UNIVERSITY OF TURKU
Turku School of Economics

Breaking the Chain of Trust

Implementing zero trust into cyber supply chain environments

Information Systems Science

Master's thesis

Author:

Kristian Robertsson

Supervisor:

Professor Jukka Heikkilä

19.5.2026

Turku

Student’s statement regarding the use of Artificial Intelligence (AI) for preparing and/or writing this thesis:
☒ I have used AI-based tools. Their use is documented in the Appendix. The AI tools were used in a way that complies with academic integrity guidelines.

The originality of this thesis has been checked in accordance with the University of Turku quality assurance system using the Turnitin Originality Check service.

Master's thesis

Subject: Information Systems Science
Author: Kristian Robertsson
Title: Breaking the Chain of Trust
Supervisor: Professor Jukka Heikkilä
Number of pages: 130 pages + appendices 4 pages
Date: 19.5.2026

Cyber supply chains have become a common avenue for cyberattacks to target global organisations. Different threat actors use varying attacks from low level phishing to sophisticated zero-day attacks to drive their motives ranging from criminal theft to corporate espionage or harming the critical infrastructure. Cyber supply chains' connected and complex nature makes them hard to control, thus making vulnerability management a difficult task. Furthermore, the consequences of successful attacks to cyber supply chains can cascade to multiple organisations and cause different damages to these supply chain partners. Traditional perimeter-based security models often fail to overcome the complex challenges of cyber supply chains, prompting interest in Zero trust, which is a potential approach to mitigate the risks coming from the cyber supply chain through continuous verification, strict least privilege access-policies, and proactive processes.

The purpose of this paper is to study how zero trust principles can improve cybersecurity in cyber supply chain environments. Thus, a literature review is conducted to identify key issues of cyber supply chains and how the characteristics of zero trust in theory could solve them. These results are then verified through the empirical study finding out what zero trust controls have been implemented across Finnish organisations.

This study takes a socio-technical approach using a people, process, and architecture framework to gain a holistic picture of how organisations approach mitigating the risks coming from cyber supply chains. The large size of cyber supply chains and their complex nature that is caused by the amount and heterogeneity of machine and human components in the cyber supply chain calls for a holistic solution, thus making the socio-technical approach suitable for this study.

In this paper a qualitative multiple-case study was used to study Finnish organisations across different sectors and sizes. The empirical data was gathered through semi-structured interviews with the people responsible for cybersecurity. The results were analysed using the Eisenhardt method through building case profiles of the organisations, dividing them into groups based on their size and zero trust maturity, and conducting within group and cross-group comparisons. These results show empirical evidence on how zero trust controls are implemented across Finnish organisations.

This study found that in the threat landscape surrounding cyber supply chains, phishing was the most critical threat due to their volume, but also more sophisticated attacks like malware were mentioned, thus being consistent with the existing literature. To mitigate the risks of cyberattacks to the cyber supply chains, the literature presents multiple foundational zero trust controls such as MFA, micro-segmentation, and background checks, which are suitable for protecting such large and complex environments. The empiric results of this study show that Finnish organisations have implemented zero trust controls to secure their cyber supply chains against threats, although the variance between organisations was high. The controls were found to be implemented in all three domains, thus showing that the implementation was not merely composed of technical controls. The results also showed that controls from the people domain were implemented more in low and medium maturity organisations, suggesting that those might be easier or cheaper compared to process or architecture controls. This study shows that zero trust is a viable solution for mitigating the cyber supply chain threats, and that elements of zero trust have been implemented by real life organisations. To contribute to the existing literature, this study provides empirical evidence of zero trust implementations in cyber supply chain environments.

Key words: Zero trust, cybersecurity, cyber supply chain, socio-technical approach, Eisenhardt method cybersecurity management, maturity model, information security, supply chain risk management.

Table of Contents

1 Introduction 7

1.1 Background 7

1.2 Research questions 9

2 Risks of cyber supply chains and cyber supply chain risk management 11

2.1 Complexity and vulnerabilities of Cyber Supply Chains 12

2.1.1 Complexity 12

2.1.2 Cybersecurity challenges of cyber supply chains 14

2.2 Threats to cyber supply chains 17

2.3 Vulnerabilities in cyber supply chains 20

2.4 Risks for cyber supply chain 22

2.5 Consequences of cyberattacks to the Cyber Supply Chain 25

3 Zero trust 29

3.1 Tenets of zero trust 33

3.2 Zero trust architecture approaches 36

3.3 Deployment models 37

3.4 Implementation and evaluation of zero trust in cyber supply chains 39

4 Methodology 44

4.1 Data collection and research data 44

4.2 Case profiles 50

4.2.1 Case organisation 1 50

4.2.2 Case organisation 2 51

4.2.3 Case organisation 3 53

4.2.4 Case organisation 4 55

4.2.5 Case organisation 5 58

4.2.6 Case organisation 6 60

4.2.7 Case organisation 7 62

4.2.8 Case organisation 8 65

4.2.9 Case organisation 9 67

4.3 Analysis criteria 70

4.4 Cross-case analysis 72

5 Findings 74

5.1 Within group comparison 74

5.1.1 Small size organisations with low maturity 1,5, 7 74

5.1.2 High maturity large organisations (Case organisations 3, 4 and 9) 82

5.2 Cross-group comparison 91

5.2.1 Small organisations with high or medium zero trust maturity compared to those with low maturity 91

5.2.2 Large organisations with high zero trust maturity compared to large organisations with medium maturity 97

5.2.3 Large organisations compared to small organisations 106

6 Discussion 113

6.1 Answers to research questions 113

6.1.1 RQ1A: What are the largest cybersecurity risks for cyber supply chains? 113

6.1.2 RQ1B: How can zero trust be implemented in cyber supply chains? 115

6.1.3 RQ1: What zero trust elements have organisations implemented to mitigate risks of cyberattacks to their cyber supply chain? 116

6.2 Theoretical contributions 119

6.3 Recommendations to organisations 120

6.4 Limitations 122

6.5 Recommendations for future research 123

References 124

Appendices 131

Appendix 1 Data Management Plan 131

Appendix 2 Declaration on the Use of Generative Artificial Intelligence 134

LIST OF FIGURES

Figure 1 Bridewell. (2024). What do you identify as the most significant cyberthreats to your operations in 2024? Statista. Statista Inc. Accessed: October 21, 2024. https://www.statista.com/statistics/1468480/moist-significant-cyberthreats-to-cni-operations-uk/ 8

Figure 2 Amount of supply chain cyberattacks in USA from 2017 to 2023. (Identity Theft Resource Center. (2024). Annual number of entities impacted in supply chain cyberattacks in the United States from 2017 to 2023. Statista. Statista Inc. Accessed: October 21, 2024. https://www.statista.com/statistics/1367208/us-annual-number-of-entities-impacted-supply-chain-attacks/) 9

Figure 3 Complexity of IT-architectures following (Widjaja & Gregory, 2020) 13

Figure 4 Cost-benefit curve of investments into zero trust following Collier & Sarkis (2021) 41

Figure 5 Domains of the study 46

Figure 6 Organisation size compared to ZT maturity 107

Figure 7 Largest threats to supply chains compared to observed zero trust maturity 116

LIST OF TABLES

Table 1 Threats to cyber supply chains 20

Table 2 Vulnerabilities in cyber supply chains 22

Table 3 Risks for Cyber supply chains 25

Table 4 Consequences of cyberattacks 28

Table 5 Study questionnaire and motives behind it 47

Table 6 Interviewed employees 49

Table 7 Interviewed companies 49

Table 8 Coding for analysis 71

Table 9 Zero trust maturities across case organisations 73

Table 10 Classification of case organisations 73

Table 11 Largest threats to supply chains perceived by interviewees 114

1 Introduction

Cybercrime has significantly increased in recent years, due to the rapid development of new technologies implemented across many sectors (Kuzior et al., 2024). Digitalisation, on the other hand, has pushed supply chains to use modern technologies, such as Internet of Things (IoT), which have made them more complex to manage due to the increasing number of human and technological components, as well as their wider geographical area (Y. Wang & Pettit, 2022). Information systems can be defined as "*socio-technical systems that include human and machine components (system segments) that are interdependent, interrelated, and/or interact with each other*." (König, 1994). Information systems in supply chains also consist predominantly of machine components, many of which can be IoT devices. This affects the size and complexity of these systems, which in term increases their attack surface. Together with the rising number of cyberattacks, the large attack surface and complex nature of the systems can be a hazardous combination. Supply chain attacks have been estimated to become the most common type of cyberattacks by 2030 (Ghanbari et al., 2024). Zero trust, on the other hand, is a holistic approach into cybersecurity and thus presents a potential solution for securing supply chains.

1.1 Background

The Finnish Emergency Supply Agency (Fin. Huoltovarmuuskeskus) published a report about the cybersecurity maturity across Finnish sectors. In the report they highlight that in highly connected environments, such as supply chains, organisations' high cybersecurity maturity is not sufficient to protect them from attacks. Even if an organisation would be protected itself, attackers can breach systems, data, or software through partners or suppliers. On the other hand, being a part of supply chains can subject organisations to attacks, because even if they wouldn't be the ultimate target themselves, just being a part of the supply chain increases the risk of cyberattacks. (Huoltovarmuuskeskus, 2026). This is why cyberattacks originating from cyber supply chains have become increasingly dangerous due to the high interconnectedness between organisations. Figure 1 shows the results of a study by Bridewell from 2024. Of the surveyed heads of IT or IT managers of critical national infrastructure companies in Brittain, 26 % identified supply chain attacks to be their most significant cyber threat, representing a rise of three percentage points from the 2023. It was ranked third after cloud storage attacks and remote working vulnerabilities as shown in the diagram. (Bridewell, 2024).

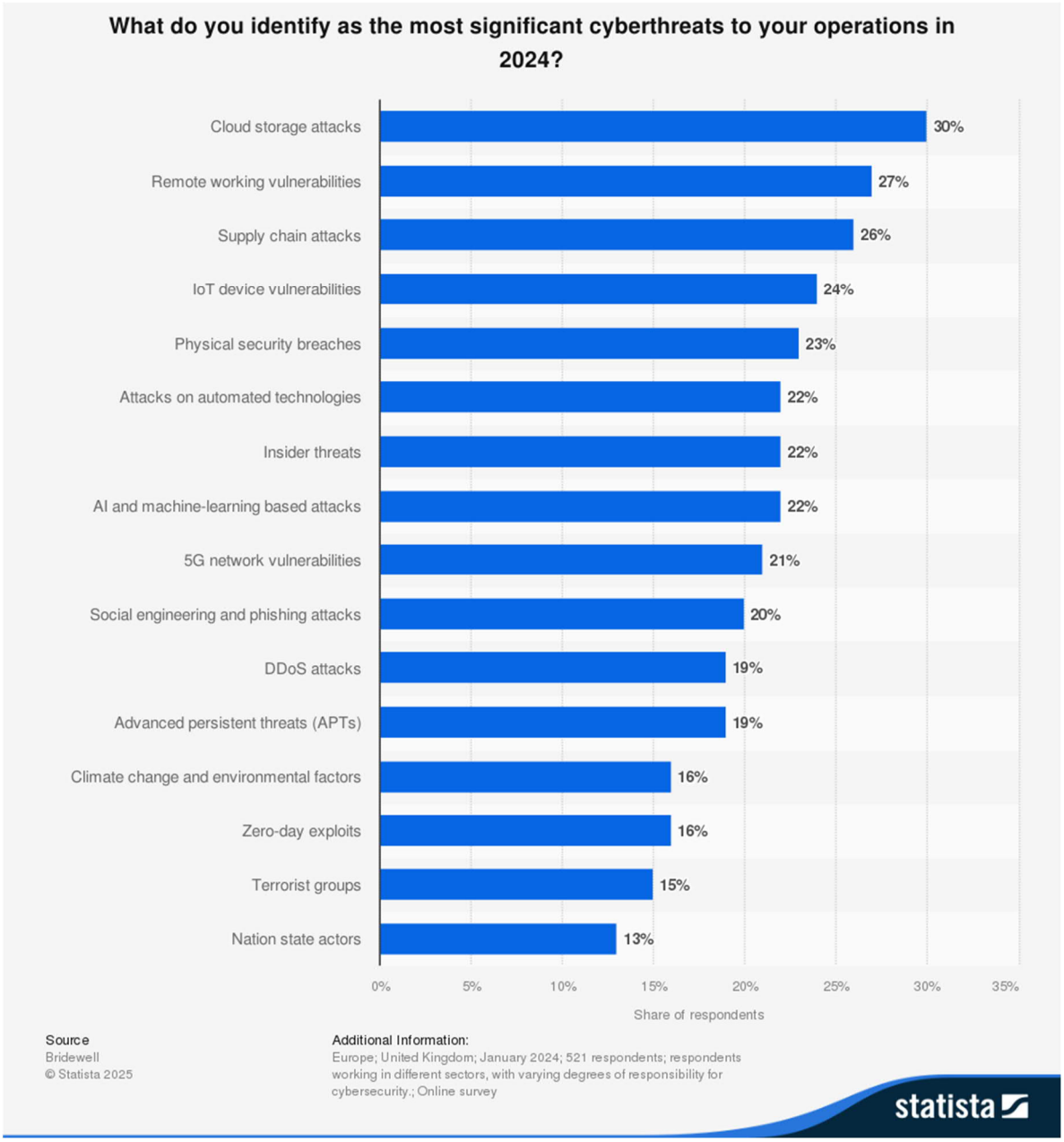

Figure 1 Bridewell. (2024). What do you identify as the most significant cyberthreats to your operations in 2024? Statista. Statista Inc. Accessed: October 21, 2024. https://www.statista.com/statistics/1468480/moist-significant-cyberthreats-to-cni-operations-uk/

Results of the Identity Theft Resource Center (ITRC) report, referred to in Figure 2, show that the number of entities affected by supply chain cyberattacks in 2023 in the United States, was 2769, compared to just 119 in 2017. The report also notes that rising supply chain attacks were a clear trend in 2023. (Identity Theft Resource Center, 2024).

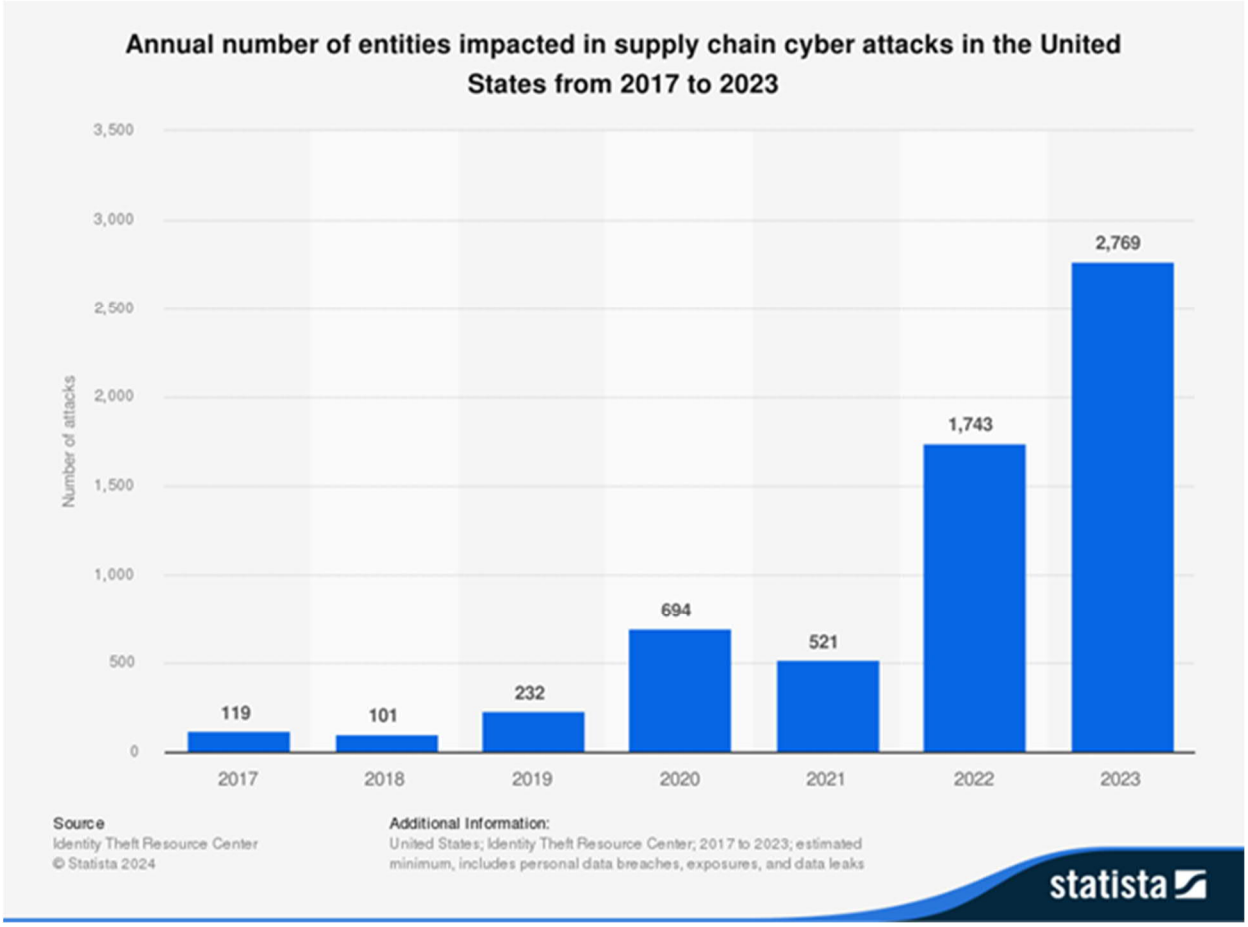

Figure 2 Amount of supply chain cyberattacks in USA from 2017 to 2023. (Identity Theft Resource Center. (2024). Annual number of entities impacted in supply chain cyberattacks in the United States from 2017 to 2023. Statista. Statista Inc. Accessed: October 21, 2024. https://www.statista.com/statistics/1367208/us-annual-number-of-entities-impacted-supply-chain-attacks/)

The European Union Agency for Cybersecurity (ENISA) also identified supply chain attacks as one of the prime cybersecurity threats in their 2024 threat landscape report. The report states that compromises in supply chains through social engineering are an emerging threat. (ENISA, 2024). This demonstrates how the expansion of supply chain systems has increased the attack surface of companies and. consequently, made supply chain cybersecurity more important than before.

1.2 Research questions

The goal of this thesis is to study how zero trust can be used to mitigate cybersecurity threats and challenges of cyber supply chains. First, to understand these threats of cyber supply chains and theoretical possibilities of zero trust, two supporting research questions are posed, which draw knowledge from the existing literature and enable reflection on the results from the main research question.

RQ1A: What are the largest cybersecurity risks for cyber supply chains?

To answer the first support research question about the risks for the cyber supply chains, a literature review is conducted to identify vulnerabilities in cyber supply chains, possible threats and their motives, and the consequences of those attacks to determine what the key risks are. To complement the literature review, background questions regarding largest perceived threats and any realized cyberattacks are included in the interviews, providing empirical verification.

RQ1B: How can zero trust be implemented in cyber supply chains?

The second support research question is answered through the conducted literature review, in which the chapter three about zero trust and its implementation is combined with risks identified in the chapter on cyber supply chains.

Finally, the main research question *RQ1 is: What zero trust elements have organisations implemented to mitigate risks of cyberattacks from the cyber supply chain?*

The main research question is answered by analysing empirical data from interviews and comparing it to the information derived from the literature review. Since zero trust isn't a binary property or a single technology, but rather a way of approaching security, the term "*element*" is used in the questions. The aim is to evaluate the solutions implemented across different domains of socio-technical cyber supply chains to determine whether they align with zero trust principles, regardless of whether the implementation was intentional or not by the organisations. Overall, the aim of this study is to understand the risks posed by cyber supply chains and how can zero trust be used to mitigate them. Therefore, the supporting research questions are answered primarily based on a literature review, while the main research question is answered through the empirical study.

