, 2014b) the SC life cycle includes: planning, selection, agreement, management, and termination. Heinbockel et al. (2017), Lu and Koufteros (2019), and Lu et al. (2017) suggest that security should be invested early in the life cycle to make the effect more prominent and yield better return on security investment.

Continued improvement: Bartol (2014), Kim and Im (2014), Lu et al. (2019), and Weiss et al. (2019) discussed the importance of continually improve security measures in the CSC.

3.4.3 Points of Penetration

All the references for the category of point of penetration in Figure 3.1 and nodes of that category in Appendix A can be seen in Table 3.4.

Table 3.4: *Conceptual framework points of penetration references*

Category	Nodes	References
Points of penetration	Human	Boyes, 2015; CISA ICT SCRM Task Force, 2021; Lu et al., 2017; NIST, 2015; Roy et al., 2012; Weiss et al., 2019
	Physical	CISA ICT SCRM Task Force, 2021; NIST, 2015; Roy et al., 2012; Weiss et al., 2019
	Technical	CISA ICT SCRM Task Force, 2021; Heinbockel et al., 2017; ISO/IEC, 2014a; NDIA, 2008; NIST, 2015; Roy et al., 2012; Weiss et al., 2019

Lu et al. (2017) stated that most SCS breaches occur due to intentional acts. Weiss et al. (2019) categorizes SCS point of penetration as human, physical, technical. Weiss et al. (2019) classifies cyber risk into five categories, physical threats, breakdown, indirect attacks, direct attacks, and insider threats. These fit into the three points of penetration categories presented by Weiss et al. (2019). With these three categories we could map out the vulnerabilities found in Boyes (2015), CISA ICT SCRM Task Force (2021), ISO/IEC (2014a), NDIA (2008), NIST (2015), and Roy et al. (2012) into one of three vulnerability categories. For example, counterfeit hardware entering the SC is a physical entry point thus, its point of penetration is physical. If

this counterfeit product then includes hardware or software Trojans it is also a technical point of penetration. (CISA ICT SCRM Task Force, 2021; NDIA, 2008; NIST, 2015; Weiss et al., 2019)

3.4.4 Cyber Security Objectives

All the references for the category of CyberSec objective in Figure 3.1 and nodes of that category in Appendix A can be seen in Table 3.5.

Table 3.5: *Conceptual framework cyber security objectives references*

Category	Nodes	References
Cyber security objectives		Barron et al., 2016; Boyes, 2015; CISA ICT SCRM Task Force, 2021; Heinbockel et al., 2017; ISO/IEC, 2014a; NDIA, 2008; NIST, 2015; Sawik, 2020
	Confidentiality	Boyes, 2015; Hassijaet al., 2020; Heinbockel et al., 2017; NIST, 2015, 2020c; Sawik, 2020; Windelberg, 2016
	Integrity	Bartol, 2014; Boyes, 2015; Heinbockel et al., 2017; NIST, 2015; Sawik, 2020; Windelberg, 2016
	Availability	Boyes, 2015; Heinbockel et al., 2017; Sawik, 2020; Windelberg, 2016
	Authenticity	Bartol, 2014; Boyes, 2015; Sawik, 2020; Windelberg, 2016
	Possession	Boyes, 2015; Hassijaet al., 2020; Kim and Im, 2014; Sawik, 2020
	Resilience	Boyes, 2015; Hassijaet al., 2020; NDIA, 2008; NIST, 2015, 2020c; Windelberg, 2016
	Safety	Boyes, 2015; Hassijaet al., 2020; NDIA, 2008; NIST, 2020c; Windelberg, 2016
	Utility	Boyes, 2015; Sawik, 2020

Boyes (2015) and Sawik (2020) argues that with these complex CPS in the CSC, the traditional CIA-triad is not enough and to properly protect and mitigate against challenges and risk to the CSC. However, Boyes (2015) and Sawik (2020) argues that the Parkerian hexad with the addition of trustworthiness is required to adequately protect the CSCS. According to Linton et al. (2014) the CSCS field is inherently interdisciplinary encompassing from security to management. Heinbockel et al. (2017) stated:

> *Supply chain attacks, just like any cyber attack, exploit a target system and then seek to control, execute and maintain presence on that system. So, a supply chain attack once delivered, will appear to a network defender like any other cyber attack.* (Heinbockel et al., 2017, p. 18–19)

Thus, according to Barron et al. (2016), CISA ICT SCRM Task Force (2021), ISO/IEC (2014a), NDIA (2008), and NIST (2015) compromises to the CyberSec objectives can lead to insertion of counterfeit parts, vulnerabilities (intentional or unintentional), physical access, compromises to the information flow regarding the CIA-triad, and many more. Thus, we see a challenge is to secure all the CyberSec objectives in the Parkerian hexad with the addition of trustworthiness (in the form of safety and resilience) (Boyes, 2015).

These CyberSec objectives are as follows:

- confidentiality

- integrity
- availability
- authenticity
- possession
- resilience
- safety
- utility

3.4.5 Multiple Vendors

All the references for the category of multiple vendors in Figure 3.1 and nodes of that category in Appendix A can be seen in Table 3.6.

Table 3.6: *Conceptual framework multiple vendors references*

Category	Nodes		References
Multiple vendors	SC relationship & large area		CISA ICT SCRM Task Force, 2021; Fukuda et al., 2019; ISO/IEC, 2014a; Lu et al., 2017; Weiss et al., 2019; Zage et al., 2013
		Weakest link:	Hassija et al., 2020; Lu et al., 2017; Singh et al., 2020; Wang and Franke, 2020; Weiss et al., 2019; Yeboah-Ofori and Islam, 2019; Zage et al., 2013
		Visibility	ISO/IEC, 2014a; Li and Ye, 2008; NIST, 2015; Windelberg, 2016
	Medium to small businesses		Fukuda et al., 2019; Singh et al., 2020

SC relationship & large area: CISA ICT SCRM Task Force (2021), Fukuda et al. (2019), ISO/IEC (2014a), Lu et al. (2017), Weiss et al. (2019), and Zage et al. (2013) stated that one challenge with CSCS is the large area that the SC encompasses, thus the acquirer and supplier inherits security risk when establishing a SC relationship.

Weakest link: One challenge to the CSCS is according to Hassija et al. (2020), Lu et al. (2017), Singh et al. (2020), Wang and Franke (2020), Weiss et al. (2019), Yeboah-Ofori and Islam (2019), and Zage et al. (2013) that CSCS is only as secure as the weakest link.

Visibility: ISO/IEC (2014a), Li and Ye (2008), NIST (2015), and Windelberg (2016) states that the reduced visibility in the SC is a challenge in CSCS.

Medium to small businesses: Fukuda et al. (2019) and Singh et al. (2020) states that most CSC attacks happened on medium to small businesses.

4 Results: Swedish Cyber Supply-Chain Security Challenges

This section presented the results from the interviews of the four participants. The interview questions used can be seen in Appendix D. All participants wanted to stay anonymous in both name and organization, with that they will be referred to as "anonymous participant 1–4".

This section is structured as follows. It begins with an introduction where the interviewees present their definition of CSCS and its related disciplines. Then the five categories of the conceptual framework and its related question come next. Then we take in their refections where we gather the interviewee's main challenges and new challenges. Then finally, a summary of the findings can be seen in Section 4.8.

4.1 Cyber Supply-Chain Security Definitions

All the interviewees described CSCS a bit differently, however, all agreed that it is an umbrella term of important subjects to secure and maintain a secure SC from both inside and outside threats. Anonymous participant 2 (anon. 2) concluded the description with "*to be able to trust one's SC*".

All the interviewees saw information security, CyberSec, IT security and CSCS as having relations to each other. Here anonymous participant 3 (anon. 3) stated "*the CSCS can affect all of these disciplines, thus, all need to work individually to be able to work together*", which we feel is a great summary of these disciplinary relationships to CSCS.