2 Risks of cyber supply chains and cyber supply chain risk management

In this chapter the security of cyber supply chains is discussed. First, the nature of cyber supply chains is examined, followed by a dive to the possible threats to supply chains, the risks the attacks pose, and potential consequences of realised risks. The aim of this chapter is to study the actors behind attacks to cyber supply chains, their motives, and why supply chains are their targets.

Cyber supply chain (CSC) refers to supply chains that are used to acquire cyber-based products from numerous global suppliers of hardware, firmware, software, and services. This means that it encompasses the term software supply chain. (Windelberg, 2016). Software supply chain (SSC) refers to the acquisition of software products, which are then used directly or integrated into larger systems, effectively creating super systems. These systems are then used to build cyber supply chains that inherit many similarities, including risks, from traditional supply chains. These risks include for example, late product delivery, human error, or counterfeiting problems. However, SSCs also contain risks of their own, such as faulty code, which can lead to intentional or unintentional vulnerabilities. These vulnerabilities can include zero days, referring to vulnerabilities that are not known until they are exploited. (Sabbagh & Kowalski, 2015) Thus, SSCs can be considered to be encompassed by CSCs because CSC includes not only software parts, but also hardware, firmware, and services. This also means that the risks originating from the SSCs are inherited by the CSCs (Windelberg, 2016).

Cyber supply chains increase the efficiency of traditional supply chains by connecting external actors, or nodes, into connected networks (Charles C. Poirier, 2002; Yeboah-Ofori et al., 2019). This improved performance of the supply chain also brings challenges, such as failure to audit third party vendors, the lack of security controls, or lack of cyber supply chain risk management (CSCRM) (Yeboah-Ofori & Islam, 2019). CSCRM can be defined to include the organisational strategy and pragmatic activities used to assess and mitigate risks in the end-to-end processes, which build the supply chain system, including the IT networks, hardware, and software. These processes include the design, development, production, integration, and deployment of the systems, making the risk management process holistic by including the whole supply chain and covering the processes from design to deployment (Boyson, 2014). This implies that CSCRM considers processes, people, and technology (Creazza et al., 2022). This means that CSCRM has a socio-technical approach integrated into it. The goal of CSCRM is to manage the risks within the cyber supply chain holistically in end-to-end fashion enabling dynamic control.

The ability to control risk in CSCRM is weakened by control exerted on it by supply chain participants. The suppliers and acquirers can have a different view of objectives of risk management, and they can vary in terms of their capabilities to control risk and defining standards. The other participants may also have different risk appetites or risk tolerances. This may lead to suppliers having an interest in making trade-offs that are detrimental to other supply chain participants. (Windelberg, 2016). Thus, managing risks in a CSC is challenging due to the number of participants in the CSC and varying levels of control that an organisation can exert over others. The CSC itself can be subjected to multiple different vulnerabilities that create risks that can be hard to mitigate.

2.1 Complexity and vulnerabilities of Cyber Supply Chains

2.1.1 Complexity

The terms complicated and complex are often used as synonyms but following complexity science they differ from each other. Complicated refers to "*systems that are made up of large number of interconnected components*." This is a necessary but not sufficient for a system to be distinguished as complex. To determine if a system is complex, the interactions between the interconnected components need to be studied. "*In a complicated system, interactions among the interconnected components are linear and well-structured."* whereas in complex systems "*the interactions are ad hoc and non-linear*." These interactions are difficult to comprehensively analyse, test, and understand. Thus, it is problematic to control system-level cybersecurity behaviours and outcomes in a complex system. (Tanriverdi et al., 2024). Widjaja and Gregory (2020) concur with the thoughts with this and go on to characterise IT-architecture complexity as a result if the number and heterogeneity of components and relations. This concurs with Tanriverdi et al. (2024), since the pure number of components or relations alone does not create a complex system, but the heterogeneity of the components and relations forms the complexity. The authors go on to add that also, dynamic nature through for example, rate of change, and modularity affect the complexity. Dynamic properties make the architecture more complex because the change in components creates uncertainty, which in terms drives up the complexity. Modularity on the other hand can lower complexity because it can drive down the heterogeneity of components and relations by standardisation. (Widjaja & Gregory, 2020). This model is visualised in figure 3, showing the different components that form complexity.

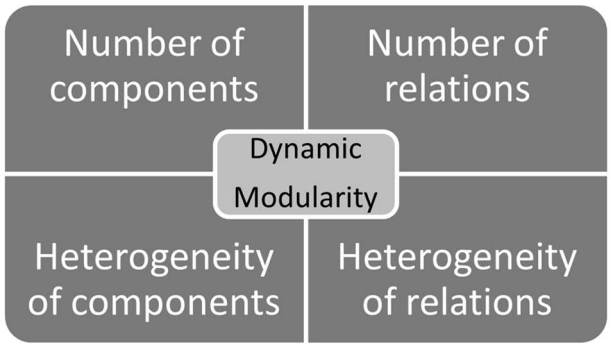

Figure 3 Complexity of IT-architectures following (Widjaja & Gregory, 2020)

CSC are often characterized as complex, because they tend to be super systems consisting of smaller sub systems, which are interrelated and interact with each other. These connections are often not well structured, which leads to the complexity. (Papastergiou & Polemi, 2018; Prathyusha et al., 2023). These sub systems are responsible for their own domains and have their own vulnerabilities and threats, which can be exploited any time. Thus, supply chain security can be hard to achieve. Many organisations also outsource parts of their CSC, which increases their vulnerability to many risks, like happened to the petrol manufacturer Saudi ARAMCOs power facility, which was completely stopped due to a cyberattack originating from the CSC. (Prathyusha et al., 2023). Complexity can be seen as detrimental to security because as Schneier (2018) explains: *"More complexity means more people involved, more parts, more interactions, more mistakes in the design and development process, more of everything where hidden insecurities can be found"*. This leads to a large attack surface, which in turn means, that there are more possible vulnerabilities that need to be fixed. Complexity itself means that there are more software modules in the software bill of materials (S-BOM), which leads to more connections between them, and again more possibilities for vulnerabilities, which can be exploited by the attacker. Knowing that the attacker might only need one vulnerability to compromise the system, an increased attack surface creates a more challenging task to secure large and complex systems. (Schneier & Vance, 2025).

Organisational complexity affects security due to several reasons. These reasons can be, for example, problems of accountability regarding responsible persons, understanding relationships between different departments, and maintaining organisations critical assets. Organisational complexity often grows due to mergers and acquisitions (M&A). M&A increases the structural complexity of an organisation, which can increase the likelihood of a data breach, since the M&A process requires technical and organisational changes to the organisation and even the small

changes can have big implications to cybersecurity. The effect of M&A to the security is amplified by the heterogeneity of the organisations. The heterogeneity can exist due to business domain, size, and strategy. Also, the publicity of the merger has been shown to increase the likelihood of a data breach, due to more attention being paid to the merger. (Schneier & Vance, 2025). For example, if two mechanic shops merge, the complexity is smaller than if a mechanic shop and a retail shop merge. And if the merger is between public organisations, more attention is paid to the merger, increasing the risk of a data breach. Thus, in the M&A process, security aspects should be taken care of and thought of.

Software itself has become more complex over the years, in terms of raw code lines but also in terms of understandability. The latest developments in AI, have specially made software complex in ways that humans can no longer comprehend it. Still, cybersecurity itself might not be worse than before, moreover there has been large improvements in terms of cybersecurity. But since the software becomes even more complex it creates a situation called the “Red Queens race”, where even though there is improvements in cybersecurity, it is still losing against the attackers, because the advances of attackers drive advances in cybersecurity. (Schneier & Vance, 2025)

Complexity is an inherent characteristic of modern IT-systems and architectures, which arises from both, the number of components and, relations but, also from the heterogeneity and non-linearity of the relations. Complexity can have adverse consequences for cybersecurity because it is expanding the attack surface of the IT-systems. Thus, managing complexity in large organisations, and in processes, like M&A, is critical, in order to preserve the security of the IT-landscape.

2.1.2 Cybersecurity challenges of cyber supply chains

Managing and controlling risks in a cyber supply chain can be a challenging task for various reasons. The cyber supply chain is a global operation, thus the actors in the cyber supply chain have to consider factors like cultural differences, geopolitics, organisational issues, and different regulations, while managing risk. On top of these, they have to naturally manage a network that consists of actors with different IT systems, standards, technologies, and different business logics, which makes fitting the actors together complicated. (Urciuoli, 2015). These challenges can be split into the following areas: third party supplier, investing into security, software supply chain, and detecting attack in the supply chain.

Because organisations share software, applications, and networks with trusted supply chain partners, a large and complex system is created with a large attack surface. Thus, attackers might

overlook tier one suppliers and target smaller suppliers on tiers three and four when targeting large organisations. Also, it is problematic to define who are the “trusted” suppliers that are granted access to the system. Measuring trust in a supply chain is hard and complex because the large organisations typically are complicated, and the systems involve a large group of partners and products. Visibility to the supply chain is also a problem for many organisations due to the fact that it might be hard to get downstream supplier information from other suppliers. Time adds to this problem since events in the cyber world happen fast and information about the suppliers should be kept updated, but that can be very problematic in large supply chains. Also, price plays a role in securing the supply chain since customers rarely pay for the cybersecurity of products, but rather choose products based on other criteria, including price. Cybersecurity is not cheap and the motive to invest into it is mainly at the top organisation. Some suppliers might have different risk appetites and risk tolerances and thus not invest so much into security. (Kshetri & Voas, 2019). Evaluating the trustworthiness and security of suppliers can be hard due to multiple reasons. The suppliers have their own suppliers and those have their suppliers, making the supply chain large and complex, making the evaluation a very complex task that is very hard to do comprehensively. Secondly, the security space is not static, it is evolving constantly making the security evaluation expire quickly. Thus, the security audits or controls should be done very often to keep the security data up to date. (Kaur et al., 2024)

Investing into organisational cybersecurity is required but not sufficient to protect supply chains. Investment into the shared digital systems that organisations use to connect is also required. Since organisations are able to achieve more efficient and smart processes and achieve flexibility and competitive advantage utilizing industry 4.0 and 5.0 technologies, they are opening their critical IT infrastructure to their suppliers when aiming to integrate their suppliers and partners to their systems. Opening the system in this way subjects the supply chain to attacks that can affect it directly or indirectly. The incentive of these partners to invest into cybersecurity also varies, and it can be described in a game theoretic situation. Since the suppliers can choose to cooperate or to compete meaning that they can choose to optimise their profits by not investing in security and hoping that they will not lose because of it. Suppliers can also choose to cooperate and then invest in security because they can see it as a profitable choice. In the shared digital system attacks can easily go unnoticed for weeks in these systems since monitoring the activity in them can be problematic without the proper security safeguards. To relieve this risk the controlling all organisations in the supply chain are required to invest in the suppliers security and thus develop their security safeguards. (Kaur et al., 2024). When investing to cybersecurity the budget is always

a limiting factor, thus optimisation of the cybersecurity investment needs to be done in order to do effective investments into the overall security of the supply chain. This objective of this optimisation can be defined to be: “determine a portfolio of security controls for implementation at different supply chain nodes to mitigate the impact of cyber risks over the entire supply chain.” (Sawik, 2022). Thus, organisations should think who they partner with and how those partners can collaboratively invest into cybersecurity to secure the whole supply chain.

As stated earlier software supply chain refers to the acquisition of software products, which are then used directly or integrated into larger systems, effectively creating super systems (Windelberg, 2016). This means that software systems and products are often built in a way that, they rely on modules that are used in multiple use cases. These modules might come from different suppliers and sub suppliers and the modules function as sub systems in the overall information system. This means that updates in the modules can include malicious code, which will then move upwards in the software supply chain. An example of this is the SolarWinds attack in 2020 where an adversary gained access on SolarWinds Orion software building system and included undetected backdoors into the software update, which then many clients installed and were then compromised. There were 18 000 customer organisations effected including large Fortune 500 corporations and USA government agencies like the DoD. (X. Wang, 2021). A similar attack was made against the Finnish dairy producer Valio, where many employee records containing sensitive information were leaked. This attack originated from an account of their software vendor Vincit, where an employee used their compromised device to log in to Valio’s information system and the attackers were able to obtain the VPN credentials. (Kangas, 2024). These software modules form the software Bill-of-Materials (S-BoM), which can be complex to manage due to the fact that management is required to coordinate the organisation as a whole including all departments and divisions and possible international offices, which all need to be kept updated (Schneier & Vance, 2025).

Traditional safety technologies like firewalls or intrusion detection systems have been found not effective in blocking attacks into the software supply chain. Those technologies are good for protecting networks from external attacks but in the case of supply chain attacks, the attacks often come from inside. These attacks can be caused by malicious insiders or by compromised accounts in the supply chain. Because the attacks are already inside the network and exploit the trust of clients, traditional approaches to security of building walls through firewalls may not work. Thus, software supply systems are hard to secure due to their size, complexity, and heterogeneity of different parts. Because traditional solutions like firewalls are not suitable for efficiently securing the cyber supply chain needs alternative solutions. (X. Wang, 2021)

Since the attacks to supply chains often come from inside the supply chain, detecting supply chain attacks is hard, thus securing the cyber supply chain is not only about securing the system itself, but also the "development, production, authentication, distribution and updates of all underlying components of the critical system." This means that purely technical systems like firewalls are no longer enough, but a more comprehensive solution is needed to secure the supply chain. Traditional intrusion detection systems (IDS) detect attacks by their signatures or by patterns in their behaviour. This is not suited particularly well in supply chains, since there is multiple software components involved, and signatures are often application specific. Thus, knowing signatures of known attacks for every software component is difficult and signatures still likely won't detect zero day attacks. (X. Wang, 2021). Attacks that utilize the human component in the cyber supply chain, meaning the users, can also be hard to detect since there are many ways they can compromise or corrupt information. Detecting these kinds of malicious or radicalised insiders can be hard since they have access to a wide range of assets, both physical and digital in the cyber supply chain and the motives can vary from personal to outsider extorsion. (Urciuoli & Hintsa, 2017).

2.2 Threats to cyber supply chains

The threat actors include a plethora of different parties with different intentions and motivations. These threat actors include hacktivism, corporate espionage, nation-state actors, terrorists and criminals but also the nature. (Boyes, 2015). According to ENISA's threat landscape the general growing trends in threats are state-nexus actors, cybercrime actors and hacker-for-hire actors, private sector offensive actors (PSOA) and hacktivists (ENISA, 2024).

Hacktivists are not as well-resourced threats as others like nation-states or criminals, but they are persistent and heavily motivated by a cause. Their objectives are to cause disruptions to drive change in for example social or political landscapes. (ENISA, 2024). The persistent nature of hacktivists makes them a threat to organisations supply chains because the change a hacktivist wants to make is not even necessarily connected to the affected organisation but rather one of its suppliers, which then causes disruptions for the whole supply chain. Also, another way around, if a hacktivist aims to disrupt a certain organisation, they might weak points in the organisations supply chain and thus target its suppliers. The persistent nature of hacktivists can make them into advanced persistent threats (APT), which are long-term attacks that are sophisticated and aim to attack a pre-determined target. This makes them hard to detect and respond. (Mitchell, 2020).

Corporate espionage can be defined as: "stealing a trade secret or proprietary information or appropriating, taking, carrying away, or concealing, or by fraud, artifice, or deception obtaining, a

trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information" (The National Counterintelligence and Security Center (NCSC), 2018). It is a threat that concerns the organisations themselves but also their supply chain. The goal of corporate espionage is to gather information about the target and their assets. Corporate espionage often involves insider threats who function as the attack vector to the organisation. Their motivation can range from revenge to monetary gain, which makes them hard to predict and find. They can also be APTs, which in a supply chain context can cause extended harm, since detecting the insiders leaking information can be difficult. (Mitchell, 2020)

Nation-state actors and state-nexus actors are threat actors with varying ties to nations. They are often well funded and protected by the nation. Nation-state actors are often more closely tied to the nation than state-nexus actors, who are more independent but still under some influence from the nation. They are generally sophisticated threats that aim to steal information or money or create disruptions. The actors usually engage in long term attacks that include long investigations to their targets to find weak spots. This makes supply chains potential targets for them since they have the resources and time to find vulnerabilities in the cyber supply chains. Nation-state actors target other nations but also large organisations to cause disruptions, steal information or drive other motivations. (ENISA, 2024)

Cybercrime is usually committed by criminals or terrorists. Their primary motivation are monetary gains through stealing money, selling information, or extorting money from victims. They often use social engineering tactics like phishing to breach the targets. The attackers can for example try to steal passwords, which can then be used to access sensitive data and services. After gaining access to valuable information the criminals can steal it or encrypt it via a ransomware. This way they can disrupt the operation of the target organisation. (ENISA, 2024). For cyber supply chains cybercrime is a problem since any of the organisations in the supply chain can be targeted by the criminals and disruption in any level of the supply chain can cause disruptions in other levels. The criminals can also attain sensitive data from the suppliers, which can then cause monetary damage for the organisation. (Pandey et al., 2020).

Hacker-for-hire actors can be included under the cybercriminals since they are actors that offer cybercrime services to less criminal organisations. Examples of hacker-for-hire services are ransomware-as-a-service (RAAS) and bought D(D)oS attacks that organisations can use to disrupt operations of their competitors. Hacker-for-hire services lower the threshold for criminal acts since

it makes it easier for non-criminals to commit cybercrimes. Hacker-for-hire actors can also be used to carry out vulnerability intelligence, which then can be exploited. (ENISA, 2024)

Private sector offensive actors (PSOAs) are threats that sell cyberweapons like zero-day exploits to their customers, which can be nation states or private entities. They are a growing concern according to ENISA since they are capable of producing advanced weapons that can be used by a wide range of clients. (ENISA, 2024). These are a threat to cyber supply chains since the PSOAs can find vulnerabilities anywhere in the supply chain and then sell the vulnerability before the target knows it exists.

Natural forces also threat to cyber supply chains. Power outages, floods, fires, earthquakes can disrupt the cyber supply chain in many ways. They can affect both physical and cyber aspects since physical blockades can for example delay shipments and power outages can disrupt information systems if the servers are offline. (Boyes, 2015)

As seen in table 1, there are many actors threatening the cyber supply chain, with various motives and capabilities. The threat they pose to the CSC varies based on the target organisation and its supply chain. The wider the supply chain is, the more attack surface and possibilities for disruptions there are. The impacts of cyberattacks to the cyber supply chains are wide, which makes them tempting targets for attackers. Thus, organisations should pay attention to their supply chains and their security.

Table 1 Threats to cyber supply chains

Threat	Motivation	Capabilities	Impact
Hacktivists (Boyes, 2015; ENISA, 2024; Mitchell, 2020)	Political or social	Persistent and possibly sophisticated, APTs	Disruptions to supply chain, data leaks, indirect monetary losses
Corporate espionage (Mitchell, 2020; NCSC, 2018)	Monetary benefits, stealing trade secrets, disrupting operations	Malicious insiders, APTs, malware, social engineering	Losing trade secrets, indirect monetary losses
Nation-state actors (Boyes, 2015; ENISA, 2024)	Causing disruptions, stealing information or monetary gains	Vast resources, long term operations, nation protector	Data leaks, disruptions to supply chain, direct monetary losses (ransomware)
Cyber criminals (Boyes, 2015; ENISA, 2024; Pandey et al., 2020)	Monetary gains	Social engineering, malware	Disruptions to supply chains and monetary losses from ransomware, data leaks
Hacker-for-hire (ENISA, 2024)	Monetary gains, stealing data, corporate espionage, causing disruption	Malware and other cyberattacks, low barriers for cyberattacks	Disruptions to supply chain, data leaks, direct and indirect monetary losses
Private Sector Offensive Actors (ENISA, 2024)	Monetary gains from selling cyber weapons	Highly sophisticated malware for other attackers	Disruptions to supply chain, data leaks, monetary losses
Nature forces (Boyes, 2015)	-	Earthquakes, fires, floods, power outages	Disruptions to supply chain and indirect monetary losses

2.3 Vulnerabilities in cyber supply chains

Vulnerabilities in supply chains can exist due to accidental mistakes, or due to poor design or operation. The vulnerabilities can be divided into people, processes, physical and technical vulnerabilities. (Boyes, 2015). Human and organisational factors are often the cause of vulnerabilities in organisations (Pollini et al., 2022). For cyber threats social engineering and manipulation are a growing method over technical hacking because of its effectiveness. Cybersecurity is inherently a socio-technical system where human and machine components interact with each other. Secure systems usually act in rational and predictable fashion, which people don't. Thus, acts of humans in the system are hard to predict, which causes insecurity. Managing people, as vulnerable components of the system, is hard, because it requires continuous efforts to create capabilities in the people, but also motivation to use those capabilities. For example, it is not enough that the people in an organisation know that they shouldn't use weak passwords, but they need to be motivated to actually use complicated passwords. (McAlaney et al., 2018). Human element referring to the people interacting with the cyber supply chain systems can be the most vulnerable and weak link, which is why they are a prime target for cyberattacks. Thus,

it is one of the direst concerns in supply chain cybersecurity. (Durugbo & Al-Balushi, 2024). However, treating people as the weakest link is often party due to the systems being built up from technical backgrounds with a lack consideration for the human elements characteristics, needs, and motivation (Pollini et al., 2022). In a cyber supply chain environment, the human element can be expected to pose a large role in cybersecurity since there are more users on different levels of the supply chain with possibly limited awareness about the possible consequences of cyberattacks targeting them.

Processes can create vulnerabilities in many aspects of the cyber supply chain (Wong et al., 2022). Since the cyber supply chains are very complex and large systems, there are a huge number of processes in them and vulnerabilities can exist in them. (Yeboah-Ofori et al., 2021). Additionally since the systems and thus processes are interconnected with each other, vulnerabilities in one systems processes can cascade to other systems (Yeboah-Ofori & Opoku-Akyea, 2019). Organisations also have different policies regarding processes, which bring organisational factors into play. However, policies, or best practices, are not always followed due to human factors as said, but also because there might be alternative motives, like efficiency or cost saving, which lead to policies not being followed. This can make processes vulnerable, if for example encryption is not used in communication. Thus, processes must be understood in order for them to be made secure. (Pollini et al., 2022).

Cyber supply chains possess physical vulnerabilities in two main ways. Firstly, if the cyber supply chain is controlled through physical controls such as servers, sensors, and other physical technical equipment. If an attacker gains physical access to this equipment, they can harm them, steal information, or otherwise disrupt the function of the cyber supply chain. Also, physical resources like electricity can be affected by a range of threats, including forces of nature, risking the function of the cyber supply chain. (S. Paul et al., 2022). The second physical threats are related to tampering the supply chain through forgeries. Especially hardware supply chains can suffer from tampering since certain components might be replaced with lower quality ones or the parts may be forgeries to begin with causing risks further on in the supply chain. (Lambert et al., 2013).

Cyber supply chains are as vulnerable technically as any other system. Also, their vulnerability can be said to be as severe as their weakest components. Often these weak components are legacy systems or poorly configured systems. Outsourcing for example servers can also drastically impact the vulnerability of the cyber supply chain since then the organisation has a lack of control over the

servers, which can subject them to vulnerabilities overall. (Ghadge et al., 2019). As seen on table 2, supply chains' vulnerabilities can be divided into different categories, that result in different threats.

Table 2 Vulnerabilities in cyber supply chains

Vulnerability	Reason	Threat
Human factors (McAlaney et al., 2018; Pollini et al., 2022)	Unpredictability, easy target for attackers, mitigation through training	Social engineering, mistakes, malicious insiders
Organisational (Durugbo & Al-Balushi, 2024; Pollini et al., 2022)	Bad security culture, poorly built systems	Social engineering, poorly configured systems
Processes (Pollini et al., 2022; Wong et al., 2022; Yeboah-Ofori et al., 2021)	Huge number of processes, different policies in supply chains,	Hackers targeting vulnerabilities, zero day-vulnerabilities
Physical (S. Paul et al., 2022)	Physical controls of CSC, physical assets	Attackers targeting physical premises, or physical devices like sensors, forces of nature disrupting operations
Technical (Lambert et al., 2013)	Large number of technical systems with their own weaknesses, lack of control due to outsourcing	Attackers exploiting vulnerabilities, especially zero days

2.4 Risks for cyber supply chain

There are multiple risks that involve the cyber supply chain. They can be divided into physical threats, breakdown, indirect attacks, direct attacks and insider threats. (Ghadge et al., 2019).

Physical risks refer to vulnerabilities that pose a risk to the physical aspects of the cyber supply chain. These aspects are things like routers, servers, switches, and other ICT equipment but also other tangible assets like products in transport. Physical threats include the human component but also nature factors like tornados and floods. These are threats that can hurt the cyber supply chain physically, for example by theft, counterfeiting or by damaging the assets. (Ghadge et al., 2019). Theft and pilferage are threats that cause harm to the supply chain by losing assets that are for example in transit. This causes mainly monetary damage to the supply chain in the form of missing goods. Sabotage refers to intentional harming of assets, both tangible and intangible. Tangible assets can be infrastructure like ICT devices or other physical infrastructure like warehouses. Sabotage can also target intangible assets like data, which could be erased or corrupted. Natural disasters can harm the cyber supply chain by causing damage to infrastructure like warehouses and servers. These can cause the supply chain systems to be inoperative, which can cause delays and loss of data. Lastly, accidents can cause unintentional damage to tangible and intangible assets in

the cyber supply chain. For example, deleting data by accident or damaging a delivery vehicle can harm the operation of the supply chain. (Urciuoli & Hintsa, 2017)

Threats arising from systems breaking down is not an exotic risk factor, but it can't be overlooked since broken down websites, firewalls or other services can pose a serious security threat to the whole organisation (Ghadge et al., 2019). These errors or failures can be related to hardware or software. Hardware errors can be for example equipment failure and software errors can be for example bugs and unknown loopholes. (Huong Tran et al., 2016).

Indirect attacks are attacks that don't target the organisation actively, but rather in a passive way by inserting traps that compromise the targets. These traps can include malware like trojans, worms, or viruses but also from counterfeit products and spoofing attacks. The idea is to get the target to fall for the bait and thus gain access to systems or to sensitive information. Social engineering including phishing is an example of an indirect threat because the breach is done by attaining sensitive information by fooling the target. (Ghadge et al., 2019). In a cyber supply chain environment, the indirect attacks can also be propagated from other tiers of the cyber supply chain and thus target the organisation even though the breach itself was not in the organisation itself (Sawik, 2022). Specially electronics supply chains can suffer from counterfeit parts because electronic waste is often recycled and reused leading to the parts being not according to standards in technical or security aspects. These can for example allow side-channel attacks where information is leaked from the components themselves. (Lambert et al., 2013)

Direct attacks include malware and other types of hacking attacks, such as denial of service attacks and social engineering attacks (Ghadge et al., 2019). Due to the size of the cyber supply systems the attack surface on them is huge. Thus, it can be hard to protect them from malware. Malware threatens the supply chain in similar ways as it does to individual organisations, but in the cyber supply chain context the vulnerabilities can be harder to spot and patch. Cyber threat intelligence can be used to understand existing and future threats using internal, external, and human sources, but it cannot detect something that is invisible. These vulnerabilities can include loopholes and configuration flaws that could then be exploited by an attacker. (Yeboah-Ofori et al., 2021). Spoofing attacks refer to attacks where an attacker impersonates someone else and tries to social engineer their way into systems. These attacks often utilize emails that appear to be originating from internal employees but truly the attacker is behind them. (Ghadge et al., 2019) Manipulation and alteration attacks can be seen as direct attacks, and they refer to violating the integrity of data by making unauthorized changes to it and thus compromising it. These can include manipulation of

for example design specifications or alterations to code. These could allow the software or device to function differently and thus gain the attacker access to systems. (Yeboah-Ofori & Islam, 2019). The SolarWinds attack can be considered as a manipulation attack because the attackers were able to access the updating system and via that create an invisible backdoor, which they then used to execute the data breach.

A zero-day attack is "a cyberattack exploiting a vulnerability that has not been disclosed publicly." This means that there are only a few ways to protect systems from them. (Bilge & Dumitraş, 2012). Zero-day exploits can create larger vulnerabilities to cyber supply chains for a few reasons. Firstly, there is a possibility to create zero-day exploits through the software supply chain. The attackers who have infiltrated the software supply chain, can insert harmful code to otherwise legitimate software updates or libraries in a way that it compromises the rest of the cyber supply chain. These zero-days can cause a data breach to the system or cause other damage to the cyber supply chain. For example, with automated manufacturing, a breach into the controlling software can cause also physical damage, which can hinder the function of the whole cyber supply chain. Secondly, zero-day exploits pose a threat because of the pure size of cyber supply chains. More lines of code mean more possibilities for vulnerabilities that won't be found until they are exploited. (Khandewal & Mahato, 2024).

Insider threats are threats that come from inside the organisation. Insider threats can pose as one of the direst and most unpredictable threat to the organisation. (Ghadge et al., 2019). They can be accidental or deliberate actions that lead to harm for the organisation. Accidental risks involve users using systems wrong due to lack of knowledge or by accident. For example, using easy passwords or leaving confidential information accessible are ways that people in the cyber supply chain might compromise the information security accidentally. Mitigating insider threats can be challenging due to background checks providing only limited information about past, but not recognising that people and their opinions change, thus possibly making them threats in the future. This can create a false feeling of safety. (Urciuoli & Hintsa, 2017). Deliberate insider threats can be linked to corporate espionage, criminality or even just pettiness. It is how ever important to distinguish deliberate insider threats from carelessness since tackling the two threats varies immensely. Accidents and carelessness can be mitigated through employee training and awareness unlike deliberate insider threats. (Ghadge et al., 2019).

Table 3 Risks for Cyber supply chains

Risk	Target	Who	Examples
Physical threat (Ghadge et al., 2019; Urciuoli & Hintsa, 2017)	Physical aspects of the CSC, including resources like electricity, physical assets	Forces of nature, criminals, terrorists	Forces of nature destroying facilities, attacker breaking into cargo
Breakdown (Ghadge et al., 2019; Huong Tran et al., 2016)	Hardware and software components	-	Broken server, firewall, website, application
Indirect attack (Ghadge et al., 2019; Lambert et al., 2013; Sawik, 2022)	Passive threats like traps for organisation and other actors in CSC	Cyber criminals	Malware, social engineering, counterfeit products
Direct attack (Ghadge et al., 2019; Yeboah-Ofori et al., 2021; Yeboah-Ofori & Islam, 2019)	Information assets, disruption, communication	Cyber criminals, nation states, terrorists, hacktivists, hacker-for-hire	Malware, (D)DoS, software backdoors, spoofing etc.
Zero-day attack (Khandewal & Mahato, 2024)	Information, software, hardware, physical aspects	Nation states, PSOA	Advantaged malware attacks
Insider threat (Ghadge et al., 2019; Urciuoli & Hintsa, 2017)	Confidential information, credentials, data	Corporate espionage, criminals, insiders	Corporate espionage, accidents, misconfigurations

As seen on table 3, there are many threats facing the cyber supply chains and those threats have different consequences on the operation of the cyber supply chain creating risks. Their mitigation also requires different actions depending on the source of the threat.

2.5 Consequences of cyberattacks to the Cyber Supply Chain

The effects of cybersecurity incidents on cyber supply chain are diverse and range from disruptions to operations to adverse effects on national security and world economy. Attacks into the supply chain can negatively affect the product quality since the attack can affect the production itself or through counterfeit products. Industry 4.0 manufacturing often relays on sensors and other automation hardware and systems, which could be tampered with in a cyberattack. This can affect the production, even by completely halting it like happened with Stuxnet, but it can also lower the quality of products, which then can cause monetary harm. (Barron et al., 2016). Cyberattacks in the cyber supply chain can also cause components to be counterfeits due to fraud or physical tampering. This is a threat especially for electronics supply chains where some components are of a higher quality than others in terms of security and counterfeit products can hinder that security by for

example creating side channel emissions, which then can cause vulnerabilities. (Lambert et al., 2013).

Operations of cyber supply chains can suffer from cyberattacks since the attack can adversely affect for example delivery times, product quality, inventory levels but also in worst cases halt the operations completely for example due to ransomware attacks. These effects often also spread through the supply chain since other actors are dependent from each other. (Barron et al., 2016). A good example of a cyberattack that affected the operations of multiple cyber supply chains was NotPetya in 2017, when the shipping company Maersk was struck by a ransomware attack, which managed to encrypt the operation system of Maersk, which meant that they lost the information about their shipping cargo, which paralysed 17 of their 76 ports around the world. This also affected a huge amount of other supply chains that had supply chain goods in those ports. (Bateman, 2020). Downtime and outages in services have been estimated to be the second largest consequence in monetary terms of cyberattacks (Soikkeli et al., 2023).

Cyber supply chains are exposed to as many attacks as any other organisation, but their interconnected nature enlarges the impact of the cyberattacks due to cascading effects. Cascading effects refer to events that affect initially a singly organisation, but the effect then spreads to other organisations. Thus, the consequences of cyberattacks in cyber supply chains are more adverse than in just single organisations since they are prone to cascade. (Al-Ansari & Alsubait, 2022; Soikkeli et al., 2023; Yeboah-Ofori & Islam, 2019). The cascading effects are the result of the complexity and complicatedness of cyber supply chains, because the systems are interconnected in ways that are not linear causing possible vulnerabilities, which attacks can utilize to spread, because the complicatedness decreases visibility causing blind spots. (Tanriverdi et al., 2024). The cascading effects can be large and severe enough to affect not just organisations, but also global trade due to major disruptions in supply chains, like happened with the SolarWinds attack in 2020 (Osman & El-Gendy, 2024).

Monetary consequences are often the most reported consequence of cyberattacks and those damages can quickly rack up. The monetary damages to a single organisation can also be enormous and also affect the stock price. For Maersk the NotPetya direct monetary damages were estimated to be over $300 million and 7 % of their stock value disappeared. (Corbet & Gurdgiev, 2020). The indirect monetary damages caused by the attack cascading to other supply chains has been estimated to be in the billions of dollars (Ghanbari et al., 2024). Monetary consequences can also follow from legal actions.

Legal and contractual consequences can result from cyberattacks when an attack to one organisation causes damages to other organisations. These lawsuits, settlements and legal fees can result in significant damages. (Simon & Omar, 2020). Following the SolarWinds cyberattack the company agreed to pay a $26 million settlement in court, which demonstrates how large the sums in these lawsuits are (Sena, 2022). Cyberattacks can cause service level agreement (SLA) violations if systems or applications are not available due to for example (D)DoS attacks. These SLA violations can then cause monetary penalties for the organisation. (Soikkeli et al., 2023).

Modern countries, including their critical infrastructure, are more and more reliable of emerging technologies and digital services, which creates a new target for cyberattacks that can cause dire consequences for security. Critical infrastructure includes assets and systems, both physical and virtual, that are by nature such that disruptions in them are able to cause impacts on national, economic, or operational security, and harm public health and safety. (Lis & Mendel, 2019) These systems include elements that are dynamic, interactive, and non-linear, which makes them complex systems. Critical infrastructure spans over different fields including for example government and commercial facilities, communications, emergency services, defence industry, energy, and healthcare. Thus, critical infrastructure extends to a wide range of sectors in a society, which makes the consequences of attacks multifaceted. (Lehto, 2022). Together with the fact that nation-state sponsored actors are able to create advanced cyber weapons, that are able to affect such infrastructure and the criticality of those systems, the consequences of cyberattacks can be dire. (Lis & Mendel, 2019).

Data breaches usually follow from successful exploitations of vulnerabilities both in technical systems and in people. In a data breach the confidentiality of data is broken and there is unauthorized access to the data. This can lead to further legal consequences and loss of reputation. (Schlackl et al., 2022). Trade secrets include various information and other assets that companies use to create and maintain value. If that information is copied, deleted, or altered in a data breach, the ability for the company to create value can suffer. Thus, in corporate espionage the goal of the attackers is to attain such information, which can then lead to market advances. Traditionally the data breaches have been done through insider threats that have had access to confidential data, but later data breaches are done more often via cyberattacks. (Ettredge et al., 2018). Thus, data breaches are often the consequence of succeeded cyberattacks done by malicious insiders or external hackers motivated by corporate espionage and monetary gains.

Stakeholders, like customers, vendors, shareholders, or employees, usually place a certain level of trust to an organisation when they are willing to engage with it using its services or products. If the organisation is affected by a cyberattack, that results in a loss of data, disturbed services or other negative consequences, these stakeholders can decide to not engage with the organisation anymore or with a lower price, since the trust that they had placed on the organisation had been violated. This results in a loss of value to the organisation since it is no longer seen as a such trustworthy partner, and it might get less customers. It can also make the shares of the organisation less worthy leading to a loss in value of the organisation. (Kamiya et al., 2021).

All in all, the consequences from cyberattacks are multifaceted and their severity varies greatly from unavailable websites to dangers of national security and public safety. These consequences are the result of risks realising from vulnerabilities that have been abused by different threats. Table 4 summarizes all of these consequences, which vulnerabilities can lead to them, and who are the likely perpetrators likely to exploit the vulnerabilities.

Table 4 Consequences of cyberattacks

Consequence	Vulnerability	Threat
Compromised product quality (hardware) (Barron et al., 2016)	Counterfeit products, physical tampering	(Cyber)criminals
Compromised product quality (software) (Barron et al., 2016)	Software supply chain	Insider threats, cybercriminals, nation-states
Compromised operation of the cyber supply chain (Barron et al., 2016; Soikkeli et al., 2023)	Denial-of-service attacks, ransomware attacks, malware	Cybercriminals, hacktivists
Cascading effects (Al-Ansari & Alsubait, 2022; Osman & El-Gendy, 2024; Soikkeli et al., 2023; Tanriverdi et al., 2024)	Cyberattacks	All
Monetary losses (Ghanbari et al., 2024)	All	All
Legal and contractual consequences (Simon & Omar, 2020; Soikkeli et al., 2023)	Denial-of-service attacks, cyberattacks,	All
Compromised critical infrastructure (‘Cyber-Attacks Against Critical Infrastructure’, 2022; Lis & Mendel, 2019)	Advanced malware, cyber weapons	Nation-states, PSOA
Data breaches (Ettredge et al., 2018; Schlackl et al., 2022)	Malware, insider threats	Criminals, hacktivists, malicious insiders
Damaged reputation (Kamiya et al., 2021)	Denial-of-service attacks, malware, data breaches	All

3 Zero trust

This chapter presents zero trust literature from the perspective of supply chain security. It starts with the basic ideas and assumptions of zero trust. Then tenets of zero trust and zero trust architecture are explained, and finally deployment models and implementation of zero trust are discussed. The aim of this chapter is to introduce zero trust and to evaluate how it fits the supply chain context.

Jon Kindervag coined the term "Zero trust" in his series of articles stating that there should not be an idea of a secure network (Kindervag, 2010b). Zero trust can be defined as: *"a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised".* Zero trust architecture (ZTA) on the other hand refers to the organisation's architecture that utilises zero trust principles in designing the infrastructure and processes and can be defined to be *"an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies."* (Rose et al., 2020). Thus, zero trust isn't a single technology but a set of core principles that create a holistic approach to protect the data and network (Buck et al., 2021). This holistic approach means that networks are treated as a whole composed of human and machine actors as well as the surrounding environment including credentials, access management, operations, endpoints, hosting environments and the interconnecting infrastructure. (Rose et al., 2020). Thus, zero trust architecture as a model assumes threats to be both external and internal to a network. This means that the assumption is that the attackers are already in the network, making perimeter based security controls ineffective. (Do Amaral & Gondim, 2021). The goal of zero trust, is thus to improve information security, by preventing unauthorized access to data and services together with making the access control as granular as possible limiting possible lateral movements (Rose et al., 2020).

Zero trust aims to limit vulnerabilities by limiting the access of users by various methods and by robust authentication of users. It balances between security and user experience and efficiency, creating a challenge for effective zero trust implementations, hindered user experience. Depending on ZT implementation methods it shows to the end users differently. MFA is the most common visible element of ZT to the end users who are forced to authenticate themselves using multiple verification steps. These authentications and strict limitations can sacrifice the user experience but with AI and ML it can be possible to adapt more dynamic policies, that wouldn't hinder the user experience as much. (Subramani et al., 2025). Zero trust can also limit access to resources by placing dynamic restrictions on access. These can include just-in-time access where the user would

need to request access to a specific resource for a specific task. (Rose et al., 2020). This would show to the end users as a step where they need to request access to a resource in order to complete their tasks, thus possibly worsening user experience. However, here the user experience could be improved by using AI and machine learning (ML). (Subramani et al., 2025). Thus, zero trust can be seen by users as constantly authenticating using MFA, and as limited access to resources, to which they need to request specifically for a selected task. Thus, the users can experience zero trust as troublesome, since it takes more effort from them to do the same tasks. However, research about improving user experience with zero trust is lacking and should be researched more deeply to mitigate the negative side-effects of zero trust implementations.