4.2 Communication

The interviewees saw different main communication challenges. Anonymous participant 1 (anon. 1) focused on time; anon. 2 focused on efficacy of the process; anon. 3 focused on the subject of security, knowledge, and its diffuseness; anonymous participant 4 (anon. 4) focused on aim, requirements, and viewpoints.

For the governing documents, all agreed it is a challenge however, anon. 2 and anon. 4 only agreed if the vendor, person, or acquirer is not knowledgeable and well versed in the governing documents that this is the main challenge and not the governing documents themselves. Anon. 4 stated "*the acquirer needs to have high proficiency in the governing documents to be able to do its job properly*". There were no specific Swedish governing documents for CSCS, there were some about procurement that anon. 1 and anon. 2 discussed, however, these were not about security and only specific to state and municipal Swedish organizations.

All agreed that requirements and responsibilities is a CSCS challenge. Anon. 1 and anon. 4 both stated that, both parties need to be communicating in the same language and have the same viewpoint. However, anon. 2 and anon. 3 did not agree that misunderstandings and misinterpretations was a challenge, with the argument "*we have not seen it at us*". The same could be said for subject difficulty with half agreeing it is a challenge and the other being mixed about it. Anon. 2 looked at it interestingly, "*I do not see it a challenge, rather we have momentum for it, many people and industries have started to discuss and take into consideration these points and become more interested and emerged in CyberSec*". This opinion was also seen by anon. 4.

Anon. 1, anon. 2, and anon. 3 saw the cost being a challenge with similar viewpoints, return on security investment being hard to estimate, or as anon. 3 said that in their organization the economics department was separated from the security department which sometimes leads to expensive security solutions the organization could not afford.

None of the interviewees saw or reflected on the vendor's reputation as a challenge, stating it is not relevant in their procurement process.

4.3 Life Cycle

The interviewees saw different life cycle challenges, anon. 1 saw the life cycle itself and in relation to what happens if the vendor gets bought up, anon. 2 also saw if the vendor gets bought up and what happens if the product or service gets changed during its life cycle, anon. 3 saw, have we received to correct untampered product and how to administer and maintain the product, and anon. 4 saw the life cycle itself and when terminating a product or service who owns the information as a challenge.

All saw similar steps in this life cycle adopting much from the product life cycle including a bit of sourcing from vendors. On the continued improvement anon. 1 stated "*yes, it is a challenge to make a system secure today and even tomorrow with tomorrow's new challenges and a potential new 'normal', with the constant development of new technologies, as a major challenge*". This constant phase was also seen by anon. 4. Anon. 3 saw this constant improvement to be a challenge depending on how one organization has implemented security into the organization workflow, for example in a DevSecOps fashion or as an added on after the fact.

4.4 Points of Penetration

All saw the same three points of penetrations: human, technical, and physical. No new examples of attacks were given that were not seen in the literature for example anon. 2 who presented SC interdiction which is a form of targeted physical attack that utilizes hardware and software alterations.

4.5 Cyber Security Objectives

All saw the CIA-triad to be essential and the base of a good CSCS. The opinions of the other CyberSec objectives were varied, and we got a lot of questions around the semantics and definitions of these objectives. With that, a summary of the results can be seen in Table 4.1, as we can see no objective was unanimously disagreed upon. However, Anon. 2 and anon. 4 each agreed traceability was missing from these objectives.

Table 4.1: *A summary of all the interviewees opinions on the CyberSec objectives.*

CyberSec Objective	**anon. 1**	**anon. 2**	**anon. 3**	**anon. 4**
Confidentiality	Yes	Yes	Yes	Yes
Integrity	Yes	Yes	Yes	Yes
Availability	Yes	Yes	Yes	Yes
Authenticity	Yes	Yes	Yes	Yes
Possession	No	Yes	No	Yes
Utility	Yes	No	Yes	Not really
Trustworthiness	No	No	Yes	Yes
Availability	Kind of	Kind of	Yes	Yes
Reliability	Yes	Not really	Yes	Yes
Resilience	Yes	No	Yes	Yes
Safety	Yes	Kind of	No	Yes
Security	Yes	Yes	Yes	Yes

4.6 Multiple Vendors

All saw challenges with multiple vendors with a similar focus on responsibility, agreements, viewpoints, and visibility. All saw challenges with both large and small organizations. Anon. 1 saw "*a larger organization dealing with multiple customers and thus, having access to multiple organizations' information. This puts larger organizations as a target for criminal adversaries*". Anon. 2 saw a large organization may have a hard time to view over themselves making it easy to miss an information leak. Anon. 1 stated small organization may not have implemented the same level of security a large one has, and anon. 3 said a small organization may not have the same level of visibility and knowledge into their SC. Anon. 2 discussed that larger organizations tend to be certified or have accreditation in security while this is rarer in smaller organizations. However, all agreed and concluded that all sizes have their own challenges.

All saw to some extent that both the number of vendors and the physical area being a challenge. The visibility was also unanimously seen as being poor when dealing with multiple vendors up or down, however, no clear preference of which direction was seen as better. No one saw CSCS to be futile and even anon. 2 states "*it is even more important now that we have this new knowledge to use*".

Anon. 1 and anon. 4 both saw the SC as a chain with a weakest link, this was expected. However, both anon. 2 and anon. 3 did not see it this way. Anon. 2 argument for why it is not the weakest link is as follows:

> *Naturally, it is the weakest link. However, I do not know if that is correct. A bad product in a system does not make the system bad if there are other security controls in place, with this I would argue it is between the weakest and average vendor.* (Anon. 2)

4.7 Interviewee Reflections

Anon. 1 concludes with the most important CSCS challenges being dependability; trusting vendors, products, and agreements; and making sure hardware and software is not maliciously alerted on its way. Anon. 2 concludes that the most important CSCS challenge is the transportation phase of both hardware and software. Anon. 2 suggests "*this [transportation] challenge is best addressed via agreements and standards*". Anon. 3 concludes that "*communication is vital to understand the CSCS risk there are*". Anon. 4 concludes that the acquirer's knowledge and competency is vital to maintain a good CSCS.

Anon. 1 came up with a challenge not presented which were the vendors are monetarily incentivized and with that not always the securest solution or process is done to save time and money. Anon. 2 saw one area not discussed where "*how do we mitigate against SC interdiction and how do we choose what threats to address and what threats do we accept the risk of*". Anon. 4 added that having a list of vendors we have worked with helps us know who we have dealt with and what follow-ups we have done.

All agreed that knowing these challenges would increase the overall CSCS and bring these challenges up when procuring products or services would be a benefit and as anon. 2 said, "*good questions give good answers and a good discussion, and all forms of negation are about meeting in the middle*".

4.8 Summary of the Interviews

All the interviews had slightly different perspectives on the CSCS challenges. The **communication** challenges focused on time, cost, diffuseness of the subject, aim, requirements, and viewpoints. These CSCS challenges were seen in the literature reviews, however, all interviewees did not agree on all the challenges seen in the literature, mainly about the governing documents, requirements and responsibilities, and subject difficulty. The unanimously disagreed challenge was the vendor's reputation stating "it is not relevant to CSCS".

The **life cycle** challenges focused on the future, including vendors getting bought up and tampering with products or services. The challenges of what happens if a vendor got bought up were not seen in the literature and are interesting life cycle challenges. The interviews highlight the importance of CyberSec future impact (both positive and negative) on an organization.

For the **points of penetration** challenges, nothing new that was not seen in the literature was presented. The same three attack vectors (human, technical, physical) were discussed. The interview only stressed the importance of a secure delivery phase of a product or service.