The traditional Approach to secure networks has been to allow external access to resources by establishing encrypted connections to the internal network. Devices in the internal network are then considered safe and have access to resources (Chen et al., 2019). However, this approach to cybersecurity has many downsides or pitfalls, that zero trust aims to fix. The pitfalls are related to the fact that in the modern threat landscape it is hard to define what to trust, whether it was interfaces in hardware, users, or traffic. The traditional assumption, that security professionals always identify which interfaces are secure and which are not, has been shown to be false, leading to misconfigurations. Similarly, internal users cannot be trusted in today's environment since they can be malicious insiders, and thus threats to security. Lastly, because users in networks can't be trusted, the network packets can't either. The identities on network level are only collections of certain attributes, that can be true or false, real or forged. (Kindervag, 2010b). Thus, the traditional approach, where internal users and devices are trusted, poses security risks to the organisation. Because the borders of organisations becoming more fuzzier with suppliers, customers, and partners having access to the internal networks of organisations, the attack surface is ultimately increased. Thus, the traditional approach causes security risks. (Collier & Sarkis, 2021). Zero trust, due to its holistic nature, covers threats that are internal or external, and caused by human or machine components. Thus, zero trust can answer to many problems rising from the dynamic nature of networks and solve problems linked to the traditional model. (Buck et al., 2021).

However, zero trust implementations can face multiple challenges. To begin with, legacy systems or existing infrastructure are often built on implicit trust where access and authorisation are based on fixed attributes, thus conflicting with zero trust principles. (CISA, 2023). Changes to these systems may cause the applications to slow down and decrease the performance. (B. Paul & Rao, 2022). Additionally, the implementation projects are also often large in scale and complexity, requiring support from many stakeholders including top management, IT staff and process owners (B. Paul &

Rao, 2022). Since the changes affect the infrastructure and workflows of the organisation, the implementation can be costly, making support from these stakeholders paramount (CISA, 2023; B. Paul & Rao, 2022).

CISA has defined six assumptions for ZTA implementation in IT systems and networks. The assumptions guide how organisations should manage network connectivity in a zero trust architecture. The first assumption is that *"The entire enterprise private network is not considered an implicit trust zone".* This means that all assets should assume breach at all times. Thus, communication inside the network should be done in a secure manner with the thought that attackers could be in the network. (Rose et al., 2020). This also holds in a supply chain context as there should be no implicit trust zones within the supply chain (Collier & Sarkis, 2021).

The second assumption is that *"devices on the network may not be owned or configurable by the enterprise".* This indicates that there can be assets in the network that are for example from visitors or contracted services, thus not controlled by the organisation. Also, if an organisation has a bring-your-own-device (BYOD) policy, those devices are not managed by the organisation. (Rose et al., 2020). In a supply chain environment this indicates that critical infrastructure in a supply chain might not be owned by the organisation and that assets requesting access to resources can be internal and external (Collier & Sarkis, 2021). Thus, organisations implementing ZTA need to consider the fact that some services, infrastructure, and assets can't be directly controlled by the organisation since they don't own them. This means that organisations need to carefully manage the access it grants to resources.

The third assumption in zero trust architecture is that *"No resource is inherently trusted".* This means that every asset's security posture needs to be evaluated every time before granting access to organisations resources. The evaluation should be continual throughout the session meaning that it should not be one time evaluation. (Rose et al., 2020). This means that even if a device is managed by the organisation it needs to be evaluated before granting access and the whole time it has access to a resource. Credentials alone should never be enough to grant access to resources and therefore should require further evaluation. However, devices owned by the organisation may have artefacts that enable authentication, and thus provide a higher confidence compared to devices not owned by the organisation. (Rose et al., 2020). In the supply chain context this assumption implies that no actor in the supply chain should be inherently trusted, requiring a per-request authentication in order to access supply chain resources (Collier & Sarkis, 2021). Thus, in the supply chain all resources, whether internal or external, organisation owned or not, must be evaluated before granting access to

supply chain resources. Just because a device would be owned by the organisation, or because it is in the internal network, doesn't mean that it would be granted access.

The fourth assumption is that *"Not all enterprise resources are on enterprise-owned infrastructure"*. This refers to both remote organisation subjects and cloud services. This means that the resources need to use local networks for connections compared to organisations private network. (Rose et al., 2020). For supply chains this means that resources within the supply chain have to interact with non-organisation actors or systems (Collier & Sarkis, 2021). Since the supply chain resources have to interact with non-organisation actors and infrastructure, like cloud services, they need to be protected properly, through tight access control, virtual and physical, and encryptions for data in storage and in transit.

The fifth assumption states that *"Remote enterprise subjects and assets cannot fully trust their local network connection."* This means that remote subjects should assume that their local connection is hostile and thus, should assume all their traffic is being monitored or tampered with. . (Rose et al., 2020) Thus, all connections should be done with the most secure way, and all connection requests should be properly authenticated and authorised. For supply chain environments this indicates that users cannot trust their local transactions of materials, information or finances (Collier & Sarkis, 2021). Thus, those resources whether physical or digital, need to be authenticated and connections be done in the most secure way possible.

The sixth assumption states that *"Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture."* This means that when moving between organisation to non-organisation infrastructure, assets and workloads should maintain their security posture. These assets can be for example hybrid remote users moving from enterprise to non-enterprise networks and workloads that include data migration from on-premises data storage to cloud services. (Rose et al., 2020) In supply chain context this means that consistent security policies and postures need to be applied to all materials, information and finances flowing between actors in the supply chain, referring to constant authentication and authorisation of these flows in the supply chain. (Collier & Sarkis, 2021).

All these six assumptions guide how ZTA should be implemented into organisational networks and ultimately to supply chain networks. Assuming breach and requiring constant authentication and authorization from assets and workflows can secure these flows of information, physical goods, and finances between actors in the supply chain. It is also important to consider that the whole supply

chain network consists of also non-enterprise owned assets that can't be controlled, thus requiring the need for constant monitoring of all assets.

Zero trust is an approach that covers organisations as a whole including their supply chain and thus is a potential answer for this growing threat. Because of this research about utilizing zero trust in supply chains is needed.

Zero trust is not a single set of technologies; it is a mindset and a new approach to cybersecurity aiming to fix the flaws in the traditional approach. In the following chapters the tenets of ZT, different approaches to ZT and different deployment models are visited more in depth. The seven tenets that guide how security should be built in the absence of trust. The three approaches provide logical components that can be implemented to the infrastructure guided by different deployment models to achieve partial or full zero trust. While the supply chain environments create challenges to the implementation, some approaches and deployment models fit it better.

3.1 Tenets of zero trust

In this chapter zero trust methodologies and tenets are visited more thoroughly. The tenets of ZT are used to define what is included in ZT or ZTA (Rose et al., 2020). Thus, the tenets in a way define the scope of ZT and ZTA.

The first tenet is *"All data sources and computing services are considered resources"*. According to this, resources are seen comprehensively. The network might consist of various devices that include small-footprint devices such as IoT-devices, Software-as-a-service (SaaS)-systems, operational technology (OT) controllers, personally owned devices, and other functions. Thus, devices can be small or large, and even not owned by the organisation, and still they should be considered as resources. An organisation might also consider users' personal devices as resources if those devices have access to the organisation's resources. (Rose et al., 2020). In the supply chain environment, the same broad thinking should be applied to resources as all up- and downstream actors should be considered as part of the supply chain. Thus, regardless of the size or importance of a supplier they should be considered resources. (Collier & Sarkis, 2021). Thus, the data sources and services are seen from a broad perspective and all systems that have access to the organisation-owned resources should be considered while implementing ZT.

The second tenet of ZT is *"Secured communication"*. It guides that all communication should be secured regardless of network location, implying that communication inside the network should be done with same security as communication between internal and external networks. Thus, the

network location itself should not imply that trust would be granted automatically, just because a device is in the internal network. All communication should be done in a way that protects the confidentiality and integrity of information while in transfer. (Rose et al., 2020). For supply chains this means that all flows, information, material or financial, should be secured regardless of location in the supply chain. All flows can be seen as potential vulnerabilities and should thus be protected. (Collier & Sarkis, 2021)

"*Per-session access to resources*" is the third tenet of ZT. Following it, access resources should be evaluated per-session basis following the principle of least privilege. Thus, granted access should be just enough to complete the specific task, that the access was granted for, and only for that specific task. This implies a just-in-time access meaning that there is no standing access to resources, but access needs to be granted for specific tasks. This also means, that access to one resource does not mean, that they would have access to other resources. (Rose et al., 2020). This should also apply to supply chain resources like all other resources. Thus, all flows in the supply chain should be evaluated per-case basis and one approved flow should not mean approval for the following ones. (Collier & Sarkis, 2021).

Access control policy is a tool that organisations use to protect their resources by defining its resources, its users, and who of those members are allowed to access which resources. Traditionally access has been given based on user roles, granting users continuous access. Following the fourth ZT tenet "*dynamic access control policies*" access to resources should be controlled by a dynamic policy meaning that it changes through certain variable factors. These variable factors can include the observable state of the client identity, application or service and the requesting asset, but also behavioural and environmental factors. Observable state of client identity refers to the account asking for access and the device characteristics, such as OS versions, used to request the access whereas the behavioural factors can include comparing present behaviour to past behaviour. Environmental factors can include for example network locations or threat intelligence. The access control policy follows always least privilege principles to restrict both visibility of resources and access to them. (Rose et al., 2020). This should apply similarly to supply chain environments (Collier & Sarkis, 2021).

NIST describes the fifth tenet, "*Continuous monitoring of security"*, as enterprises' need to maintain situational awareness of all owned and associated assets by monitoring and measuring the integrity and security of the devise (Rose et al., 2020). An enterprise can implement this into their supply chain by ensuring the most secure state of all actors and infrastructure by monitoring the

security state to ensuring the assets remain in their most secure state (Collier & Sarkis, 2021). Gathering this information about threats and vulnerabilities of assets from internal and external sources, is referred as threat intelligence (TI). The aim of TI is to prevent and mitigate future threats by proactively finding them. (Syed et al., 2022). Vulnerability scanning is one method of doing threat intelligence and it entails scanning the network and comparing the scan results to a database of signatures of existing vulnerabilities (Holm et al., 2011). Thus, organisations should extend their TI, like vulnerability scans, to also associated infrastructure to maintain the most secure state possible throughout the supply chain.

The sixth tenet "*Strict and dynamic resource authentication and authorisation"* can be described as a "constant cycle of obtaining access, assessing threats, adapting and continually reevaluating trust". This can be achieved by continuously monitoring communications and demanding reauthentication and reauthorization in user transactions. These should be defined by a policy, which can include for example time-based, resource requested, resource modification, or anomalous subject activity. The goal of this is to achieve a balance between security and availability, usability and cost-efficiency. (Rose et al., 2020). In a supply chain context this means that authentication and authorization should be dynamic and strictly enforced before allowing access to supply chain flows or infrastructure (Collier & Sarkis, 2021), which could show to user for example as a need to reauthenticate after 30 minutes or when accessing new information.

The seventh tenet of zero trust, "*Collect all relevant security information"*, guides organisations to collect "as much information as possible about the current state of their assets, network infrastructure and communications" in order to better their security posture by using this data in policy creation and enforcement. This information can be gathered from wide sources like network traffic, access requests or assets security posture. (Rose et al., 2020). In a supply chain context this can be implemented as collecting as much information as possible about the current state of the entire supply chain, including actors, infrastructure, and communications. This information should then be used to improve the security posture of the supply chain. (Collier & Sarkis, 2021). Thus, all relevant log information should be collected from the supply chain environments and used improve policies to be more secure and efficient.

To summarise the tenets, organisations should classify all devices, regardless of their size, importance, or ownership, to be resources, meaning that they should be protected by tight access control policies that utilise dynamic policies, while only granting per-session access. This access should be continuously monitored and reauthentication and reauthorisation should be required when

needed. Communications to these resources should be done in the most secure way possible regardless of their location while collecting comprehensive log information from this network traffic as well as access requests and other device behaviour. Like communication the organisations should always monitor devices themselves to ensure their integrity and security posture at all times. Thus, no trust should be placed on any device or any communication.

3.2 Zero trust architecture approaches

ZTA can be implemented in three main approaches that differ with the main components and the main source of policy rules. These approaches use one or two tenets or zero trust as their policy drivers but implement all tenets in some way. The three approaches are ZTA using enhanced identity governance, ZTA using micro-segmentation and ZTA using network infrastructure and software defined perimeters. A full zero trust implementation consists of all three approaches that complement each other's and help counter flaws in each other. However, some of the approaches fit organisational structures and workflows better than others and thus, an organisation can start implementing ZTA with one approach and later implement also others. (Rose et al., 2020).

ZTA using enhanced identity governance following its name utilises identity actors as the core component in policy creation. Thus, the access control policies to are based on the identity and assigned attributes of the subject requesting access to a resource. In this approach the access to resources is thus based on the access privileges that have been granted to the subject trying to access those resources. Other factors can also be used to alter the final confidence level calculation that is used to whether a subject should be granted access to the resource. These other factors can include for example the device used, assets status, or environmental factors. Granting access can also be tailored based on these factors to for example grant only partial access. This approach works best with open network model or with organisations that have non-organisation managed devices accessing their networks, since network access is initially granted to all assets while access to resources is restricted to identities that have been granted access. This creates a problem since malicious actors can abuse the open network access to conduct network reconnaissance or launch DoS attacks creating a need for the organisation to monitor and control their networks. This approach works well with cloud-based services or with a resource portal model since organisations can utilise the identity of the asset requesting access to enforce the access control policy. Thus, organisations with open networks and with heterogeneous assets accessing resources using could services or resource portal models can implement enhanced identity governance to implement ZTA.

(Rose et al., 2020). This seems to fit supply chain environments well due to their complexity and size as well as the number of non-controlled devices accessing resources.

Micro-segmentation is the second approach to implement ZTA. Micro-segmentation can be implemented gateway- or host-based. Gateway based implementation means placing the individual, or groups of, resources on their own network segments that are protected by a security gateway. This can be achieved using infrastructure devices like intelligent switches, Next generation firewalls (NGFW), or special purpose gateway devices, which are able to enforce the access control policies. Host-based micro-segmentation can be implemented using host-based software agents or firewalls on the endpoint devices. These can grant access to resources dynamically based on the requests of the service, client, or asset. Thus, micro-segmentation can be implemented resource or client based. This is why micro-segmentation can be implemented in many use cases and deployment models. In order to work fully, micro-segmentation requires an identity governance program (IGP), while it still relies on the gateway devices to enforce the policies. To enable efficient micro-segmentation implementation the gateway devices, need to be able to react and reconfigure to counter threats or answer to changes in workflows. While this is possible to be achieved using simpler gateway devices, managing them would be difficult and costly hence the implementation would not work as intended. Thus, by implementing gateway devices or host based agents, organisations can protect their resources by separating them into network segments. (Rose et al., 2020). Micro-segmentation seems to also be a potential avenue for implementing ZT into supply chains using for example vendor specific segments.

The third approach for ZTA implementation is using network infrastructure and software defined parameters. In this approach zero trust is achieved using an overlay network where the requesting agent and the resource gateway establish a secured communication channel between the agent and resource. There the resource gateway acts as the policy enforcer (PE) deciding if agents have access or not. The policy administrator (PA) controls the network setting up and reconfiguring the network based on the decisions by the PE, creating the connections between agents and resources. This approach is also referred as software defined parameter (SDP) approach and often includes concepts from software defined networks (SDN) and intend-based networking (IBN). This approach thus protects the resources by allowing them to enforce access control policies. (Rose et al., 2020).

3.3 Deployment models

All three previous components or approaches to implement ZTA are logical components that might consist of several assets, or one asset that can perform many tasks. However, these components can

be deployed following four main models; device-agent/gateway based, enclave based, resource-portal-based or device application sandboxing. (Rose et al., 2020).

Device-Agent/Gateway-based deployment model utilises two parts, one at the device and one at the resource end. The agent software in the device directs traffic to the policy enforcement points (PEP) that evaluates the requests and grants or denies access. The resource end software is a gateway that is in front of the resource itself. Thus, the resource communicates only with the gateway that acts as a proxy for the resource. This gateway acts as a policy enforcement point and communicates with the policy administrator to allow only approved communication through to the resource. Once a request from an agent to a resource is approved, an encrypted communication channel is established that is used to flow data. The channel is closed once the workflow is completed or when triggered by a security event. This model works best for organisations with a robust device management and with separate resources that are able to communicate with the gateway. (Rose et al., 2020).

The enclave-based deployment model is a variant of the previous model, and it differs from it in the resource side. Where in the agent-gateway model the gateway was in front of the resource, in the enclave model there is a boundary around the entire resource where the gateway resides. This can be for various reasons but most commonly this is used with resources that only serve one business function or are not able to communicate with the gateway. This can be useful with resources like legacy applications or on-premises data centres that can’t communicate with the gateway because they for example are missing an API for the communication. When an asset is granted access to this enclave, they receive access to the whole resource, which is the downside of this model. Because the resources inside the enclave can’t be protected individually, the subject accessing the enclave might see resources they don’t have privileges to access. (Rose et al., 2020).

Resource portal-based deployment model differs from the earlier two with having only a single component as the PEP, which acts as a gateway portal between subjects and resources. This resource can be a single resource or an enclave entailing multiple resources. In this model the subject sends the PEP a request, which the gateway sends to the policy administrator, and if approved, creates the connection between the subject and the resource. The main benefit of this model is that it requires no installed software for the client devices, which makes it more flexible with BYOD or with interorganisational projects. The downside of this is that the organisation only has limited information about the subjects and their devices since they can only see or perform scans on them when they are connecting to the PEP portal. This also means that the organisation cannot monitor these assets continuously for example for malware or vulnerabilities. This model

also allows attackers to discover and attempt to access the portal and also is susceptible for DoS attacks. (Rose et al., 2020). Since this model doesn't require software to be installed on client devices, it fits better for supply chain environments since the organisation can't control these external devices, but it comes with its downsides that the organisation needs to consider and try to mitigate.

Device application sandboxing deployment model is also a variant of the client-gateway model, but in this model, there are trusted applications within the assets that communicate with PEP to request access to resources. While these specific applications are able to request access to resources from PEP, the PEP will block access from other applications. The benefit of this is that when the organisation is unable to scan the asset for malware or vulnerabilities, these individual sandboxed applications can be protected from the rest of the asset. The disadvantage of this is that the organisation must maintain these sandboxed applications with for assets while possibly having no visibility into the clients. Ensuring security of all sandboxed applications may be laborious and require more than monitoring making this method possibly costly. (Rose et al., 2020).

3.4 Implementation and evaluation of zero trust in cyber supply chains

Zero trust implementation has been researched in the supply chain context in a few studies. Collier & Sarkis (2021) brought up that zero trust could be a potential avenue for securing supply chains. They compared the differences between IT systems and supply chains when it comes to the effects of zero trust to them. In their comparison four domains were found. The resources that should be protected, the assets and users in the networks, the object that is secured and the perimeter of the protected network. Based on these differences they went on and analysed the tenets and assumptions of zero trust, and what those mean in the context of supply chains. The authors go on to theorize that the cost-benefit curve of investing into zero trust implementation is exponential, meaning that eventually marginal benefits are received from investments. In the same diagram they also present that zero trust has four stages. Perimeter-based, hybrid, near zero trust, and pure zero trust stages. This is important regarding implementation because it means that zero trust is not a binary characteristic, but a continuum, where zero trust can be implemented partly to the organisation and receive a better security posture as a result. (Collier & Sarkis, 2021)

Do Amaral and Gondim followed up on the recommendations made by Collier and Sarkis in their 2021 article by creating a roadmap for integrating zero trust into supply chains by introducing controls. Their model of integrating zero trust into supply chains has four steps. First, it is necessary to identify components of the cyber supply chain in question. This is done by creating a Software

Bill of Materials (SBOM), which is a breakdown documentation of all components that the cyber supply chain consists of. It details the different components and their relationships. SBOM can be used to identify vulnerabilities and help the organisation visualize their cyber supply chain. (Do Amaral & Gondim, 2021)

Second step includes assessing the adherence of individual components in SBOM to the zero trust principles defined in the NIST standard 800-207. These principles are assessed in different domains that are infrastructure and networks, identity, device, governance and data, application and finally DevSecOps and data science. The controls are divided into these domains and use three levels, basic, intermediate, and advanced, to assess the current state of each control. Generally, the basic level assesses if there is any zero trust compatible regulation regarding the risk category in question. The intermediate level evaluates how the practices are done regarding the zero trust architecture, and finally the advanced level assesses whether the mechanisms are updated dynamically in real time using automation. (Do Amaral & Gondim, 2021)

The third step is gap analysis. In the analysis the goal is to verify the current state of the organisation and develop a roadmap for improving its security. An example, of a such control would be access control, which is located in the infrastructure and networks domain. At the basic level, the control is: “is there an access policy considering cyber supply chain aspects”. In the intermediate level the controls are for example: “is access control performed in every session” and “is role segregation performed?” In the advanced level the control question would be for example, “is the access control based on a dynamically updated policy that allows real-time decisions?” In this step the stage of every software component can be evaluated. After all the components have been analysed, the results can be combined to form the global analysis, which shows the state of different domains. The final step in their model, is to design a roadmap based on the gap analysis for improving the security of the design. (Do Amaral & Gondim, 2021)

Maturity models often consist of series of levels that show a path that can be anticipated, desired or is logical from initial stage to desired stage. So, maturity levels indicate the present or desired capabilities regarding a specific area. Commonly maturity models are used to assess the current situations to find ways for improvement. (Becker et al., 2009; Pöppelbuß & Röglinger, 2010). Thus, maturity models are developed to help organisations measure and improve their conduct in a specific area. An example of such steps can be seen from figure 4 showing a zero trust maturity model. The model shows different stages of zero trust compared to the cost of the implementation and the achieved security levels. Here the steps illustrate that the stages are not equal in size and the

costs related to them are not linear but rather exponential. It also shows that zero trust is not binary, but rather a continuum between traditional perimeter-based approach and a pure zero trust implementation.

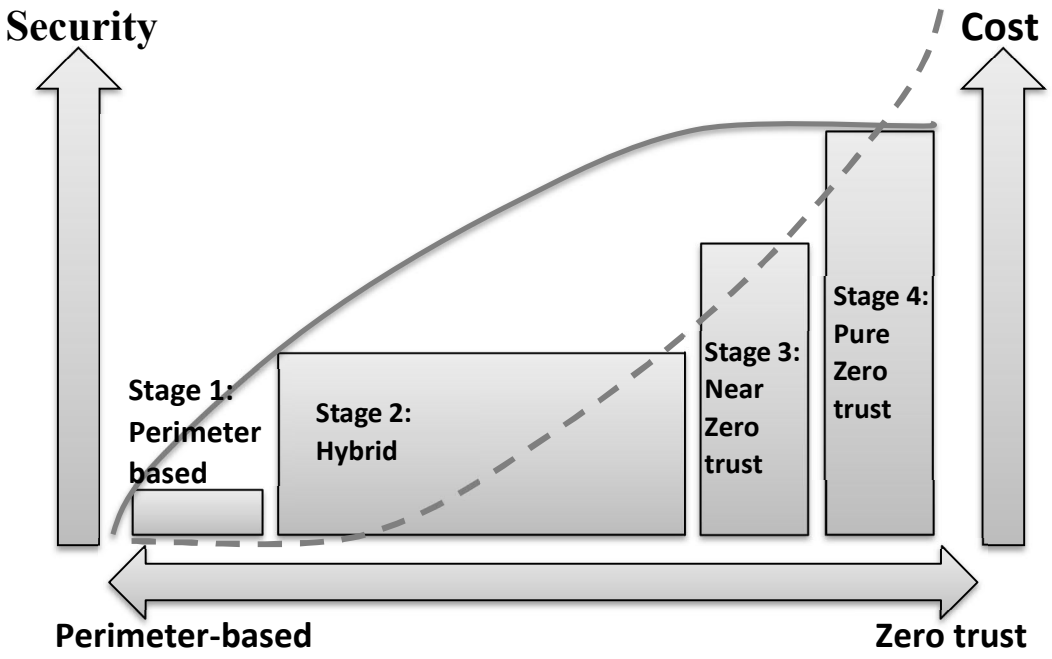

Figure 4 Cost-benefit curve of investments into zero trust following Collier & Sarkis (2021)

The level of implementation of zero trust in organisations can be evaluated using different maturity models. These models assess the level of maturity of zero trust in different domains. Different maturity models have different domains and those often reflect the area of which the maturity model is focused. (Tokerud et al., 2023).

The ZTMM model incorporates five domains: identity, devices, networks, applications & workloads, and data. Building on these domains the model distinguishes four stages of zero trust maturity: traditional, initial, advanced and optimal. (CISA, 2023).

Do Amaral and Gondim (2021) proposed a maturity model for zero trust implementation in cyber supply chain environments. They built their model on the domains adapted from Microsoft's Zero Trust Guidance Centre's and the ZTMM by CISA (2023). The domains they adapted are the following: *Infrastructure & networks* (D1), *Identity* (D2), *Device* (D3), *Governance & Data* (D4), *Application* (D5), and *DevSecOps & data science* (D6). This model takes into consideration also the human component by including it to several of the domains like identity (D2), which cover

identifying the users and Governance & Data (D4) incorporating policies and processes that guide how the organisation answers to cyberattacks.

The extended zero trust maturity model (EZTMM) created by Tokerud et al. 2023 distinguished three domains: technology, processes, and people. This emphasizes the human component on the socio-technical aspects of these systems. Under the domains the authors have identified multiple focus areas. Under technology domain there are network segmentation & infrastructure, dynamic access and threat protection. Under processes there are: identity & access management, change management, asset management, incident management, supply chain management, and data governance & protection. Under people there are employee awareness & training and infrastructure security culture. (Tokerud et al., 2023). Supply chain environments are directly connected to the EZTMM since they are mentioned under process domain. The model incorporates the socio-technical view, which many zero trust maturity models are lacking and since the human component is crucial in supply chain environments since the users are not only from the internal organisation but also external actors.

Cybersecurity Capability Maturity Model (C2M2) created by US Office of Cybersecurity, Energy Security, and Emergency Response in 2021 has ten domains and is broader by its nature since it is aiming to improve the overall security posture (Tokerud et al., 2023). The C2M2 model was designed for the energy sector, which can be labelled as critical infrastructure. Thus, the goal of the C2M2 model is to help critical infrastructure organisations manage their capabilities related to information technology (IT), operational technology (OT), and their operation environments. The C2M2 model has ten domains. Asset, change and configuration management (ASSET), threat and vulnerability Management (THREAT), risk management (RISK), identity and access management (ACCESS), situational awareness (SITUATION), event and incident response, continuity of operations (RESPONSE), third-party risk management (THIRD PARTIES), workforce management (WORKFORCE), cybersecurity architecture (ARCHTITECTURE), and cybersecurity program management (PROGRAM). (Cybersecurity Capability Maturity Model (C2M2), Version 2.0, 2021). The number of domains illustrates how broad the C2M2 model is compared to other models. Thus, it is a good model to refer when looking at supply chain environments since domains such as access, response, and third parties are relatable to supply chain environments due to their nature of connecting third parties to the organisation and their importance to the organisation’s operations.

Maturity models have been created to measure zero trust implementations and situations. Different models focus on different areas with models like ZTMM being focused more on the technical side whereas models like EZTMM approach zero trust more holistically including the human component. However, it is important to point out that different maturity models approach security differently. The ZTMM by CISA builds on these security control planes such as identity, devices, and networks while socio-technical maturity models like EZTMM by Tokerud et. al (2023) uses domains people, processes, and architecture, which are used to describe the organisational context and the interaction between human and technical components. Thus, there are overlapping in the maturity models but there are differences related to the scope and focus of the models.

4 Methodology

In this study qualitative methods are used in a multiple case study. A qualitative method was chosen over quantitative since it can provide more in depth understanding and give more comprehensive knowledge (Dunwoodie et al., 2023). Case study research is well suited to information systems research for a few reasons. Firstly, it allows the researcher to study the information system in a natural setting. This allows the researcher to learn about cutting-edge technologies and develop theories from practice. Secondly, the case study research method allows understanding the complexity and nature of processes taking place through “why” and “how” questions. Thirdly, case study research is well suited for research areas without much previous research. (Benbasat et al., 1987). Because this study focuses on an implementation of a novel technology and many studies about zero trust implementations in supply chain context have not been made, case study method is well suited for this research. Multiple case study is used to improve rigorousness and relevance to the world of practise (Stewart, 2012). This is important because the data from the interviews was expected to be heterogeneous. Thus, a multiple case study was chosen also because zero trust technology is a novel technology, and to study how a such novel technology has been implemented across Finnish organisations, one case would not have given sufficient empirical evidence.

Eisenhardt method is used to analyse the interview data. First within case analysis is conducted by describing cases to generate insights. This is done to allow patterns rise from the cases based on criteria derived from the scientific literature. Cases then characterised into groups. Then within group analysis is done to find similarities and cross-group comparisons are done to find differences between the groups. Thus, patterns are identified in the data to explain what characteristics affect the occurrence of zero trust elements in organisations. Eisenhardt method improves rigorousness through its iterative nature and allows novel theories to be found from comparing the cases. (Eisenhardt, 1989)

4.1 Data collection and research data

This empirical study was done with qualitative data. Qualitative method was chosen to better understand the methods companies use for securing their supply chains and whether those methods include zero trust principles. Data for the research is gathered using semi-structured interviews. Semi-structured interviews are suited for describing, explaining and interpreting phenomena, which enables more richer data and better understanding of organisational policies and governance (Dunwoodie et al., 2023). The aim was to interview company managers who hold responsibility for

cybersecurity in the company since they are most likely to know the details how their organisation manages cybersecurity in their supply chains. The companies selected for the interviews were selected either for their size or industry. to focus on organisations that had large supply chains.

The questions for the semi-structured interviews are based on the CISA Zero Trust Maturity Model (ZTMM) created by Cybersecurity and Infrastructure Security Agency (CISA) in 2021 but later revised in 2023, the Zero Trust supply chain model (ZTSC) by Do Amaral and Gondim (2021), the Extended Zero Trust Maturity Model (EZTMM) by Tokerud et al. (2023) and the Cybersecurity Capability Maturity Model (C2M2) by the Office of Cybersecurity, Energy Security, and Emergency response (2021) that were discussed in the fourth chapter. From these four models, aspects related to cyber supply chains are compared and combined to form the questions used in the semi-structured interviews.

In this study the focus is on the supply chains and thus the domains of questions will be centred around it. To keep the study simple, focus will be placed on three domains: People, Processes and Architecture. (Figure 5).

People was chosen to be the first domain because in a socio-technical systems such as a cyber supply chain, the human component is responsible for many possible threats, including insider threats. The human component in the system is often managed via policies and education that guide the actions of the users and educate them to use best practises (Lähde). The changes made by zero trust principles to the technical system might also extend the importance of the human component (Tokerud et al., 2023).

Process was selected as the second domain because following the standard people, process, technology model, processes include workflows and procedures that guide how organisations operate. Many of the zero trust principles are implemented in processes like for example, identification and authentication processes or asset management.

Architecture was opted as the final domain instead of technology since talking about supply chains and networks, the term felt more suited, but it encompasses the same areas that Tokerud et al., (2023) had in their technology domain that focused on dynamic access and threat protection. Similarly, infrastructure & networks following Do Amaral & Gondim (2021) wasn’t chosen because, end user devices were desired to be included into the domain.

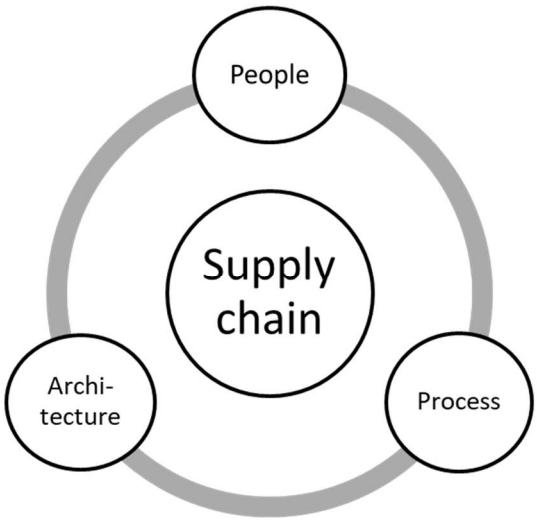

Figure 5 Domains of the study

The questions that are used in the semi structured interviews are based on the academic literature and maturity standards according to the table 5. By sources ZTMM refers to the Zero Trust Maturity Model by CISA 2023, ZTSC refers to the model by Do Amaral & Gondim (2021) that explored zero trust in supply chain environments EZTMM refers to the Extended Zero Trust Maturity Model by Tokerud et al. (2023). The difference between question people 1 and processes 3 is that in the people domain, focus is in using logs to improve security training, for example based on past incidents, whereas in the process domain the focus is improving security policies based on the past incidents. Both utilize data from security incidents and logs but in people domain that data is used in training and in process domain it is used in updating policies.

Table 5 Study questionnaire and motives behind it

Domain	Question	Source	Goal
People	How does your organisation handle security incidents?	EZTMM (People 10, 18) ZTSC (C18)	To find out if organisation reports security incidents, improves upon them, and includes them in employee training.
People	Do you control which people are allowed to access your supply chain system via for example background checks?	ZTSC (C6)	To find if the organisation tries to find out possible insider threats when hiring and later on with regular checks.
People	How does your organisation improve the cybersecurity awareness of your employees? Do you also include external users of your systems in this?	ZTSC (C14), EZTMM (People 2, 4, 8, 15)	Is the organisation maintaining a cybersecurity awareness program, are also external users of systems included in this training and how the program is updated)
Process	How does your organisation guarantee the security of the software products / systems it uses?	EZTMM (Process 48) ZTSC (C17) ZTMM (Devices)	Find out if the organisation has security requirements for its software vendors to avoid software supply chain attacks.
Process	What kind of system logs is your organisation keeping of events in the system?	ZTSC (C1, C15)	Are the organisations trying to detect security incidents by analysing logs and thus promote accountability
Process	How do you update your access control policies?	ZTSC (C8, EZTMM (Technology 18,19	What kind of information do you use to support the updating process? Logs or threat intelligence?
Process	Have you identified your critical supply chain assets and if so, how did you identify them?	ZTSC (C10) ZTMM (Devices)	Do you have a contingency plan for these assets? How often do you update this plan?
Process	Does your organisation have a cyber supply chain incidence plan? If so, what does it include?	How often is it updated? Does it include information sharing?	How the organisation plans to recover and maintain operations in cases of cyber supply chain incidents?
Process	Are you proactively trying to find vulnerabilities in your supply chain system?	EZTMM (Processes 30, 40) Technology (18, 21)	To find out if the organisation is actively trying to find vulnerabilities from itself but also its suppliers using for example red teams.
Process	Do you consider security aspects while selecting your suppliers?	EZTMM (Processes 48, 49)	To find out if cybersecurity is a factor in selecting vendors, how the capabilities are checked and are unnecessary suppliers removed.
Architecture	Do you perform network micro-segmentation? Meaning have you split the system in a way that a selected user has	EZTMM (Technology 3,4) ZTMM (Networks) ZTSC (C1,)	To find out if organisation performs network segmentation in a way that limits access and thus improves network security.

	access to only a limited section of the network?		
Architecture	How does your organisation utilize encryption? Networks, data in storage, communication?	ZTMM (Data) EZTMM (Processes 53, 58, 62) ZTSC (C12)	To find out if the organisation utilizes encryption in its communication, networks and for data in storage.
Architecture	What kind of access control is used to identify and authenticate users?	ZTMM (identity) ZTSC (C1, C5) EZTMM (Technology 9,12 / Processes 5,6)	Determine how the organisation is authenticating its users, is MFA used, is the authentication session based, does access require a business need or third-party approval?
Architecture	How does your organisation guarantee end device security?	EZTMM (Technology 3) ZTMM (Devices, Data)	Determine if the organisation controls that operating systems, antivirus and other software are kept updated. And if end device data is used to improve security for example firewall rules.
Architecture	How do external users access your systems?	EZTMM (processes 52), ZTMM (Networks, Applications & workloads)	To find out if the organisation uses technologies (VPN) or separate systems (proxy server) that external users use to connect to systems.

Table 5 shows that the questionnaire that follows the three domains of the study while trying to comprehensively find how organisations have implemented zero trust in their supply chains. The questions followed themes found in several maturity models created for measuring zero trust implementations making them scientifically founded.

Nine organisations were interviewed in this study representing different fields and different organisation sizes. Next research data will be presented starting with metadata about the interviewees and organisations to allow understanding the role of interviewees and the context of the organisation followed by case profiles.

All interviewed organisations were given the chance to review and comment their case descriptions. Explicit permissions for publishing the descriptions were received from five organisations while the rest didn't comment anything. For the organisations that didn't give explicit permissions, additional anonymisation was done, to ensure the anonymity of the organisations.

Table 6 shows the interviewees, their role and time in their role as well as their prior knowledge on zero trust. This allowed understanding if the people responsible for cybersecurity had a predominantly business-oriented or technical perspective. Table 7 introduces the case organisations showing their differences in size, field, number of suppliers, management of cybersecurity and

experienced cyberattacks. This shows that the organisations varied in size and field but also had different size supply chains and overall represent a wide selection of Finnish organisations.

Table 6 Interviewed employees

Case	Role	Time in role	Knowledge about zero trust
1	Administrative director	4 years	No prior knowledge
2	Head of IT	3,5 years	Had prior knowledge
3	Head of IT security	6 years	Extended prior knowledge
4	Cybersecurity team lead	3,5 years	Had prior knowledge
5	CFO	22 years	Had heard about it
6	Head of ICT	9 years	Had prior knowledge
7	IT manager	1,5 years	Had prior knowledge
8	CIO	8 years	Had prior knowledge
9	IT specialist	6 months	Had prior knowledge

Table 7 Interviewed companies

Case	Employees	Field	Number of suppliers	Cybersecurity management	Cyberattacks in last 5 years
1	<50	Manufacturing	25-50	Technical management outsourced	Phishing attempts
2	<50	Logistics	100-150	Governance internal, technical outsourced	DoS, data leakage in supply chain
3	7500-10000	Insurance	Hundreds	Internal, some technical solutions outsourced	Identity fraud attempts, malware attempts, DoS, AI based attacks
4	3000-3500	Retail	300-350	SOC outsourced, everything else internal	Phishing
5	<50	Energy	50-100	Outsourced	No attacks to targeting the organisation
6	400-500	Manufacturing	500-750	Management internal, services like CSOC outsourced	Phishing and exploitation of vulnerabilities
7	150-250	Manufacturing	150-250	Management internal, technical implementation, monitoring, and surveillance outsourced	Phishing
8	500-750	Manufacturing	500-1000	Mostly internal, some technical services like network management and SIEM building outsourced	Phishing and man-in-the-middle attacks. Ransomware attack more than 5 years ago
9	100-150	Manufacturing	Hundreds (thousands in global organisation)	Parent organisation is responsible for cybersecurity	Phishing and CNC attempts

4.2 Case profiles

In this chapter Eisenhardt method was followed by doing a within-case analysis. The goal of within-case analysis is to allow the researcher cope with volume of data. For example, this can be done by writing descriptions of the organisations. (Eisenhardt, 1989). In this study the analysis is done by creating profiles of each case organisation, which enabled evaluating cases and eventually categorising them. The profiles were built around the theoretical framework, people, process and architecture, and the metadata of the organisations visible on table 8, thus creating a wholistic profile of the organisations. This profiling was done iteratively, on the first iteration zero trust components were identified from the interviews, which were transformed into the coding visible in table 9. On the second iteration, the interviews were compared against the coding, allowing the categorisation based on zero trust maturity on top of organisation size.