The **CyberSec objectives** was the challenge most divisive among the interviewees, as can be seen in Table 4.1. The interviews suggest that an additional objective was missing namely, traceability. This objective was not seen in this literature review and is a common CyberSec objective and often added on to the CIA-triad. The main conclusion that could be drawn here is that every product or service has different objectives that are vital and needs protection.

The challenges seen with **multiple vendors** were very interesting as some differed from the literature. For the small to medium size business being less secure the interviewees agreed however, they concluded that all organization sizes have their unique challenges from small to large. This was sort of seen in the literature with the examples of CSCS breaches affecting large enterprises. Another interesting thing, half of the interviewees brought up was the disagreement of the weakest link challenges, stating that you can protect your system to mitigate some of the weakest links and turn it into almost an average link. This line of thought was very interesting and reassuring that CSCS is not futile and can be protected.

5 Discussion

It was unexpected how little academic research on CSCS we found. With how devastating and common CSCS attacks and breaches seem to be. Within the writing process multiple CSCS attacks were published in media such as a breach in the PHP repository (Anderson, 2021; Constantin, 2021; Osborne, 2021), a Microsoft Exchange zero-day vulnerability (Lakshmanan, 2021a; Microsoft, 2021; Palmer, 2021), and a breach in a water treatment facility where the attacker tried to poison the water supply (Krebs, 2021b; Robles & Perlroth, 2021). It was also surprising how lax some organizations took CSCS as Z. Williams et al. (2008) found some organization CSCS approaches were. Another interesting thing was the article by Keegan (2014), who argued for the promotion of domestic CSC with the ease of governance compliance and the knowledge of standardized minimum security. With as much in-house software and closer you are to the CSC are benefits seen in NDIA (2008). However, with the globalization of the CSC, this becomes more difficult and costly (NDIA, 2008). This is an interesting point of view in CSCS that goes into ENISA (2015) SC integrity keeping your SC partners few and in high quality and security reduces CSCS risks.

It was fascinating to find these CSC attack vectors and in theory how difficult they would be to mitigate if they are exploited early in the CSC. After reading David and Sakurai (2018) which discussed the insertion of hardware Trojans into integrated circuits and the article by Gupta, Tiwari, Bukkapatnam, and Karri (2020) who discussed CSCS challenges within the 3D printing industry. Both present some devastating consequences for CSCS when attacks are implemented early in the CSC. After reading these two articles, we speculated some interesting potential CSCS attacks: inserting malicious code and hardware into integrated circuits in an aircraft and being able to weaken materials, and changing CAD drawings for the same aircraft. The limited visibility you have upstream makes these attacks hard to impossible to find if you are multiple vendors down the CSC.

5.1 Cyber Supply-Chain Security Challenges

The CSCS challenges found in this thesis have been categorized into five areas: communication, multiple vendors, points of penetrations, CyberSec objectives, and life cycle. The **communication** challenges were found to be focused on stating the right thing, to the right person, at the right time, in an understandable agreed upon language. The literature reviews found that standards and governing documents can be a challenge. However, this was not seen in the interviews where they found it to be a helping point both in communicating and in knowing if a vendor had met certain guidelines. A challenge seen by both was cost, specifically return on security investment being difficult to accurately estimate, especially when discussing attacks that have not happened or been prevented.

The **life cycle** and the continued improvement raised some challenges focusing on looking at the bigger picture of the CSC and in longer terms. Here we saw challenges such as how to acquire and what to acquire, how to terminate an agreement and what information is left, and who owns this information. We also saw challenges in improving security and as anon. 3 saw that it also depends on how one organization has implemented security in their organization.

The three **points of penetration** we found were: human, technical, and physical. These are quite wide and cover a large range of attack vectors. The main point with this wideness was to show that CSCS attacks can happen essentially everywhere and are not limited to one area. This is a challenge and coupled with multiple vendors indicating that the point of penetration can happen anywhere in the CSC. For example, a weakness in the physical infrastructure letting

hardware getting modified before it reaches your organization.

The **CyberSec objectives** challenges demonstrate that a product, service, and or SC can be breached at multiple objectives and result in a "bad" product. The interviews focused on the CIA-triad as the base while the other objectives deepened the interpretation of what product or service we have. We agree to this line of thought that not all objectives are essential or even applicable to all products or services you acquire in a CSC. In general, from the information, we have gathered we would state that all of these objectives need to be accounted for and argued which are important or not important for a product or service.

The **multiple vendors** challenges were focused on the lack of control and visibility an acquirer may have. The weakest link has been argued here as the importance of proper CSCS controls which we saw in the interviews helping to mitigate this point. Still, this is a challenge. We also found the size of the vendor to change what challenges are seen. We did not find a size (small, medium, large) that was objectively better in terms of CSCS. This was interesting as the literature review hinted at larger organizations being better and at the same time presenting multiple cases of large CSCS attacks on these large organizations.

These challenges really show that CSCS is not an easy job and covers many areas to properly protect one organization. CSCS also requires good teamwork and communication to get these different disciplines and areas to work together with a common goal of maintaining and improving CSCS.

5.2 Research Objective 1: Conceptual Framework

We chose to develop a conceptual framework as this visualized the qualitative data we gathered. According to Verdinelli and Scagnoli (2013) this is an essential step in theory building. We agree upon as this conceptual framework model helped group and reduce the number of key concepts. Making the developed conceptual framework a great summary of what CSCS challenges an organization might encounter. The challenges constructed in the conceptual framework were not unique. However, it was quite interesting how multidisciplinary CSCS was. Where we found information security management, traditional CyberSec practices, IT security practices, physical security, SCS practices, and system development practices.

The conceptual framework had five nodes with a few number of references[1] for its motivation. Two of which we feel were not clear enough in its motivation due to the additional references not mentioning the CSCS challenge directly.

Communication → communication issues → subject difficulty this was the node with the least number of references at only one. However, NIST (2018, 2020c) discusses communication via outcome-based approach, the same solution that Fukuda et al. (2019) proposed to combat the subject difficulty. As the NIST standards did not present the challenge of subject difficulty and only one solution to it. We would also argue that the point Lu et al. (2019) brought up with top management's trickle-down effect on CSCS practice and if top management does not promote and communicate good CSCS to its organization a weakened effect on CSCS can be seen. These two arguments are circumstantial, and we feel fitted better here in a discussion and not in the qualitative inductive approach as they are indirectly arguing for this point.

Communication → SCS requirements & responsibilities this node was a very clear and unique communication challenge presented by the two ISO/IEC (2014a, 2014b) standards. We also saw, however, not mention clearly enough to include as a source in the NIST

[1] less references than the first quartile of the references in each node, $Q_1 = 4$

(2012, 2015) standards but in most of the security controls and not presented as a CSCS challenge. Thus, we did not include these references for the same reason as the *subject difficulty* node.

The other three nodes with few references[2] were:

Communication → communication issues → miscommunication & misunderstanding this was a clear information security management challenge and a general challenge when working in a global CSC. It is, however, a clear communication issue which is why it is under that second level node. We have gone back and forth discussing if it should be merged into communication issues or be left as a separate node. In the end, we feel it is a distinct enough CSCS challenge not to be merged.

Cyber security objectives → utility this is part of the core of the Parkerian hexad, which was motivated as essential to maintaining good CyberSec. With the abundance of references, we have used to motivate why CyberSec objectives are an important CSCS challenge we feel justifies its inclusion in the framework.

Multiple vendors → medium to small businesses which we feel the motivation behind is very clear. That smaller organization may not have adopted adequate CSCS measures, and a SC is only as secure as its weakest link. One could argue this is also part of the *weakest link* node. However, the weakest link can be a large organization like Microsoft or SolarWinds and still be the weakest link. This point is presenting that one should be extra careful when working with smaller organizations. Thus, we feel it is separate from the *weakest link* and is distinct enough to yield a separate node in the framework.