4.2.1 Case organisation 1

Case 1 is a middle-sized organisation that manufactures technological instruments. They have outsourced most of cybersecurity management and the person responsible for cybersecurity was the administrative director, which implied that they didn't have an internal person responsible for IT. They had experienced only phishing attacks targeting employees. They identified a global shutdown as the main threat for their supply chain. Thus, it could be said that cybersecurity is not in the focus of the organisation, and it is not perceived as the main threat to their operations. Operating in manufacturing, the case organisation 1 has an increased attack surface due to many suppliers of both software and physical components and due to external access to information systems of some suppliers. Having both IT and cybersecurity skills outsourced leaves the general capabilities inside the company low. Thus, the attack surface of organisation 1 is relatively high compared to the general capabilities.

In the people domain the capabilities of were related mostly to their communication policies. The organisation 1 had plans in place for cyber incidents, which included informing their own employees but also external parties with significant incidents. Thus, the current situation relating cyber threats was communicated to the employees but also external parties. The organisation stated that they have one-time background checks as a part recruitment process but no checks for external users. However, it must be stated that there were only a handful of external users, which limits the risk. They described their employee cybersecurity awareness training being informing them about the current attacks and offering a voluntary external online training made by a service provider. Thus, it can be stated that people in the organisation are well informed and aware about the present

cyber threats, but cybersecurity training has been left to themselves. Employees' backgrounds are checked as a part of the recruitment process, but external users are not checked. This doesn't present any zero trust aspects in the people domain, thus leaving possibilities for internal threats that might be caused by mistakes made by untrained users or malicious external users.

The capabilities in the process domain where mainly limited to usage of role-based access control and having contingency plans for the physical supply chain. However capabilities in other areas in the domain where left lacking. Only considering cybersecurity aspects and not having formal processes or checks when choosing software vendors leaves the capabilities to detect vulnerabilities or risk factors low. Similarly, not collecting comprehensive system logs nor analysing these logs proactively or conducting regular vulnerability scanning or penetration testing, show only limited capabilities for detecting attacks when they happen. Thus, the capabilities in the process domain show only low zero trust maturity when considering the lack of implemented zero trust principles compared to the attack surface.

Case organisation 1's architecture showed only few capabilities. Their network had not been micro segmented. The interviewee did not know if their data and communications were encrypted. The organisation utilized password and two-factor authentications. MFA was used in certain environments and applications and was not user dependent. To access their on-premises systems externally a VPN connection was used to connect to their network. Their IT partner was responsible for maintaining their endpoint devises and securing their networks. Securing the devices included an antivirus software. The architecture of case organisation 1 did not show proper signs of a zero trust implementation even though MFA was implemented to certain environments and applications.

All in all, the capabilities of case organisation 1 showed no or only little zero trust components. However, the attack surfaced of the organisation is increased due to multiple software and component providers and external access of some suppliers, resulting in a low zero trust maturity in all three domains.

4.2.2 Case organisation 2

Case organisation 2 is a medium sized logistics organisation. The person interviewed was their IT-manager who was also responsible for their cybersecurity. Their attack surface is on the higher side due large number of suppliers and having both customer and supplier external access to their systems. They have experienced DoS attacks and data leaks originating from their supply chain, on top of various minor incidents. They saw low level Microsoft 365 phishing attacks, that can lead to

deeper infiltration to the supply chain as the biggest threat to their operations. They stated that whilst there is a lot of discussion about nation state threats, the low-level attacks are much more likely and, thus are the largest threat. The interviewee had heard of zero trust and told that they have implemented zero trust principles. Thus, it can be stated that the organisation sees cybersecurity as essential part of enabling their business functions, which should cover the relatively large attack surface.

The people domain showed extensive zero trust capabilities. The organisation had extensive policies and processes in place for cybersecurity, which were documented and updated regularly. Thus, the organisation had policies for internal communication, and in the case of major disruptions also external communication. The organisation defends itself against internal threats by utilizing formal security clearances done by the Finnish National Security Agency (SUPO) for anyone accessing critical systems. Employee training was also emphasized by policies and guidelines that stated mandatory regular micro-trainings, phishing simulations, and annually a major training or exercise. This demonstrates an approach to security, which includes the people as a part of the system. There are clear policies and guidelines showing a top-down approach, which guide how incidents are handled and communicated. Users of critical systems have had security clearances checked and they have been trained properly. Thus, it can be said that zero trust elements were present in the people domain creating high capabilities.

The processes domain also showed also high zero trust capabilities. The organisation utilised ISO certifications for both internal quality control (ISO 9000) and to vet their most significant suppliers (ISO 27000). For less important suppliers, a safety appendix was required. These verified or certified processes were audited using security scanning to their own systems and security audits to suppliers, which both were becoming more regular. Real time system log monitoring was established in the organisation through a freshly implemented SIEM system, which enabled the organisation to respond to potential threats in real time. The organisation aims for a centralised access management, where every system has a defined system owner. The annually reviewed access rights were updated through a process triggered by changes in employment initiated by HR or supervisors. The access control utilised dynamic components, e.g. threat intelligence, to define requirements for access control like MFA. The organisation classifies its systems into three criticality levels and has established continuity plans, which should be updated annually, for the most critical systems. The processes demonstrate some zero trust elements but leave still room for improvement procurement processes for services and planning for cyber supply chain. Regular

vulnerability scanning and more extensive log collection and analyse are under development and will improve the zero trust performance regarding processes.

The architecture showed the most zero trust components of all domains. Extensive micro-segmentation its network was implemented, and communication was run on private fibres to the data centre, which is why not all traffic was encrypted, although all critical traffic is point-to-point encrypted. Their technical access control is managed in Microsoft Entra ID where there are conditional accesses, which enables secure authentication of users according to zero trust policies including MFA for all non-trusted devices. The passwords required are minimum 16 characters with complexity requirements, which needs to be changed annually. The organisation secures endpoint devices with Microsoft Intune and EDR (Endpoint detection & response) solutions, which means that the endpoint devices are automatically monitored for anomalies or signs of attacks. For securing external users' access to their systems, they are using a client-based VPN solution that requires MFA and still the access is granted to only required segments, thus demonstrating zero trust and minimal required access. Thus, the architecture of the organisation demonstrates many zero trust elements, like micro-segmentation, conditional access policies, protecting endpoint devices and securing external accesses. To improve the zero trust performance the organisation could implement just-in-time or per case access to limit the access for users to only necessary.

In conclusion case organisation 2 had extensive processes regarding people and the business processes themselves. Their architecture still outshines the other domains with very comprehensive zero trust implementation but with still room to improve. Many aspects of zero trust can be found on their policies while some are still under development like vulnerability scanning and log collection. All in all, for its size the organisation demonstrated high zero trust capabilities.

4.2.3 Case organisation 3

Case organisation 3 is a large international insurance company. The person interviewed was their head of IT security. The attack surface of the organisation is very large due to having hundreds of partners that provide software or other services and due to the sensitive nature of their data. These partners offered their services through an API platform that connects to some of the organisation's systems. The large size however enables them to have an internal IT and a dedicated cybersecurity organisation managing information security. The large attack surface had materialised in many cyberattack attempts including identity theft, malware, denial-of-service attacks but also AI based attacks even though rarer than the previous. From the perspective of the Head of IT security the largest threat to their cyber supply chain was a data breach somewhere in the supply chain, which

would allow confidential information to leak to outside actors. They also acknowledged that they are moving towards a zero trust and have it implemented in their architecture. Thus, it can be said that the organisation handles sensitive data and due to its size, they are a target to many cyberattacks, which is why they have a department for IT-security.

In the people domain the organisation had a robust standard process to handle security incidents, which includes people, process, and technology perspectives. These processes include communication to relevant management groups internally. They also communicate cyberattacks externally as a part of their monthly reporting and specially to certain stakeholders. Previous attacks are also used as examples in the organisation's cybersecurity awareness training, which is done during the cyber month in October. They also have ongoing mandatory cybersecurity trainings including phishing simulators and micro-trainings. The organisations on-boarding process includes background checks, which might be trough national security agencies depending on regulations. It can be said that the people domain in the organisation shows many traits of zero trust like official background checks, mandatory training including past incidents and a properly documented incident handling process and communication.

The organisation has a procurement process where the IT security team provides security requirements for procurement of products or services that vendors must fulfil. These requirements technical and procedural requirements mandate required security levels for vendors that vary based on the services provided by the vendor. An example for this would be that vendors handling personal data are required to fulfil specific requirements for data processing. The procurement process for physical components and services has a broad security toolkit that is used to verify supplier claims. The process includes demonstrating security controls, staff training and other governance measures that guarantee security of suppliers. The IT security team helps the procurement team for the security related requirements. Thus, the organisation aims to mitigate risks coming from the supply chain by mandating levels of security from suppliers. While doing this they accept certifications like ISO 270001 but those are never enough on their own and the vendors still need to pass the audit of the security organisation. The organisation utilises a SIEM system to collect both security and access logs both analysed automatically to identify possible security incidents and thus, maintaining a good situational awareness. They also have a solution that enables deeper investigation to incidents that may have passed the automatic analysis. The organisation manages their access control rules through a centralized identity and governance administration process where users apply access from the central system and log details are collected on, who asked, which accesses, and who accepted it. These are reviewed regularly, biannually with personal

information and annually for other information. The access rules are often role based but some roles utilise just-in-time access where they are only granted access for the task in hand. This shows zero trust implementation balanced with traditional role-based access that maintains efficient duties for mundane duties but for unordinary accesses an extra layer of protection via zero trust is introduced. The organisation has implemented robust contingency plans to mitigate the large attack surface. They have identified critical resources in their supply chain, and the contingency planning responsibility has been delegated to the departments responsible for those platforms. For cyber supply chain incidents, the department has their own security incident process while also relying on the vendor contracts including reporting obligations. Thus, the organisation has multiple levels of contingency. The organisation maintains its security posture by daily vulnerability scans and by performing security checks for all new software products. Thus, the organisation takes a proactive approach on finding vulnerabilities showing zero trust implementation. Overall, the processes of the organisation demonstrate multiple zero trust components in various processes like procurement of software and services, proactive vulnerability scanning and automatic log analysing.

The architecture of the organisation utilizes some zero trust principles. They are utilising micro-segmentation for certain critical services but some networks like office networks are not micro-segmented at host level. They utilise encryptions following zero trust principles, encryption at rest, encryption at transit, and authenticating everything. This applies to both internal and external communication. This is also mandated by legislation since the organisation falls under DORA legislation. They use a centralised identity provider and a centralised access management to authenticate users. This includes MFA for all external access, which is encrypted varying on the data. For critical information IPsec tunnels with MFA are used but for other traffic TLS/SSH encryptions are used. These architecture choices show the same balance with efficiency and security in encryption and in micro-segmentation and thus, show a high zero trust maturity.

Overall, organisation 3 shows high maturity zero trust implementation in all domains. Balancing between security and efficiency can be seen especially in process and architecture designs, but security aspects are taken well into consideration in all of the decisions the organisation makes.

4.2.4 Case organisation 4

Case organisation 4 is a large parent organisation for a group whose core operations are in retail. The organisation provides services for the group’s entities. The person interviewed was the team lead and supervisor of the IT department, which currently has eight cybersecurity specialists. The cybersecurity organisation is half decentralised in a way that the specialists are in different

departments but still belong to the central cybersecurity team. To complement the internal cybersecurity team, the organisation had on outsourced CSOC service. The organisation is widely connected having hundreds of partners itself while most of the suppliers are of the local entities. Their systems are partially integrated to outside actors and service providers since the traditional IT is mostly outsourced, while some on-premises environments exist. On top of that there are a huge number of system integrations that connect the local actors to the parent organisations systems. Thus, the attack surface of the organisation is substantial. The organisation has experienced many cyberattack attempts, most of which have been phishing. Some of those attempts have been successful and compromised some credentials but there have been no major successful attacks. The organisation acknowledges the whole supply chain is a threat and the Valio-case has stirred a lot of discussion. Their top threats still are phishing, identity threats, and cyberattacks to the supply chain.

The organisation handles security incidents through the C-SOC that should detect most of the attacks, but in case anyone in the organisation observes an attack they are instructed to notify the C-SOC. This notifying obligation is also spread to the partners of the case organisation. There is not much communication of small attacks where only individuals are affected but for larger incidents there is a crisis management team responsible for internal and external communication. The organisation does basic checks in the personnel as a part of recruitment process, this currently does not include security clearances from the Finnish Security and Intelligence Service (SUPO), but it is under consideration for certain roles. Currently the organisation has a mandatory annual web-based security training for employees and a continuous phishing simulator offering also micro-trainings. They have recognised that the web-based training is a bit stiff and are exploring for alternative solutions. The people domain shows only little zero trust components currently, while there are proper communication channels and some level of background checks following zero trust principles, but more frequent and engaging training could be beneficial as well as proper background checks. Also including and informing normal employees about low level cyberattacks can raise awareness and help educate users of the most common threats.

The procurement process of systems and software entails standard security requirements that the organisation requires from their suppliers. The data protection or security evaluation process is mandatory for all new suppliers. The case organisation also accepts certifications like ISO or SOC 2 or information security governance descriptions. However, if the vendor has none of those and the purchasing party is adamant on purchasing from that vendor, the security team can conduct their own evaluation. Thus, the organisation regards certifications higher than its own security audits, which puts lots of trust on those certifications. This procurement process applies to also physical

service providers and those must be evaluated in the same way as software service providers. The case organisation also develops their internal software, which is done through DevSecOps following a guidebook on secure programming practices. The software products are also checked by vulnerability scanners to find vulnerabilities before deployment. The organisation also performs regular vulnerability scans to its own systems and expects their suppliers to report any vulnerabilities they might have. This shows zero trust implementation since they regularly and proactively check for vulnerabilities and perform security checks to systems before releasing them. The organisation leverages XDR agents to collect security logs into a SIEM, which is used by the SOC to monitor the security in real time. The organisation manages access control rules centrally by an IAM (Identity and access management)-team that use a central tool to manage the access controls. Role-based access policies are used, which are created and updated by changes in user's duties. These accesses are also reviewed regularly. This demonstrates some level of zero trust since everything is logged, but access is granted based on roles and not case by case. The organisation has identified their critical processes and the related systems and people roles. They have contingency plans for critical processes, and the risk management department keeps them updated. For cyber supply chain incidents, the organisation has a C-SERT playbook for certain events but having conducted regularly cyber exercises involving the security team, C-SERT and IT teams for CMT, they have noted that no two attacks are the same, and playbooks might not work. Having these exercises shows zero trust implementation since it one of the best ways to prepare for possible attacks and create knowledge in the organisation. All in all, the processes show a high zero trust maturity but to increase the maturity even higher the organisation could leverage just-in-time access policies and analyse more comprehensive logs.

The architecture of the organisation aims to accomplish certain zero trust principles. They have implemented segmentation to their networks, but the level is not in the micro-level. They have for example separated office, IoT and device networks completely and the access they give to their suppliers is limited to supplier specific segments. They generally encrypt all traffic, especially all external traffic. They encrypt data in storage that is either classified or contains personal information. These show efforts on following zero trust principles but to attain a higher zero trust maturity more micro-level segmentation would be needed. Also encrypting all traffic and utilizing secure tunnels like IPsec or VPN to external traffic would increase the maturity. They use a centralised single sign-on, which utilizes MFA on all users and devices according to risk-based dynamic rules. They protect these endpoint devices by having an XDR agent installed, which enables C-SOC to monitor devices for security. For external users they use a partner VPN tunnel,

which is opened per supplier when needed and this access is work-station and purpose-limited. The users are still authenticated by a case organisations MFA that is used for logging the sign-ins and monitoring them. These show a high maturity of zero trust since users are authenticated using dynamic policies, which utilise MFA when needed. On top of that the endpoint devices are constantly monitored by the CSOC making them secure. The external access follows tight micro-segmentation, and access is granted following the principle of least privilege.

All in all, organisation 4 demonstrates high levels of zero trust maturity in process and architecture domains and medium maturity in people domain. They could improve these by having background checks on users accessing critical systems, having a sturdier supplier review process that doesn't rely on certifications and by implementing a more micro-segmentation network. Also, their external user access is built around zero trust principles since suppliers' access has been segmented, opened only when needed, encrypted and authenticated properly.

4.2.5 Case organisation 5

Case organisation 5 is a small organisation operating in the energy sector. Their core businesses are managing an electric grid and selling electricity. The interviewee was responsible for their finances and business operations. They have dozens of partners, which only have limited access to the organisations systems, the electric grid controlling system from surrounding systems, but commercial systems like CRM and finance systems are connected to IT vendors, additionally the organisation is connected to external SaaS environments where they provide data. The external actors however don't have access to the systems only exception being some IT support users. Thus, the attack surface of the organisation is split into the business side and grid control side, where the grid control has a limited surface while the business side systems have a larger surface. The organisation has not faced serious cyberattacks and they aren't even aware of most of the attempts since an external party, that cybersecurity has been outsourced, handles everything. The primary threat to their cyber supply chain is an attack towards their software providers, which would affect electricity market functions and thus, cause monetary damage to the case organisation.

The organisation described their cybersecurity incident handling to be according to law, especially with personal information that is under GDPR legislation. The organisation has communication protocols in place for cyber incidents that include internal and external communication. However, their external cybersecurity partner handles the cybersecurity management, which explains the lack of processes related to incident recovery or incident handling. The case organisation doesn't conduct formal background checks on their employees, just the basic checks during recruitment

process. They have annual mandatory cybersecurity awareness training, which comes as a package that everyone in the organisation must complete. The package is primarily concerned about GDPR regulations but has additional levels for management that contain NIS-2 subjects. This training is however more focused on following legislation than maintaining information security and thus doesn't promote zero trust principles. Trusting an outside vendor to handle security incidents and having only little control over them shows a low maturity zero trust management, even though the SOC monitoring is effective in identifying possible threatening anomalies. Having practically no background checks is also not showing a high zero trust maturity. There would be possibilities for a higher zero trust maturity, if there would be more security focused training for background checked employees and robust internal processes on handling security incidents. Thus, the zero trust maturity in the people domain stays low.

The processes domain showed an outsourced approach towards security. The procurement process of new software systems relies on the external service providers expertise since they are the ones conducting security evaluations and installing those systems whereas for physical services and products there was no robust process and security requirements depended on the size and importance of the product. This is not following zero trust principles since the organisations trusts and relies on an external party for the security of their products and organisation making them depended on that service provider. However, all logs were collected and analysed by their service provider's 24/7 SOC, thus informing the organisation of any incidents. This extensive logging follows zero trust principles since everything is monitored, and any incidents can be noticed in real time. The access policies of organisation follow the principle of least privilege and are either role or user-based, thus showing some zero trust implementation. The organisation has identified the electric grid and its control systems as the most critical systems and the CRM-system as critical for business functions and has contingency plans in place for these resources. Due to the electric grid being critical infrastructure, legislation mandates the organisation to communicate and update these plans every other year. The organisation conducts regular vulnerability scans to its information systems, including the SaaS environment. The processes of the organisation show signs of zero trust implementation regarding the logging and using a SOC to monitor traffic. The access control follows the principle of least privilege, but the policies could be more dynamic to limit exposure. Otherwise, many of the processes like procurement or recruitment don't show signs of zero trust rather a very high trust on service providers. Thus, the processes demonstrate medium level zero trust maturity.

The organisation has a micro-segmentation project on going that will separate the office network to its own separate compartment and their plan is to change the whole infrastructure to follow NIS-2 requirements regarding planning and risk mitigation. The energy grid control system is totally segmented to its own, which is not connected to anything, separating the office networks from operational technology. According to the interviewee the organisation is not using encryptions where it is not needed by law referring to GDPR and encrypting personal information. External communication was done via a VPN connection making it encrypted. The endpoint devices are protected by an antivirus software and monitoring by the SOC. External actors are allowed into the networks only by the organisation IT provider, which opens ports and interfaces for the tasks at hand. This connection is done by VPN connections making it encrypted. All in all, the architecture of the organisation shows zero trust implementation regarding the segmentation of critical systems and a goal of micro-segmenting the rest of the networks as well. External usage is only allowed by the IT support, which opens a limited access to the external users. However, more encryptions could be used in communication and in storage and the authentication process could benefit from a centralised single sign-on process secured by MFA.

The organisation has two sides when it comes to zero trust maturity. The electric grid control system follows strict zero trust being totally isolated, but the rest of the organisation has only limited principles implemented. Thus, generally in zero trust maturity in the people and architecture domains stayed low, whereas in the process domain it was medium. For the energy grid control the architecture domain maturity was high.

4.2.6 Case organisation 6

Case organisation 6 is a medium size organisation operating in industrial manufacturing. The interviewee was the ICT lead at the organisation that functions as parent organisation in their group. They are responsible for all ICT matters but also cybersecurity. The organisation is widely connected having over 500 partners and suppliers. These partners have access to their systems and there is some integration with their suppliers like EDI integrations and API based integrations creating a large attack surface. The organisation has outsourced some services like CSOC keeping the general cybersecurity management is internal. They have encountered some cyberattacks, which have been mostly phishing and exploitation of vulnerabilities. The interviewee stated that from ICT standpoint the largest threat to the supply chain from the cybersecurity side is leaked credentials due to partners not having an adequate security level. From general perspective the interviewee named material shortages as a large risk.

The organisation handles cybersecurity incidents through a process that starts with classifying the incident based on criticality and severity and then mitigating it. Classifying incidents is needed due to two of the group's organisation falling under NIS-2 directive and its reporting obligations. This process includes also internal communication. When the impact of incidents is relevant, the organisation communicates to the affected stakeholders, both external and internal. This process is part of the employee cybersecurity awareness training, which is included in the onboarding process. The organisation also has an external party providing regular cybersecurity training currently biannually or annually, but they are updating their policies currently and looking for a suitable interval. The organisation doesn't conduct background checks on their employees but are protecting themselves from internal threats through a CSOC service. Generally, the people domain, does show some signs of zero trust implementation. Having the SOC to monitor anomalies from network traffic. However, to protect the organisation to attacks employees could get more regular training and there could be background checks for the people with access to sensitive systems and information. And since the SOC service has only just been implemented, at the time of the interview, the maturity stays medium.

When acquiring systems or software services the organisation has a process, which entails evaluating the availability of those systems and the criticality of the information if stores. For low criticality products there is no security assessment, but for critical systems the organisation checks the vendors certifications and if those are non-existent, they use their own secure questionnaire to guarantee that the products are safe. This process is the same for physical products or services since they lack the capabilities to check for vulnerabilities in hardware themselves and trust the process in most procurements. The organisation collects login data from computers, firewalls and servers, which are then analysed by their CSOC. All logs are not there yet because the CSOC service was taken on less than a week before the interview. This will increase the zero trust maturity of the organisation in the future, when more comprehensive logs are observed by the CSOC. The access control policies the organisation uses are role-based where needed access levels are defined at the beginning of the employment and updated if needed requiring a supervisor's approval. They also have certain spaces where the owner's approval is needed for giving access to someone. The organisation has identified critical components in their supply chain but contingency plans for those resources are not ready yet. For cyber supply chain security, the organisation relies on their partners informing them. In their assessment process the organisation has a contingency plan for critical resources. These plans can include for example duplicate network connections or services. The organisations partner providing the CSOC service also performs regular vulnerability scans to the

organisation's servers and endpoint devices, which helps the organisation to hunt for vulnerabilities proactively, and through CSOC, reactively. The organisations processes show a movement towards zero trust implementation with implementing the CSOC service and regular vulnerability scanning. Also including security assessments in procurement process is good. To improve zero trust maturity the organisation could better evaluate the security of its services and products by for example doing penetration testing, even if they were not critical. They could also improve their access control policies by reviewing the accesses more often. Thus, the zero trust maturity regarding processes is medium.

The organisation had implemented some use case based segmentation to its networks but not on microlevel. They are going towards encrypting all critical data and communications, but some older systems are not supporting it so where possible, everything is encrypted. The organisation primarily uses single sign-on with MFA but again some systems didn't support it. The single sign-on access control is conditional based meaning that based on a number of criteria MFA can be enforced or not. To secure endpoint devices, the organisation has installed an antivirus and monitoring software to the devices, which are also monitored by the SOC. External access to the organisations systems is case-specific. Cloud systems are accessed through the cloud with MFA, some on-premises software is accessed through a VPN-connection, and some systems are only opened on demand. The architecture of the organisation shows progression towards zero trust but is not there yet. More micro-segmentation and replacing old systems enabling encryptions would increase the maturity in the architecture domain. Also, if possible, more systems should be opened to external users only when needed, even though the connection would be secured by VPN connections. Thus, the zero trust maturity stays medium also in the architecture domain.

As a conclusion, the organisation seems to be moving towards a zero trust implementation but for now the maturity is medium on all domains. By adopting newer systems, implementing stricter policies, and training users more, they could reach a higher zero trust security maturity.

4.2.7 Case organisation 7

Case organisation 7 is a medium sized manufacturing organisation, where the interviewee is responsible for the IT of the entire organisation. The organisation has around 200, suppliers, but those have only little connections to the case organisations systems, apart from the cloud-based systems. Mainly the IT-partners are connected to the organisations networks and have access to the on-premises systems. The organisation has mainly outsourced the technical implementation of cybersecurity including monitoring and surveillance. The organisation has experienced small

phishing attacks but are not aware of any major attack attempts. As for the largest threats for their supply chain, the organisation feels that a material shortage is the most severe and one that has also materialised. Thus, the organisations attack surface is reduced by only limited access by supplier but risks with cloud-based systems still exist.

The organisation handles cybersecurity incidents through a process, which includes root cause analysis and communicating openly with employees and external parties. This way the employees stay aware of any current threats and are able to identify them better. The organisation does not conduct background checks on its employees and doesn't have means, apart from network monitoring, to identify insider threats. Their employee cybersecurity and awareness training are done via online training service that includes short sessions and simulated attacks. The training is mainly targeted for office workers, which make for half of the staff. To contribute to the awareness training the organisation openly shares real-life examples and communicates of present attacks. The training is mandatory and continues through a year with bi-monthly modules. The people domain shows the implementation of zero trust principles especially on communicating about cyber incidents and employee awareness training, but to improve the maturity of the implementation there could be background checks on employees and training for also factory floor workers. Thus, the zero trust maturity in the people domain is medium.

The process domain showed the goal of securing the organisation, but those processes could benefit from more formality. Security aspects are discussed in all procurement process, and the supplier is asked to provide a document on their processes, which is one of the selection criteria in procurement process. The organisation develops their own OT-software through a partner, but due outsourcing the partner's internal processes have to be trusted. The organisation collects log information varying on the system. Their cloud system collects all logs, which are monitored by the SOC, whereas in the ERP system logs are collected, but those logs are not actively monitored. Their Microsoft 365 environment also has logging turned on, but it is used to follow how users do things in order to streamline processes, not for security purposes. VPN and firewall logs are used to track who and from where users are signing in. On top of that all foreign traffic is blocked due to the organisation being very localised. In cases that employees go for a trip abroad, access from those countries is opened for that time period. These logs would allow more mature zero trust implementation if those would be analysed in real time by a SOC or an automated service, but blocking all foreign connections shows signs of zero trust since it limits the possibilities of foreign attacks. The organisation updates its access control policies regularly through processes. The most important part of it is included in the on- and offboarding processes but also changes in roles trigger

changes in the accesses given. The access is role-based but due to the small size of the office staff, users often have multiple roles. These access control policies show only little zero trust even when role-based access is the goal. Logging information and having more dynamic access rights would increase the maturity of the organisation. The organisation didn't actively identify its supply chains critical resources since they are quite isolated and aren't seeing major risks in that area, but for cyber supply chain they have a documented business continuity plan for external threats, although these threats are more of threats of nature like power shortages and not cyber side threats. This is also reflected to the fact that the organisation doesn't conduct proactive vulnerability scanning or penetration testing. In total, the processes of the organisation would allow a much more mature zero trust implementation if log information would be used to detect security incidents, and if there was a more robust security screening as part of the procurement process. The access controls could benefit from more dynamic access management, and planning for external cyber incidents could be beneficial. Thus, the maturity in the process domain stays low.

The organisation has segmented its factory environment and OT into a separate segment from the office networks. The factory environment contains some automation that the organisation has wanted to keep offline. Thus, external access to the factory network is restricted. The interviewee was not able to disclose whether the organisation used encryptions on data storage or communication, but all external traffic was done through a VPN tunnel making it at least encrypted. The authentication method of the organisation utilises MFA where possible, but for example the ERP solution was too outdated to support it. The organisation doesn't enforce regular password changes but has a password length requirement of 18 characters. The goal of the organisation would be to use MFA everywhere, but some systems still aren't supporting it. The organisation has a central asset register, which includes all computers but not phones. Those computers are managed and updated automatically by a service provider, which ensures updated software including an antivirus software. Phones are able to connect to the organisations only to Microsoft 365 platform. The organisation has only two external parties with access to their systems. The main infrastructure partner has administrator level access, but for others, the organisation grants external identities through active directory, making those accounts separate from the internal ones. These connections to on-premises software are secured via VPN connections. Having the OT in its own network segment follows zero trust, but wider segmentation in the office networks could still be beneficial. Having outdated systems that don't support MFA can introduce risk, especially when the system in question is the core ERP system. By implementing a wider MFA usage and optionally a centralised single sign-on service would increase the zero-trust maturity. Per the interview it can't be stated

how the organisation utilises encryptions, but at least the external connections are encrypted by VPN. Thus, the maturity in the architecture domain also stays low.

All in all, the zero trust maturity of the organisation stays low. In people domain the organisation has great communication about cybersecurity incidents and trains people well, however background checks or other ways of identifying internal threats could be beneficial. For processes the organisation could introduce stricter cybersecurity evaluations into their procurement process. They could also use their log information for cybersecurity reasons by having a SOC service or an automated software. They could also benefit from identifying external cyberthreats and from having a more dynamic access control. For architecture, the organisation has segmented the OT environment from the office networks to protect automation, but more segmented access could still be beneficial. The organisation could increase the zero trust maturity by migrating to solutions supporting MFA and centralised single sign-on. Thus, the overall zero trust maturity stays low even but there is potential for more mature implementation.

4.2.8 Case organisation 8

Case organisation 8 is a relatively large operator in machinery and equipment manufacturing focusing on projects in the forestry industry. The interviewee was the CIO of the case organisation, which is a parent for five different subsidiaries. This part of the group produces the IT services for others in the group. They have a very wide partner and supplier network with 500 – 1000 active suppliers. The organisation has tried to minimise integrations with its suppliers but the ones that exist are mostly done via EDI-pipelines or APIs. Only partners with access to the organisations systems are the IT partners to whom internal network management has been outsourced. Apart from this internal network management and a SIEM, the cybersecurity management is handled internally. The organisation has faced cyberattacks in the past. In the last five years these have been phishing, that have led to some employee passwords being briefly compromised, and man-in-the-middle attacks. More than five years ago they had also experienced ransomware attacks. Thus, from cybersecurity perspective they identify malware entering through trusted suppliers and spreading in their environments as the largest threat to their cyber supply chain. The attack surface of the organisation is relatively small related to their size since they have greatly limited external accesses and are limiting integrations.

The organisation has a dedicated cybersecurity team that is responsible for cybersecurity incidents. Depending on the severity of the incident they also include external experts. The communication is extended to also external parties if needed but the internal communication is spread internally

through teams. The organisation can conduct background checks on people that have higher level admin credentials since it has been stated in their contracts but that has not been done with current employees due to their long careers with the company. The organisation detects insider threats by monitoring active directory logs, network drive usage and through DLP tools. They also have firewalls and their own SOC in place. Cybersecurity and awareness training at the organisation is done through continuous phishing training that also includes some smaller information packages about information security. On top of that, their onboarding process includes a security training, which everyone must complete before obtaining any devices. They also have had online trainings, which like the others, have been mandatory for employees. The organisation also provides summaries of past major incidents in their intranet to raise awareness of possible incidents and how they have happened. Thus, it can be stated that the organisation is following zero trust approach in the people domain since they are openly communicating about past incidents, have mandatory and regular security training and have a way of detecting insider threats through security logs or background checks.

The organisation ensures their systems and software products through contracts stating necessary levels of cybersecurity, but this part is currently being updated due to building an ISMS. One of the subsidiaries in the group builds automation software for OT environments and they have some security testing of software products, but it has no major role and is mostly functional testing. For services, the organisation is creating criteria for auditing suppliers that would state minimum security requirements. However, this mandating these criteria can be sometimes hard since the large software vendors like Microsoft don’t respond to these demands due to their market position. The organisation collects security logs into their SIEM, which automatically analyses the logs for anomalies and sends alert. These anomalies are sometimes followed up on, but they are not hunted, so to say. The organisation follows a role-based access control policy through centralised single sign-on. The organisation is on the process of identifying their supply chains critical resources and creating a contingency plan for those resources. This issue has come to surface through NIS-2 and ISMS implementation. In the future the contingency plans will be updated annually or every two years, but those still have to be formalised. The organisation has incident management plans that include IT systems in the supply chain, but those plans are also under construction. For material supply chain the organisation terminates any connections if there is misuse detected in a supplier. Identifying the critical resources in the supply chain needed in order to implement zero trust in it. To increase the maturity regarding the supply chain and cyber supply chain, the organisation should have plans for its key resources. They have performed some vulnerability scans to their

environments, but those scans are not yet systematic. This, like almost all processes, is on path of implementing zero trust approach. Having regular vulnerability scans helps the organisation to recognise vulnerabilities before they are exploited. The organisation could increase its zero trust maturity in having a more robust cybersecurity process in procurement and by adding all logs to the SIEM and analyse them with SOC and /or automation. Thus, the zero trust maturity in the process domain stays medium.

The organisations architecture features segmentation between building networks, office networks, and backup networks for the production environment. However, this segmentation could be tighter to ensure different segments for different systems and data. The organisation has capabilities to use encryption on all communication channels. However, they are classifying data and thus the encrypted messaging is still mainly used by data protection team. Data in endpoint devices and backup storage is encrypted. They are moving towards having encryptions on all communications and all data, but the process is long and will take years to fully adapt. They secure endpoint devices by managing them all, via Microsoft Intune. Then they are encrypted using BitLocker and multifactor authentication. They also feature antivirus software and XDR agents. The organisation authenticates users using MFA as de facto but not on trusted devices. For external users, the access is created through virtual machines on most systems but on few systems the external actors can access through their own devices due to software limitations. To increase the zero trust maturity in the architecture domain, the organisation could do tighter segmentation, migrate to systems supporting wider encryption and utilise more dynamic access control than just trusted devices.

As a conclusion, the organisation is performing well in the people domain having the possibility to do background checks for people with high-level access, education employees well and communicating about incidents and thus, has high zero trust maturity there. In the processes domain they are in the currently updating many operating policies, which will increase the zero trust maturity but for now the organisation could improve by having regular vulnerability scans, having a more robust cybersecurity process in procurement and by increasing the logs analysed in real time. The organisations architecture could utilise more encryptions and have a more dynamic access control. Thus, the zero trust maturity on process and architecture domains stays medium.

4.2.9 Case organisation 9

Case organisation 9 is a medium size organisation operating as a local branch of a global manufacturing organisation. The organisation itself has hundreds of partners, 50 of which are for IT, but if counting the partners coming from the European and global branches of the entire

organisation, the number raises to thousands effectively creating a huge attack surface to the global organisation. The person interviewed was an IT specialist who was part of the small IT-team in the case organisation. The cybersecurity management is handled centrally in the global organisation, but local actors are involved in cases regarding cybersecurity. The organisation faces phishing and CNC (command & control)-attempts, but no successful attacks had faced the local organisation in the six months that the interviewee had been in the company. The organisations systems are tied to the international organisations and for example their ERP system is hosted at the European actors' servers. Their external partners can have access to the systems, but those accesses have to be accepted by the global parent organisation. For the organisation, the biggest cyber related threat would be a breach or sabotage to one of the critical systems, since those would cause the most financial damage. The case organisation 9 differs from many other case organisations since it is the subsidiary organisation of a much larger parent organisation, whereas the other organisations have been those parent organisations. This is reflected to perspectives on cybersecurity processes.

The organisations cybersecurity incidents are handled by the centralised cybersecurity organisation who has CSIRT and SOC teams. The cybersecurity organisation conducts very thorough investigations on all incidents, for example they obtained a phishing email and experimented with it in a virtual environment to investigate what it could have caused. Internally there is limited communicating about ongoing attacks, inside the case organisation there naturally is communication about possible attacks if those are noticed and the central organisation contacts the affected parts of the organisation about incidents. However, from smaller attacks into other branches are not communicated to the others. The organisation protects itself against internal threats by following the principle of least privilege when providing access control policies. For external users, the background checking is left to the vendors, leaving them with the responsibility of ensuring that the users are who they claim to be. The central SOC also monitors the traffic to protect against attack attempts. The organisation provides global mandatory cybersecurity and awareness training. This training starts from the onboarding process where new employees receive credentials to a training portal where they have a month to complete the security trainings and if not done within a month, their supervisor gets notified. They also have mandatory training a few times every year containing courses for threats like phishing and email spoofing. These trainings also test the learning, meaning employees can't just click through them. Taking a few workdays to complete, the trainings can feel to be a bit much for non-tech savvy or non-IT personnel. The people domain shows a global approach to securing the organisation. All incidents are handled by a central team involving the affected areas and communicating appropriately. Principle of least privilege and

continuous SOC monitoring are used to mitigate risks related to internal threats and comprehensive cybersecurity awareness training is mandatory for all employees globally. These show a high zero trust maturity in the global level, but on a local level the organisation could conduct background checks on the people with higher level access into confidential information like trade secrets.

The case organisation shares most of its systems with the global organisation and the security of those systems is handled centrally. Even the systems that only the case organisation has, are still connected to the Europe or global organisations. The systems are secured through tight access control and logging actions in the systems. The organisation collects comprehensive logs from its systems that are analysed automatically by Rapid7 and TrendMicro software and their SOC that contacts the local branches whenever anomalies are detected. This shows a high zero trust maturity since security logs are actively processed, and anomalies are checked fast allowing the organisation to mitigate all incidents fast. The organisation controls their access policies through group policies, which all have to be approved by the global organisation. All access, internal and external, have to be requested through a ticket system, where each person gets just the level of access that they need for their duties. This again demonstrates high zero trust maturity and following the principle of least privilege. The organisation has identified its critical supply chain resources due to an ongoing Europewide NIS-2 implementation. They identified three services that fulfil the criticality criteria of NIS-2, for which the NIS-2 team in Europe has created notification chains and assigned the proper ownerships and responsibilities. The organisation had protocols before NIS-2, but due to it those have become larger and more specific. For cyber supply chain incidents, the organisation feels well protected since the access of the external partiers are very limited. If a third party is breached, they have a reporting obligation allowing the case organisation to act cutting the access of the breached party. The organisation conducts 24/7 vulnerability scanning using Rapid7 and the CSIRT team monitors any CVEs that might affect anything in the entire organisation and alerts relevant partners when needed. The CSIRT has the power to shut down services from partners if they aren’t complying with the CSIRTs requests to patch CVEs. The fact that the power to shutdown services has been given to CSIRT shows good zero trust implementation since the organisation continuously monitors vulnerabilities of external parties and also has the power to mitigate them. The procurement process for physical components and services is guided by the global organisation’s strict requirements for third parties. The cybersecurity requirements include NDAs, following secure practises and using up-to-date software. The processes of the company show the larger level zero trust implementation with strict protocols on procurement, centralised access control following

the principle of least privilege and monitoring the systems for vulnerabilities continuously. Thus, the zero trust maturity on processes is high.