The interviews provide new challenges and new perspectives not seen in the literature reviews. There were two main points brought up in the interviews that we feel need to be reflected in the conceptual framework. (1) All organization sizes have unique challenges, the same line of smaller size may not have adequate CSCS measures, however, larger organizations are not immune and might be a larger target of attacks. (2) the tractability CyberSec objective was missing and seen as vital objectives, which we also agree was missing from the Parkerian hexad. These two changes we feel need to be reflected in an extended conceptual framework, this is depicted in Appendix E. Two other interesting points brought up were the weakest link and the relation between cost and security. For the weakest link one should still plan for it accordingly with proper security controls, with that we feel it is still a challenge. Discussing the relation between cost and security and that vendor may choose a less secure method just to save money and or time is a distinct challenge. However, we would argue this is a part of the communication cost challenge seen in the conceptual framework.

The conceptual framework seen in Appendix A and E helped address **RObj1** quite well. We were able to gather and understand the relationships of the challenges seen in this thesis. The conceptual framework was depicted in two versions: a summary (see Figure 3.1) and a detailed version (see Appendix A[3]). Both capture the challenges very well with the detailed version providing an easier understanding of what each category represents. We also acknowledged that no assessment or evaluation of the conceptual framework has been done, this was not the aim of the **RObj1**. Thus, we state **RObj1** is addressed in this thesis. However, One could also argue that developing the interview question based on the conceptual framework was a form of

[2]See footnote 1

[3]This detailed version was also extended with the information gathered via the interviews and can be seen in Appendix E

evaluation of said conceptual framework. Thomas (2006) suggests using interviews to assess the trustworthiness of the developed conceptual framework, which we did in this thesis. However, not to the extent we feel needed to confidently say "we have assessed or evaluated the developed conceptual framework" which is due to the limitations of the interviews. However, we wanted to address this partial step in the thesis.

5.3 Research Objective 2: Swedish Cyber Supply-Chain Challenges

The interviews provided some very interesting points and perspectives not seen in the literature reviews. One very interesting point was the two perspectives seen in the weakest link. Anon. 1 and anon. 4 saw the other security controls in place being able to help protect the overall security in CSCS, thus it not being a weakest link. We do agree with this argument that it is not as black and withe and it should be between the weakest and average link. However, if you come in with the mindset of the weakest link and protect from there that seems to be a good way to handle this challenge.

It was also interesting how they all looked at large organizations to have challenges and not as seen in the literature review being mostly small to medium size businesses. During the interviews when they laid out the challenges, they saw with large organizations we agree with them and have drawn the same conclusion that challenges exist with all sizes however, different challenges emerge deepening on the size of the organization you are working with.

It was interesting how anon. 1 looked at continued improvement as we do not know what challenges that arise tomorrow and how the world can change leading to a new normal with new challenges. This got us reflecting on the recent pandemic and how it quickly changed what technologies we needed day-to-day. For example, the increase in video conferencing solutions and what security implications this may have had.

With the CyberSec objectives, it was interesting how one could state "yes, this is vital" while another could say "no, I do not see this being a challenge". This was probably due to them having different backgrounds and how multidisciplinary CSCS was. It might also be because they did not have the same definitions of these terms. However, as we did not have one objective with a clear disagreement, we consider them to be CSCS challenges but to different degrees deepening of what you are doing.

The four interviews in the two Swedish organizations helped address **RObj2**. However, due to the interviewees only being in a public organization we have an obscured view into private organizations CSCS challenges. But these interviews provided new perspectives to look at the CSCS challenges seen in the conceptual framework as well as new CSCS challenges not seen in the literature. As we did not claim in the **RObj2** to investigate CSCS challenges in both private and public organizations and as the interviews were not the main research question, we conclude that we have addressed this research objective, but we note that more interviews, especially with private organizations, would be better. However, we do consider only conducting interviews with Swedish government and municipality organizations being better here as these are national Swedish organizations, and thus we would get a better insight into Swedish CSCS challenges compared to more global private organizations that happened to do work in Sweden.

5.4 Research Question: Identifying Cyber Supply-Chain Challenges

Research question (**RQ1**) was "*What are the challenges in the management of CSCS in the context of interorganizational collaboration?*" and this thesis have explored a wide variety of interorganizational CSCS challenges in academic, scientific, standards, state of the art, and

interviews of specific Swedish organizations. These sources have presented a good representation of what CSCS challenges seem to exist. With the addressing of both research objectives and the development of the extended conceptual framework as well as the additional literature review of organizations CSCS challenges. We would conclude that the research question is answered and the results can be summarized into the conceptual framework seen in Appendix E.

This thesis contributed towards CSCS research and helped fill the research gaps presented by Linton et al. (2014), Sawik (2020), Singh et al. (2020), and Weiss et al. (2019). Where we explored CyberSec and inter-firm relationships and what CSCS challenges these presents. We also developed a conceptual framework based on these challenges. This is something seen by Hou et al. (2019) as missing: CyberSec in a SCS framework.

The results of the thesis were not groundbreaking, we did, however, summarize and explore CSCS challenges in a wide variety of ways. We also, to our knowledge was the first to develop a conceptual framework of CSCS challenges. Also, to our knowledge was the first to investigate Swedish CSCS challenges, however, similar they might be to the global CSCS challenges that exist. Thus, we would state the results presented here are of benefit to the field of CSCS research in giving light to the wideness of areas that are included in CSCS and the importance of everyone responsibility in protecting the global CSCS.

We would argue the CSCS challenges in the thesis are applicable to other organizations. As Boyes (2015) and Sawik (2020) wrote, no single framework, model, or method can make an organization 100% immune against CyberSec vulnerabilities and this can also apply to CSCS vulnerabilities. With that, we would say “knowing is half the battle”. Knowing how multidisciplinary CSCS challenges are and a representation of what they are is a great benefit. This was backed up by the interviews as a great benefit in mitigating CSCS challenges. We would state that the results are significant. They can be used by organizations to identify these CSCS challenges and from their build mitigation steps to secure their CSC.

6 Conclusions

This thesis investigated CSCS challenges in the context of interorganizational collaboration. CSCS challenges can lead to devastating consequences as the CSC is interconnected. Meaning if one vendor somewhere in that CSC encounters CSCS attacks the entire CSC could be affected. We have also seen more globalization and more vendors in the CSC in recent times. With this incense making CSCS even more critical. We investigate what CSCS challenges an organization might encounter when introducing new vendors and generally working with multiple vendors.

The research question and aim were to investigate and identify challenges with CSCS in the context of interorganizational collaboration. This was done through two research objectives (**RObj1** and **RObj2**) to operationalize the work. These research objectives developed a conceptual framework to map-up the CSCS challenges seen in the thesis (**RObj1**) and investigated Swedish CSCS challenges (**RObj2**). The research question (**RQ1**) was answered in the thesis. We have presented a wide range of multidisciplinary challenges seen in CSCS in academics, standards, state of the art, and in Swedish organizations. **RObj1** where to operationalize the relationships with the CSCS challenges discovered. The aim of **RObj1** was to construct a conceptual framework of CSCS challenges seen in the literature reviews. This was done through a qualitative inductive approach. The conceptual framework developed five main categories (communication, multiple vendors, life cycle, points of penetration, and CyberSec objectives). The categories captured the range and multidisciplinary nature of CSCS challenges seen in the context of interorganizational collaboration. With this categorization and development of the conceptual framework (see Appendix A, E) **RObj1** is concluded as addressed. **RObj2** where to investigate Swedish CSCS challenges as this was something not found in any literature in the literature reviews. This also brought new perspectives into CSCS challenges that the academic and standards did not present. The aim of **RObj2** was to investigate CSCS challenges seen in Swedish organizations. This investigation was done via interviews, the interviews were conducted on Swedish government organizations further pointing to only investigate Swedish organizations and no multinational organization. With the interviews and new CSCS challenges and perspectives seen from the Swedish government organization **RObj2** is concluded as addressed.

The results from either the conceptual framework or the challenges seen in the Swedish organization all provided what areas we should look for when collaboration with other vendors and the potential challenges that can arise. Thus, we state the results of this thesis are beneficial. We would argue that these challenges are transferable to any organization working with multiple vendors. However, some challenges may be more or less relevant to deepening on the maturity of your CSCS practices of both the supplier and acquirer.

To conclude, it was interesting how devastating attacks against a CSC can be and what severe consequences these attacks can have. This coupled with how young the field is and how little academic research there was, makes this an interesting and scary field to study. The field was also surprisingly multidisciplinary both in what it covered and from whom research and practice has been initiated by.

6.1 Limitations

This thesis had three main limitations, two with the development of the conceptual framework and one with the interviews.

For the conceptual framework, no rigorous assessment or evaluation has been done. This means we cannot assess the conceptual framework's trustworthiness and state if it is properly applicable. All sources and thus challenges in the conceptual framework were gathered from

second order sources i.e., the two literature reviews. With the newness of the topic and the young field of CSCS there was a limited amount of literature, specifically about CSCS. However, there were more on SCS which is related. This was also a young field. Thus, the second limitation where the number of trusted sources to use in the development of the conceptual framework.

The main limitation of the interviews was the limited number of participants (4) and limited selection of organizations (all being government organization). This was due to time constraints as well as the ability to find relevant participants with experience in CSCS practice.

6.2 Future Work

An assessment and evaluation of the developed conceptual framework seen in Section 3.4 and Appendix E should be done. This is to gather how applicable the findings in this thesis are as well as to corroborate the challenges presented are representative of CSCS challenges seen in organizations around the globe. In addition, collecting and developing new CSCS conceptual frameworks, from more first order sources (and from public and private organizations in more countries). Then evaluating it against the one developed here to see differences and similarities would also be interesting.

Another future research area is to develop a way to communicate these challenges when acquiring new interorganizational relationships. To properly mintage against these known CSCS challenges. This being a checklist, framework, method, or something similar. To make the communication as seamless and mitigate misunderstands and miscommunications.

A need for more academic research on different areas of CSCS. Also, in line with Weiss et al. (2019) findings, more CSCS research is needed in European, African, and South American countries. According to Weiss et al. (2019) majority of CSCS research is from the United States of America, United Kingdom, and India.

References

Anderson, T. (2021). PHP repository moved to GitHub after malicious code inserted under creator rasmus lerdorf's name. Retrieved March 30, 2021, from https://www.theregister.com/2021/03/29/php_repository_infected/

Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering*, *149*, 1–18. doi:10.1016/j.cie.2020.106829

Barron, S., Cho, Y. M., Hua, A., Norcross, W., Voigt, J., & Haimes, Y. (2016). Systems-based cyber security in the supply chain. In *2016 IEEE systems and information engineering design symposium (SIEDS)* (pp. 20–25). doi:10.1109/SIEDS.2016.7489299

Bartol, N. (2014). Cyber supply chain security practices DNA – filling in the puzzle using a diverse set of disciplines. *Technovation*, *34*(7), 354–361. Special Issue on Security in the Cyber Supply Chain. doi:10.1016/j.technovation.2014.01.005

Blackhurst, J., Ekwall, D., & Martens, B. J. (2015). Special issue on supply chain security [special issue]. *International journal of physical distribution & logistics management*, *45*(7). doi:10.1108/IJPDLM-04-2015-0104

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia Computer Science*, *149*, 65–70. ICTE in Transportation and Logistics 2018 (ICTE 2018). doi:10.1016/j.procs.2019.01.108

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, *5*, 28–34. doi:10.22215/timreview/888

Brinkmann, S., & Kvaled, S. (2018). *Doing interviews* (2nd edition). London, United Kingdom.

Cybersecurity & Infrastructure Security Agency (CISA) Information and Communications Technology (ICT) Supply-Chain Risk Management (SCRM) Task Force. (2021). *Information and communications technology supply chain risk management task force – threat evaluation working group: Threat scenarios – version 2.0*. Retrieved from https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report-v2.pdf

Cisco. (2015). Cisco supply chain security. Retrieved February 10, 2021, from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/supplychainsecurity.pdf

Cisco. (2019a). 3rd party cloud service provider security: The value chain security perspective. Retrieved February 10, 2021, from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-third-party-cloud-security-infographic.pdf

Cisco. (2019b). Cisco value chain security program. Retrieved February 10, 2021, from https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/value-chain-security.pdf

Constantin, L. (2021). PHP backdoor attempt shows need for better code authenticity verification. Retrieved March 31, 2021, from https://www.csoonline.com/article/3613593/php-backdoor-attempt-shows-need-for-better-code-authenticity-verification.html

Conway, E. (2015a). For value chain security collaboration, use a carrot with your stick. Retrieved February 10, 2021, from https://blogs.cisco.com/security/for-value-chain-security-collaboration-use-a-carrot-with-your-stick

Conway, E. (2015b). Securing the supply chain is a collaborative effort. Retrieved February 10, 2021, from https://blogs.cisco.com/security/securing-the-supply-chain-is-a-collaborative-effort

Conway, E. (2015c). Securing the supply chain throughout the product lifecycle. Retrieved February 10, 2021, from https://blogs.cisco.com/security/securing-the-supply-chain-throughout-the-product-lifecycle

CVE-2014-0160. (2014). Available from National Vulnerability Database, CVE-ID CVE-2014-0160. Retrieved January 25, 2021, from https://nvd.nist.gov/vuln/detail/CVE-2014-0160

David, M., & Sakurai, K. (2018). Hardware trojan cyber-physical threats to supply chains. (pp. 448–455).

De Veaux, R. D., Velleman, P. F., & Bock, D. E. (2016). *Stats: Data and models* (4th ed.). Boston: Pearson.

European Union Agency for Cybersecurity (ENISA). (2015). Supply chain integrity: An overview of the ICT supply chain risks and challenges, and vision for the way forward.

ENISA. (2020). Guidelines for securing the internet of things: Secure supply chain for IoT. doi:10.2824/314452

Fruhlinger, J. (2017). What is the heartbleed bug, how does it work and how was it fixed? Retrieved January 25, 2021, from https://www.csoonline.com/article/3223203/what-is-the-heartbleed-bug-how-does-it-work-and-how-was-it-fixed.html

Fukuda, Y., Kawamura, I., Kubota, Y., & Wataguchi, Y. (2019). Supply chain security measures using outcome-based approach. *Fujitsu Scientific & Technical Journal*, *55*(5), 23–29.

Gupta, N., Tiwari, A., Bukkapatnam, S. T. S., & Karri, R. (2020). Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks. *IEEE Access*, *8*, 47322–47333. doi:10.1109/ACCESS.2020.2978815

Hassija, V., Chamola, V., Gupta, V., Jain, S., & Guizani, N. (2020). A survey on supply chain security: Application areas, security threats, and solution architectures. *IEEE Internet of Things Journal*, 1–25. doi:10.1109/JIOT.2020.3025775

Heinbockel, W. J., Laderman, E., & Serrao, G. J. (2017). *Supply chain attacks and resiliency mitigations*. (MTR170477). Retrieved from https://www.mitre.org/publications/technical-papers/supply-chain-attacks-and-resiliency-mitigations

Herr, T., Loomis, W., Scott, S., & Lee, J. (2020). *Breaking trust: Shades of crisis across an insecure software supply chain*. Atlantic Council. Retrieved February 10, 2021, from https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf

Hou, Y., Such, J., & Rashid, A. (2019). Understanding security requirements for industrial control system supply chains. In *2019 IEEE/ACM 5th international workshop on software engineering for smart cyber-physical systems (SEsCPS)* (pp. 50–53). doi:10.1109/SEsCPS.2019.00016

Information-Technology Promotion Agency. (2019). 10 major security threats 2019. Retrieved February 12, 2021, from https://www.ipa.go.jp/files/000076989.pdf

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). (2014a). *Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts*. International Organization for Standardization. (ISO/IEC Standard No. 27036-1:2014). Geneva, CH. Retrieved from https://www.iso.org/standard/59648.html

ISO/IEC. (2014b). *Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements*. International Organization for Standardization. (ISO/IEC Standard No. 27036-2:2014). Geneva, CH. Retrieved from https://www.iso.org/standard/59680.html

Keegan, C. (2014). Cyber security in the supply chain: A perspective from the insurance industry. *Technovation*, *34*(7), 380–381. Special Issue on Security in the Cyber Supply Chain. doi:10.1016/j.technovation.2014.02.002

Kim, K., & Im, I. (2014). Research letter: Issues of cyber supply chain security in korea. *Technovation*, *34*(7), 387–388. Special Issue on Security in the Cyber Supply Chain. doi:10.1016/j.technovation.2014.01.003

Krebs, B. (2021a). Sealed u.s. court records exposed in solarwinds breach. Retrieved February 1, 2021, from https://krebsonsecurity.com/2021/01/sealed-u-s-court-records-exposed-in-solarwinds-breach/

Krebs, B. (2021b). What's most interesting about the florida water system hack? that we heard about it at all. Retrieved March 30, 2021, from https://krebsonsecurity.com/2021/02/whats-most-interesting-about-the-florida-water-system-hack-that-we-heard-about-it-at-all/

Lakshmanan, R. (2020a). Microsoft says solarwinds hackers accessed some of its source code. Retrieved February 1, 2021, from https://thehackernews.com/2020/12/microsoft-says-solarwinds-hackers.html

Lakshmanan, R. (2020b). Nearly 18,000 solarwinds customers installed backdoored software. Retrieved February 1, 2021, from https://thehackernews.com/2020/12/nearly-18000-solarwinds-customers.html

Lakshmanan, R. (2021a). Hackers are targeting microsoft exchange servers with ransomware. Retrieved March 30, 2021, from https://thehackernews.com/2021/03/icrosoft-exchange-ransomware.html

Lakshmanan, R. (2021b). Solarwinds hackers also accessed u.s. justice department's email server. Retrieved February 1, 2021, from https://thehackernews.com/2021/01/solarwinds-hackers-also-accessed-us.html

Li, T., & Ye, Q. (2008). New thoughts about supply chain security after 9-11 terrorist attack. *2*, 2397–2400. doi:10.1109/SOLI.2008.4682937

Linton, J. D., Boyson, S., & Aje, J. (2014). The challenge of cyber supply chain security to research and practice – an introduction. *Technovation*, *34*(7), 339–341. Special Issue on Security in the Cyber Supply Chain. doi:10.1016/j.technovation.2014.05.001

Lu, G., & Koufteros, X. (2019). Organizing practices to combat supply chain security breaches. *IEEE Engineering Management Review*, *47*(3), 72–78. doi:10.1109/EMR.2019.2931540

Lu, G., Koufteros, X., & Lucianetti, L. (2017). Supply chain security: A classification of practices and an empirical study of differential effects and complementarity. *IEEE Transactions on Engineering Management*, *64*(2), 234–248. doi:10.1109/TEM.2017.2652382

Lu, G., Koufteros, X., Talluri, S., & Hult, G. T. M. (2019). Deployment of supply chain security practices: Antecedents and consequences. *Decision Sciences*, *50*(3), 459–497. doi:10.1111/deci.12336

Microsoft. (2021). Analyzing attacks taking advantage of the exchange server vulnerabilities. Retrieved April 6, 2021, from https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/

National Defense Industrial Association (NDIA). (2008). *Engineering for system assurance*. National Defense Industrial Association. (NDIA Guidebook). Arlington, VA. Retrieved from https://www.ndia.org/-/media/sites/ndia/meetings-and-events/divisions/systems-engineering/sse-committee/systems-assurance-guidebook.ashx

Ni, J. Z., Melnyk, S. A., Ritchie, W. J., & Flynn, B. F. (2016). Why be first if it doesn't pay? the case of early adopters of C-TPAT supply chain security certification. *International Journal of Operations & Production Management*, *36*(10), 1161–1181. doi:10.1108/IJOPM-01-2015-0041

National Institute of Standards and Technology (NIST). (2012). *Notional supply chain risk management practices for federal information systems*. National Institute of Standards and Technology. (NISTIR 7622). doi:10.6028/NIST.IR.7622

NIST. (2015). *Supply chain risk management practices for federal information systems and organizations*. National Institute of Standards and Technology. (NIST No. SP 800-161). doi:10.6028/NIST.SP.800-161

NIST. (2018). *Cybersecurity framework version 1.1*. National Institute of Standards and Technology. (NIST Cybersecurity Framework Version 1.1). doi:10.6028/NIST.CSWP.04162018

NIST. (2020a). *Case studies in cyber supply chain risk management: Summary of findings and recommendations*. National Institute of Standards and Technology. doi:10.6028/NIST.CSWP.02042020-1

NIST. (2020b). *Key practices in cyber supply chain risk management: Observations from industry*. National Institute of Standards and Technology. (NISTIR 8276 [Draft]). doi:10.6028/NIST.IR.8276-draft

NIST. (2020c). *Security and privacy controls for information systems and organizations*. National Institute of Standards and Technology. (NIST No. SP 800-53). doi:10.6028/NIST.SP.800-53r5

Ogbuke, N. J., Yusuf, Y. Y., Dharma, K., & Mercangoz, B. A. (2020). Big data supply chain analytics: Ethical, privacy and security challenges posed to business, industries and society. *Production Planning & Control*, 1–15. doi:10.1080/09537287.2020.1810764

Osborne, C. (2021). Official PHP Git server targeted in attempt to bury malware in code base. Retrieved March 30, 2021, from https://www.zdnet.com/article/official-php-git-server-targeted-in-attempt-to-bury-malware-in-code-base/

Palmer, D. (2021). Microsoft exchange server attacks: 'they're being hacked faster than we can count', says security company. Retrieved April 6, 2021, from https://www.zdnet.com/article/microsoft-exchange-server-attacks-theyre-being-hacked-faster-than-we-can-count-says-security-company/

Portesi, S., Chatzichristos, G., Drogkaris, P., Trimintzios, P., Dufkova, A., Palkmets, L., & Liveri, D. (2017). *Cybersecurity in the EU common security and defence policy (CSDP): Challenges and risks for the EU*. doi:10.2861/853031

Prokop, D. (2017). *Global supply chain security and management* (1st ed.). Oxford, United Kingdom: Butterworth-Heinemann.

Ramos, M. (2020). What is supply chain security? Retrieved February 10, 2021, from https://www.ibm.com/blogs/supply-chain/what-is-supply-chain-security/

Robles, F., & Perlroth, N. (2021). Dangerous stuff: Hackers tried to poison water supply of florida town. Retrieved March 30, 2021, from https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html

Roy, A., Gupta, A. D., & Deshmukh, S. G. (2012). Information security in supply chains — a process framework. In *2012 IEEE international conference on industrial engineering and engineering management* (pp. 1448–1452). doi:10.1109/IEEM.2012.6837986

Saiti, A., & Stefou, T. (2020). Hierarchical organizational structure and leadership. *Oxford Research Encyclopedia of Education*. doi:10.1093/acrefore/9780190264093.013.709

Santos, O. (2020). *Cisco CyberOps associate CBROPS 200-201 official cert guide*. Indianapolis, Indiana: CISCO Press.

Sawik, T. (2020). A linear model for optimal cybersecurity investment in industry 4.0 supply chains. *International Journal of Production Research*, *0*(0), 1–18. doi:10.1080/00207543.2020.1856442

Singh, R. K., Gunasekaran, A., Kaushik, A., & Pandey, S. (2020). Cyber security risks in globalized supply chains: Conceptual framework. *Journal of global operations and strategic sourcing*, *13*(1), 103–128. doi:10.1108/JGOSS-05-2019-0042

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11). doi:10.3390/electronics9111864

Synopsys. (2020). The heartbleed bug. Retrieved January 25, 2021, from https://heartbleed.com/

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American Journal of Evaluation*, *27*(2), 237–246. doi:10.1177/1098214005283748

Urciuoli, L. (2015). Cyber-resilience: A strategic approach for supply chain management. *Technology innovation management review*, *5*(4), 13–18. doi:10.22215/timreview/886

Urciuoli, L., Männistö, T., Hintsa, J., & Khan, T. (2013). Supply chain cyber security – potential threats. *Information & security*, *29*, 51–68. doi:10.11610/isij.2904

Verdinelli, S., & Scagnoli, N. I. (2013). Data display in qualitative research. *International Journal of Qualitative Methods*, *12*(1), 359–381. doi:10.1177/160940691301200117

Volz, D., & McMillan, R. (2021). Solarwinds hack breached justice department system. Retrieved January 10, 2021, from https://www.wsj.com/articles/solarwinds-hack-breached-justice-department-systems-11609958761

Wang, S. S., & Franke, U. (2020). Enterprise IT service downtime cost and risk transfer in a supply chain. *Operations Management Research*, *13*(1), 94–108. doi:10.1007/s12063-020-00148-x

Webster, J., & Watson, R. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Weiss, M., Caldwell, N. D., Wilding, R., Ghadge, A., Weiß, M., & Caldwell, N. D. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply chain management*, *25*(2), 223–240. doi:10.1108/SCM-10-2018-0357

Wilding, R., & Wheatley, M. (2015). Q&a. how can i secure my digital supply chain? *Technology Innovation Management Review*, *5*, 40–43. doi:10.22215/timreview/890

Williams, C. (2014). Security in the cyber supply chain: Is it achievable in a complex, interconnected world? *Technovation*, *34*(7), 382–384. Special Issue on Security in the Cyber Supply Chain. doi:10.1016/j.technovation.2014.02.003

Williams, Z., Lueg, J. E., & LeMay, S. A. (2008). Supply chain security: An overview and research agenda. *The international journal of logistics management*, *19*(2), 254–281. doi:10.1108/09574090810895988

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

Yeboah-Ofori, A., Islam, S., & Yeboah-Boateng, E. (2019). Cyber threat intelligence for improving cyber supply chain security. In *2019 international conference on cyber security and internet of things (ICSIoT)* (pp. 28–33). doi:10.1109/ICSIoT47925.2019.00012

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future Internet*, *11*(3). doi:10.3390/fi11030063

Zage, D., Glass, K., & Colbaugh, R. (2013). Improving supply chain security using big data. In *2013 IEEE international conference on intelligence and security informatics* (pp. 254–259). doi:10.1109/ISI.2013.6578830

Zheng, K., & Albert, L. A. (2019). A robust approach for mitigating risks in cyber supply chains. *Risk Analysis: An International Journal*, *39*(9), 2076–2092. doi:10.1111/risa.13269

Appendix A Conceptual Framework: Interorganizational CSCS Challenges

The interorganizational Cyber Supply-Chain Security (CSCS) challenges conceptual framework with all nodes and subnodes for the five categories depicted (see Figure A.1). This framework is meant to represent the main CSCS challenges seen when two organizations are collaborating, thus integrating each other into a common Supply-Chain (SC).

The order and placement of the categories, nodes, and subnodes are not representing anything specific, however, the lines show the relations between the categories, nodes, and subnodes.

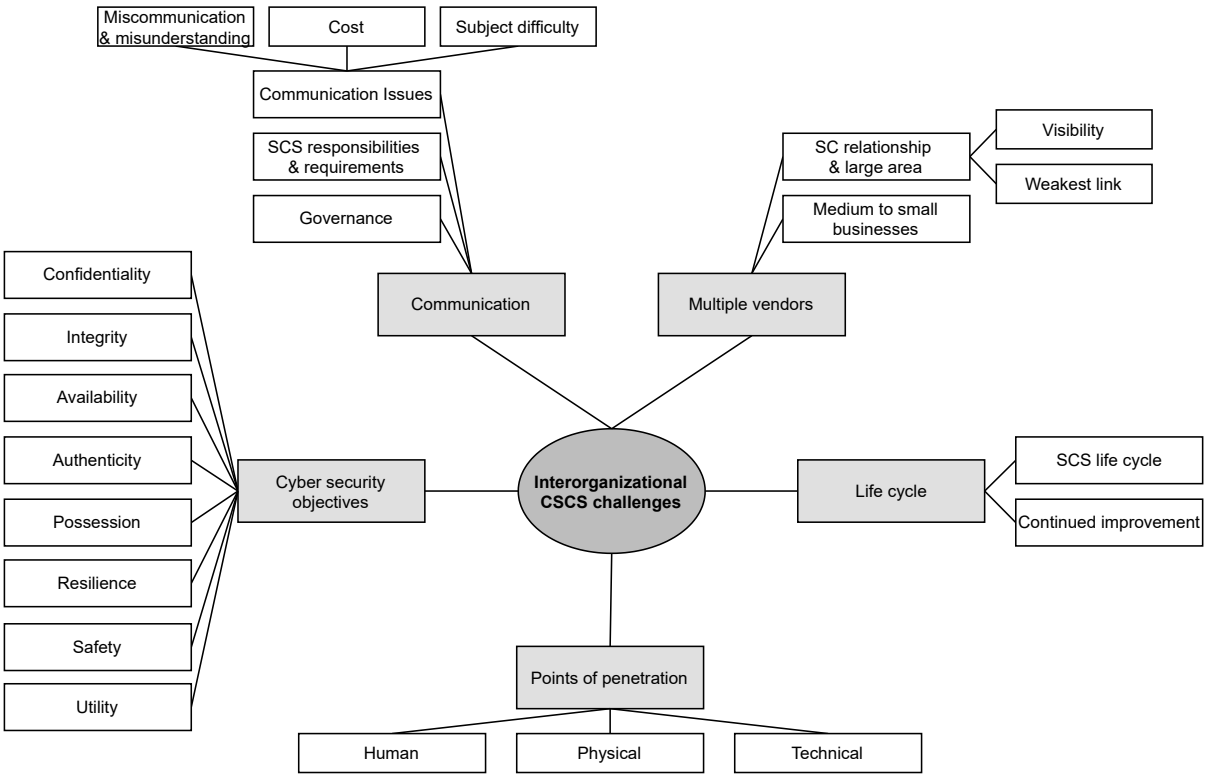

Figure A.1: *Detailed conceptual framework*

Appendix B List of Standards and Standard Organization for the Literature Review

This appendix presents the standard and standard organization found (see Listing B.1) in the first literature review on academic and scientific sources.

```
Authorised Economic Operator (AEO)
CISA ICT SCRM Task Force
Consistently Optimized REsilient Secure Global Supply-Chains (CORE)
Customs-Trade Partnership Against Terrorism (C-TPAT)
DoD Key Practices 2009-2010
ISO/IEC
ISO/IEC 28000
ISO/IEC 12207
ISO/IEC 15288
ISO/IEC 27036
MITRE
MITRE's Adversary Attack, Techniques & Common Knowledge (ATT&CK)
NDIA Guidebook
NIST
NISTIR 7622
NIST SP 800-171
NIST SP 800-53
NIST SP 800-82
OWASP
SAFECode
UK Centre for Protection of National Infrastructure (CPNI) Good Practice
    ↪ Guide for Process Control
```

Listing B.1: *List of standards and standard organization*

Appendix C Organizations List for the Literature Review

This appendix presents the organization found (see Listing C.1) in the two literature reviews as well as in the discussion with the supervisor.

```
Atlantic Council
Cisco, Inc
ENISA
Fire Eye
Fujitsu
IBM
Intel
Juniper
Mayo Clinic
Mitre
NIST
Oracle
Palo Alto Networks, Inc
PwC
Seagate Technology
```

Listing C.1: *List of organization*

Appendix D Interview Question

The interview questions in Section D.2, D.3, D.4, D.5, and D.6 has been constructed from the conceptual framework seen in Appendix A. While the other question has been constructed from the literature review to provide an introduction and conclusion to the interview. The italicized questions are probe questions and not meant to be seen by the interviewee, to achieve the semi-structured interview without missing any key points from the conceptual framework.

D.1 Cyber Supply-Chain Security Definitions

1. How would you describe Cyber Supply-Chain Security (CSCS)?
2. What difference do you perceive between information security, Cyber Security (CyberSec), Information Technology (IT) security, and CSCS?
3. How have you been involved in CSCS?

D.2 Communication

1. What communication challenges do you see in CSCS management?
   (a) *What about governance? i.e., standards, law, and relegation.*
      i. *Any particular noteworthy ones you need to follow here in Sweden?*
   (b) *What about Supply-Chain Security (SCS) requirements and responsibilities?*
   (c) *What about communication issues like:*
      i. *Miscommunication and misunderstanding?*
      ii. *Cost of CSCS practices?*
      iii. *Subject difficulty?*
   (d) *What about the reputation of the vendor?*

D.3 Multiple Vendors

1. What challenges do you see in CSCS due to multiple vendors?
   (a) *What about the size of the vendor? Do you see any particular challenges there?*
   (b) *What about the number of vendors in the Supply-Chain (SC)?*
   (c) *What about the geographical area of the Cyber Supply-Chain (CSC)? large or small does this pose different challenges?*
   (d) *What about visibility up and down the CSC?*
2. How would you describe the CSCS when working with multiple vendors? And what is the motivation behind this description?
   I. as secure as the least secure vendor
   II. as secure as the mean/median secure vendor
   III. as secure as the most secure vendor
   IV. all vendors are as secure as themselves
3. *Is CSCS futile when working with multiple vendors?*

D.4 Life Cycle

1. What challenges do you see in the life cycle of CSCS? That can be a product, service, or relationship with another vendor.
   (a) *What steps do you see in this life cycle?*
   (b) *What about continued improvement in CSCS is that a challenge?*

D.5 Points of Penetration

1. Which attack vectors/planes do you see in CSCS?
   (a) *What about the human vector as a CSCS challenge? i.e., insider threats, human error, social engineering.*
   (b) *What about the technical vector as a CSCS challenge? i.e., direct and indirect attacks, information security attacks, CyberSec, breakdown.*
   (c) *What about the physical vector as a CSCS challenge? i.e., direct and indirect attacks, tampering with hardware, break in, theft of materials, breakdown, physical threats.*
   (d) *Can you give some examples of CSCS attacks which uses each of these three (human, technical, physical) attack vectors? (preferable one of each)*

D.6 Cyber Security Objectives

1. What CyberSec objectives like Confidentiality, Integrity, and Availability (CIA) do you see as challenges in CSCS? Or is it just these three?
   (a) *What about authenticity?*
   (b) *What about possession?*
   (c) *What about utility?*
   (d) *What about trustworthiness?*
2. *What CSCS objectives do you believe is liked with trustworthiness?*
   (a) *Would you describe availability as part of trustworthiness?*
   (b) *Would you describe reliability as part of trustworthiness?*
   (c) *Would you describe resilience as part of trustworthiness?*
   (d) *Would you describe safety as part of trustworthiness?*
   (e) *Would you describe security as part of trustworthiness?*
3. *Are there any other CyberSec objectives not mentioned that are a CSCS challenge?*

D.7 Interviewee Reflections

1. Of all the challenges discussed, which challenges do you consider to be most important?
2. Are there any CSCS challenges that we have not discussed?
3. Would knowing these challenges help your organization when acquiring new CSC relationships or acquiring new products or services?

Appendix E Extended Conceptual Framework: Interorganizational CSCS Challenges

The interorganizational Cyber Supply-Chain Security (CSCS) challenges conceptual framework extended to reflect the interview's viewpoint on the CSCS challenges (see Figure E).

The changes are as follows; added traceability as a Cyber Security (CyberSec) objective; changed size of the vendor to include both small to large as they all have different challenges.

The order and placement of the categories, nodes, and subnodes are not representing anything specific, however, the lines show the relations between the categories, nodes, and subnodes.

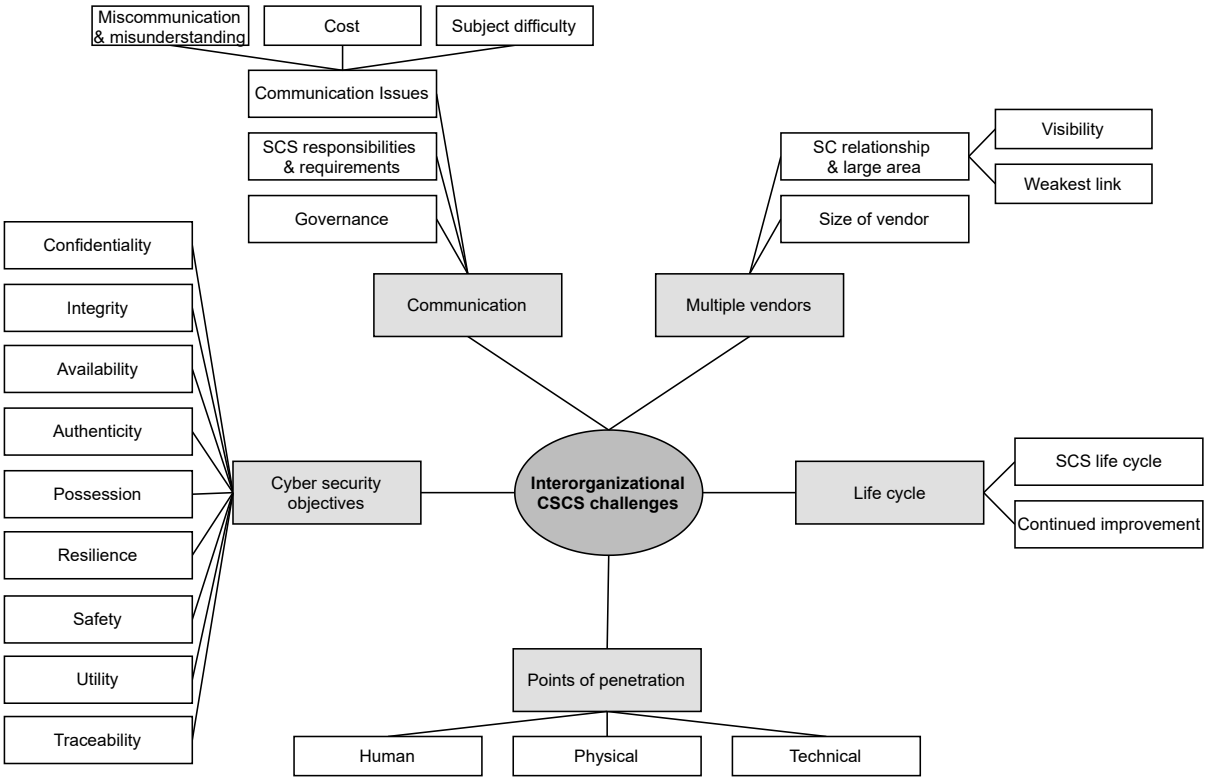

Figure E.1: *Extended detailed conceptual framework*