The architecture domain demonstrated highly formal corporate centralised architecture, which implement security to the network. The interviewee didn't know about the micro-segmentation of the organisation since the networks are managed centrally. But for the usage of encryption the interviewee stated that in principle everything is encrypted, both data in storage and communication. The access control differs between systems, but MFA is enforced everywhere apart from some factory environments where systems aren't supporting it. For Office systems the MFA can be set to be only every 90 days but for some systems, like the ERP it is required every time. The access to ERP is executed through a Citrix portal, which keeps users logged in for only 15 minutes and requires reauthenticating if opening the system again after the time. The endpoint computers are protected using multiple software and continuous monitoring, and phones are able to access the Microsoft In-tune portal only after the device has been approved by the global organisation having its IMEI code. This shows a zero trust implementation to endpoint device management since all devices are managed by global organisation and continuously monitored. The external access to the systems is granted in segments and specific systems. If a partner needs access to the ERP system, it is done through the Citrix portal. For other systems, the organisation must whitelist the partners IP addresses and to get access. The architecture of the organisation again shows the size of the global organisation and a high maturity of zero trust implementation, especially with the endpoint device management. Most likely there is micro-segmentation done by the global organisation.

As a conclusion, the case organisation shows a high maturity of zero trust in all domains. Being the subsidiary of a large international organisation, the case organisation is secured by global processes and services. All domains show global level processes and procedures that are there to ensure global cybersecurity.

4.3 Analysis criteria

To analyse the interview data, the case organisations were evaluated on different themes derived from zero trust maturity models. In these themes, an iterative process was used to derive the codes seen on table 8, from the interview data. The cases were then, on next iteration categorised based on maturity in these themes through iterative analysis. The cases were then divided into small and large organisations and based on their zero trust maturity in these themes. This division to groups created the base for the cross-case analysis done in the next chapter.

Table 8 Coding for analysis

Theme	Codes
Incident response planning	Extensive regularly updated incident recovery plans and processes / Incident plans and processes / No planning
Incident communication	External & Internal / Internal / No communication
Identifying internal threats	Regular security screenings of external and internal users / SOC 24/7 monitoring of network anomalies / One-time background checks for external and internal users / One-time background checks for internal users / No background checks
Cybersecurity training	Regular, mandatory cybersecurity awareness training for internal & external users / Using past security incidents to educate users / Regular non-mandatory training for internal users / No regular training available
Software supply chain – Vendor security	All vendors are validated using formal processes / Vendors are security scanned / Major vendors are validated using formal processes/ Vendors are validated through processes including security certifications / Cybersecurity aspects are taken into consideration while choosing vendors / Cybersecurity aspects are not significant when choosing vendors
Software supply chain – Software security	All software products are formally tested / Critical software products are formally tested / Software products are not formally tested / Internal software is developed using secure development practises / Internal software is developed not using secure development practises
Log collection and analyse	Comprehensive logs are collected and proactively analysed using automation / SOC is used to monitor events 24/7 / Comprehensive logs are collected and analysed manually after security incidents / Some logs are collected and analysed only after security incidents / Logs are not collected
Log usage in security awareness training	Security incident logs are used in security awareness training / Past incidents are not used in security awareness training
Access control policies	Centralised automated dynamic policies / Centralised just-in-time access policies / Centralised per case approved policies / Static regularly updated role-based policies / Static role-based policies / Static person-based policies / No policies

Supply chain incident planning	Incident planning regarding critical or major supplier including reserve suppliers and processes to isolate incidents to suppliers / Contingency planning regarding critical suppliers / Reserve suppliers for critical components / No planning
Vulnerability management	Routine vulnerability scanning of own and vendor systems / Routine vulnerability scanning of own systems / Irregular vulnerability scanning of own systems / No vulnerability scanning
Physical supply chain	Formal procurement process that includes cybersecurity aspects / Cybersecurity aspects considered in procurement process / Cybersecurity has only minor influence in procurement process
Network micro-segmentation	Extensive micro-segmentation of networks / Vendor specific micro-segmentation / Micro-segmentation of critical systems / Micro-segmentation of office, IoT and OT networks / No Micro-segmentation
Encryption practises - Communication	All internal and external communication are encrypted / External communication to systems is encrypted / No communication is encrypted
Encryption practises - Storage	Data in storage is encrypted / Data is storage is not encrypted
Technical access management	MFA enforced through dynamic policies on all systems/ MFA enforced on some systems / Password authentication /
Endpoint device security	Endpoint devices secured with EDR solutions/ SOC monitoring of endpoint devices / Security measures include antivirus / Security measures not implemented on all devices
External access control	Access only through VPN / IPsec tunnels using MFA / Encrypted access (TLS / SSH) using MFA / Encrypted access with no MFA / External access using VPN / No encryption with MFA / No encryption no MFA

4.4 Cross-case analysis

Following the Eisenhardt method, a cross-case analysis was conducted through a within group and cross-group comparisons. The goal of these comparisons is to process the information, find patterns in the data, and to keep the researcher from jumping into premature conclusions by having different perspectives on the data (Eisenhardt, 1989).

In this study cases were grouped based on their organisation size and the zero trust maturity. Table 9 shows the basis of the case groupings by illustrating varying zero trust maturities and organisation sizes. The organisation size has been divided into small and large with 500 employees being the limiter, the only exception being case organisation 9, which is classified as a large organisation due to being a subsidiary of a large international organisation and having the security capabilities of a large company. Table 10 illustrates how the grouped cases were divided to each group.

Table 9 Zero trust maturities across case organisations

Case	Size	People	Process	Architecture	Overall
1	Small	Low	Low	Low	Low
2	Small	High	Medium	High	High
3	Large	High	High	High	High
4	Large	High	High	High	High
5	Small	Low	Low	Medium / high	Low / (Medium)
6	Small	Medium	Medium	Medium	Medium
7	Small	Medium	Low	Low	Low
8	Large	High	Medium	Medium	Medium
9	Large	High	High	High	High

Table 10 Classification of case organisations

Zero trust maturity	Organisations size	
	Small	Large
High maturity	2	3, 4, 9
Medium maturity	(5), 6	8
Low maturity	1, 5, 7	

Thus, the cross-case comparisons were conducted first through within group comparison between small size organisations with low maturity and large organisations with high maturity. Then a cross-group comparison was be done between small organisations with high or medium zero trust maturity compared to those with low maturity, large organisations with high performance compared to those with medium performance and finally between small and large organisations. The comparisons were done by comparing the practises of organisations on different topics using codes presented in table 8.

5 Findings

This chapter contains the findings of cross-case comparison beginning with within group comparison and ending with cross-group comparison. These consist of comparisons between the cases that are structured to follow the people, process, and architecture structure. This study found implementation of zero trust across all domains but variance especially among smaller organisations was large. Larger organisations also tended to have a higher zero trust maturity.

5.1 Within group comparison

5.1.1 Small size organisations with low maturity 1,5, 7

Out of five small case organisations, three had low zero trust maturity whereas one had a high and another medium maturity. The organisation sizes vary between case less than 50 with organisation 5 to 150-250 with case organisation 7. Case organisations 1 and 7 operated in manufacturing and organisation 5 at the energy sector. All three organisations had fairly little suppliers with case organisation 1 having only 25-50 and case organisation 7 having 150-250. The persons interviewed, and responsible for IT, were administrative or finance directives for organisations 1 and 5, and the IT manager for organisation 7. The two with non-IT leadership roles had more cybersecurity outsourced compared to organisation 7, which handled more management in house. Thus, organisations 1 and 5 were very reliant on their suppliers compared to the organisation 7. Past cyberattack attempts reflect this well. Case organisation 5 explained that:

> Well, our organisation has not been seriously targeted by cyberattacks. Actually, we don’t always even know because the external party handles most of it. (Case 5)

Practically all organisations face some sorts of cyberattacks like phishing and being this reliant on the supplier might affect the situational awareness of the organisation. Case organisations 1 and 7 had encountered phishing attacks but nothing more. Organisations 1 and 7 were the only ones in the entire study to name other than cyber related incidents as largest threats to their supply chains. This is most likely due to the fact that these threats, at least for organisation 7, had materialised and caused issues in the supply chain. Organisation 5 named a cyberattack to a software service provider, which reflects their business being selling electricity and attacks to the service providers would halt selling it, making this a similar issue to the physical threats experienced by the other two organisations. Generally, these three organisations illustrate the challenges small organisations face, they are too small to have cybersecurity handled internally, which leads to reliance on the suppliers

and the threats they perceive as largest are issues in physical material supply or with selling their product.

In the people domain organisations 1 and 5 had low maturity whereas organisation 7 had medium level maturity. Incident response planning for organisations 1 and 7 included plans and processes, which included communicating to internal and external stakeholders. Organisations described their processes followingly.

> There is a clear process for handling breaches—we try to identify root causes and communicate openly with any external parties that might be affected. We aim to communicate as fast and as openly as possible. (Case 7)
>
> That, at least we communicate in the company that something like this happened and then we may inform also to the service provider 1 that there is something like this. (Case 1)
>
> Our network traffic is monitored 24/7.
> If anything, unusual happens or someone tries to access us from outside, we get immediate alerts.
> If our Service provider 1 notices anything unusual they take action. (Case 5)

These captions show that the processes vary considerably. For cases 7 and 1 the actor doing the processes and communication is internal, but for case 5 it is an outside actor, showing a more outsourced management of cybersecurity.

To protect themselves against internal threats the organisations had varying methods. All cases had no formal background checks done by SUPO on their employees, just basic checks. However, case 5 had a SOC service in place to monitor network traffic, which can protect the organisation from malicious internal behaviour. This shows that small organisations tend to trust their employees and they aren't experiencing possibilities on corporate espionage or other malicious behaviour and thus, are not following zero trust principles on their internal actors.

Employee cybersecurity and awareness training is one that sets these three cases apart. Case 1 had no mandatory or continuous training for their employees, but they communicated about current threats improving the awareness of employees. They stated that:

> And then we have had a training offered by service provider 1 and then there was some, other similar service providers had webinars like this available for all employees, but not everybody attended them. (Case 1)
>
> If there are these attempts of attacks or these, people are informed about them. (Case 1)

Thus, the training was not mandatory for employees and having only a webinar offered by an external party does not cover the individual characteristics of an organisation and does not encourage employees to learn safe practises. However, informing employees about current threats and attacks improves awareness.

Case 5 described their training followingly:

> It's a package that everyone must complete. There's a questionnaire, and we go through everything. Management has additional levels, and there are separate NIS-2 levels too. (Case 5)
>
> It covers what employees can and cannot do, where they can go, and what to watch out for. (Case 5)

This shows that the organisation had regular mandatory training for their users, which had different levels depending on the position of an employee but the focus on the training is on legislation, especially GDPR and what it prohibits users on doing. It is of course good that there is a mandatory annual training for all employees, but the focus could be more in the cybersecurity part.

For case 7, the employee cybersecurity and awareness training, was the most comprehensive.

> We use an online training service with short sessions and simulated attacks. (Case 7)
>
> Previously, we had multi-hour training sessions, but we thought that a continuous online training with monthly or bi-monthly updates could be better. (Case 7)

This demonstrates that the organisation has invested in a continuous training for their employees, which consists of short sessions monthly or bi-monthly. This keeps the awareness higher and reminds employees of cybersecurity.

> We try to also share real-life examples and communicate about attacks to raise awareness. (Case 7)

By actively sharing and communication real life attacks that the organisation has faced, the organisation increases awareness of employees. This is why organisation 7 has the highest zero trust maturity regarding employee training out of the three.

Considering all these factors organisations 1 and 5 had a low performance in the people domain, but organisation 7 had medium maturity especially due to the extensive employee training and documented internal incident management processes.

In the processes domain all three organisations showed low zero trust maturity. When it came to ensuring security of software vendors and their products, all organisations took a different

approach. Case organisation 1 described that when choosing vendors or products, cybersecurity is "always in the back of my mind somehow" reflecting to the fact that those details are considered but that there is no formal process of evaluating security aspects. Case organisation 5 followed the same outsourced path stating that:

> If we get new systems, our IT support—who provides those services—ensures their security because they also install them. So, the expertise lies with them. (Case 5)

This demonstrates the lack of capabilities or processes in place for the organisation itself to assess the security of their software vendors or systems. This leads to higher reliance on a single vendor and does not create capabilities within the organisation. For physical goods or services case organisation 5 only includes security assessments in procurement of products like cameras, but otherwise no. This shows the lack of a procurement process that would include at least some level of security assessment.

Case organisation 7 on the other hand has a procurement process that also included cybersecurity aspects that they described followingly:

> We try to ensure the vendor has proper processes and that the product is secure. We don't have a formal process like a security check, but we discuss these aspects during procurement process and ask vendors to provide a summary of how they ensure security of their products. It's one of the selection criteria, though not a very robust process. (Case 7)

This shows that even though the checks are not the most robust and still relay on the vendors summaries, they include security to their procurement process, which affects the procurement decisions. For physical goods and services, case organisation 7 utilises the same process, where cybersecurity aspects are included in the procurement process and that those aspects are relevant while making decisions.

The organisations differ considerably in their event logging. Case organisation 5 clearly separates itself from the other two with the SOC monitoring and thus comprehensive log collections. Having the monitoring in place, the organisation is constantly searching for anomalies and signs of security breaches before they happen, thus following zero trust principles. For case organisation 1, some logs from certain systems, like their ERP system, are collected and some files have tracking turned on. However, these logs are not analysed and would probably be investigated only in the case of a data breach. Case organisation 7 follows the previous, having logging with their core ERP system as well as with Microsoft 365 environments. However, those logs are mainly used in troubleshooting and trying to make processes more efficient. The organisation also collects VPN

sign-in logs, which they can use to see who has entered their environments. In the end the only organisation from these three using log information following zero trust principles is case organisation 5.

The organisations also differed significantly with their access control policies. Case organisation 5 described their access control policies followingly:

> There's a defined protocol—access rights are assigned to specific credentials, and not everyone has access to everything. (Case 5)
>
> It's both user- and role-based. (Case 5)
>
> Even if someone is the CEO, they don't have access to everything unless it's necessary for their role. So, access is based on the need to know. (Case 5)

This presents access controls based on both roles and persons themselves, but that it follows the principle of least privilege, meaning that users have access to only required information for their duties. This somewhat follows zero trust thinking by limiting the potential breach to smaller given access. However, the access is still static meaning that users have continuous access to the information and a more mature zero trust way of doing this would be with dynamic just-in-time or per case approved access policies.

For case organisation 1 the access policies were very brought. The interviewee stated that:

> Yes, it is almost the case that if the right is ever received, then it will probably not be taken away. So then, when someone leaves away, so then the access is of course reset. But there has never been a need for someone to have their rights removed.
>
> Access is granted to so large entities in a way that are then given to someone. So, someone who has been given access in them, it is then carefully considered so that it does not need to be changed. (Case 1)

This reflects the way many smaller organisations handle their access control policies. The entities that access is granted are very large and often based on duties. This can lead to a wider given access than necessary. Case organisation 7 struggled with the same issue stating that "Yes, though in a small organisation, one user might have multiple roles" referring to their role-based access control. However, the case organisation 7 differs from case organisation 1 by updating the access control policies through formal processes, which they described followingly.

> Firstly, our onboarding and offboarding processes are the most important. Role changes also trigger access updates. There is lot to improve but updating access rights are heavily tied to processes. -- We ensure access is granted, revoked, or modified as with role changes. (Case 7)

Thus, the organisation grants access to smaller areas and updates those accesses when needed. All in all, even with case organisation 5 implementing the principle of least privilege to their access control policies, these do not show mature implementation of zero trust. But for small organisations efficiency often takes priority over security and thus, the organisations often are forced to grant larger accesses than they would want.

The three organisations approached the security of their supply chain a bit differently. Due to being legislated heavily as an energy company, organisation 5 is required to have formal continuity plans for major suppliers and have a cyber supply incident plan in place. Even though required by legislation, this also follows zero trust in the sense that incidents in supply chains should not adversely affect the case organisation. Organisation 1 approached supply chain incident planning from manufacturing perspective and thus, had contingency plans for critical suppliers stating that:

> Something within the quality system is somehow recorded, who are our critical suppliers, for example, and whether we can find backup suppliers for them if necessary. And so on and so forth, but that's mainly for the sake of keeping up the production and not for the sake of information security. (Case 1)

This demonstrates how the focus is on keeping production up, whether it is due to material shortage or a cyber incident affecting the supplier. On the other hand, case organisation 7 stated that they think that their cyber supply chain is isolated digitally that they didn't see risks in it. They stated:

> Yes, we have a documented continuity plan, mostly for external threats like power outages and how we can continue operations in those sorts of situations. (Case 7)

This shows how an organisation operating in manufacturing has suppliers mostly for physical goods, which was also reflected in the fact that their largest perceived threat was a material shortage.

This perception of isolation can also be seen in how these organisations look for vulnerabilities or rather aren't looking for them. Case organisation 5 is the only one of the three that conducts routine vulnerability scan to their network. For case organisations 1 and 7 there was no routine vulnerability scanning, which is likely caused by them feeling that they are digitally isolated and thus, that there is no need for vulnerability scanning.

The processes domain showed differences how these organisations conduct their operations. The processes of the two manufacturing companies (Cases 1 and 7) show that they perceive physical threats larger to their supply chains than cyber related threats. This reflects to how these organisations approach possible vulnerabilities and continuity planning regarding supply chain

resources. Case organisation 5 on the other hand has much more mature processes in network surveillance and proactive vulnerability scanning but since they rely on their suppliers on everything it can't be considered zero trust since there is significant trust placed on those few key suppliers.

In the architecture domain the size of the organisations becomes visible. Out of the three organisations, case organisations 5 and 7 performed segmentation on their networks separating the office network from production or OT networks. For case organisation 5 they are just implementing the segmentation of office networks to behind separate firewalls. For case organisation 7 they stated that their factory and office networks are separated due to automation in the factory, which needs to be protected, thus limiting external access to the factory OT. Organisation 1 didn't have any segmentation in their networks but rather relied on access controls to limit information to selected users.

The ways the three case organisations used encryptions also varied a lot. The interviewees in case organisations 1 and 7 didn't know whether they used encryptions in communication or data, but external connections to the systems in both cases were done via VPN connections meaning that at least external communication is encrypted. For case organisation 5 the interviewee stated that encryptions were done only with data that is subject to GDPR. Also, data stored wasn't encrypted according to the interviewee. Case organisation 5 utilised VPN for external connections similarly to the others making at least external communication encrypted. With external connections case organisations 5 and 7 differed from others. First of all, for case organisation 5, the external service provider controlled all external access meaning that only them could grant the access. But also, their energy grid controlling operations has a significantly more secure architecture since it is completely isolated from external connections. Thus, bringing the zero trust maturity high for architecture domain and overall organisation to a medium level. But since the organisation as a whole is analysed here, it stays medium. Case organisation 7 differs from the others by blocking all outside of Finland connections, unless someone is on vacation. They stated that:

> our operations are heavily localised, so we block all foreign traffic, and it is opened when someone is traveling. (Case 7)

This highlights how a small organisation can leverage its size to protect themselves from many cyberattacks.

The methods for authenticating users also varied between the three organisations. Organisations 1 and 7 utilised MFA if possible. They described their processes followingly:

> We use MFA wherever possible. Our ERP is too old for MFA. Passwords have minimum length and special character requirements for our cloud services and to our Microsoft 356 environment. (Case 7)

> It's (MFA) only for certain applications and certain environments maybe rather than person dependent. (Case 1)

These show that being relatively small organisations, they have systems that aren't supporting MFA but that it is used on those who support it. Case organisation 5 didn't open up their authentication more than that they use passwords for devices and different credentials for the systems. Using MFA on all systems all ways or through dynamic rules would follow zero trust principles but for now since most systems aren't supporting it, the zero trust maturity stays low.

Methods for securing and maintaining endpoint devices also varied. Case organisation 5 relied on the service provider for the EDR solutions and SOC monitoring to secure the endpoints. Case organisation 7 described their process followingly:

> First off all they require authentication. We keep an asset register of all computers which is used to manage and update the systems including the security updates. Phones are not formally registered or managed. (Case 7)

This demonstrates central control for devices and enforcing updates. They also added that an additional antivirus software was included in the devices, protecting them from malware. Case organisation 1 had a similar process where their service provider maintained the devices and installed an antivirus software there. This again reflects the size of the organisations and the fact that organisation 5 is completely reliant on the service provider.

As a conclusion the small organisations that had low zero trust maturity were heterogeneous regarding their processes and ways to secure their organisations. In the people domain the major differences were regarding cybersecurity training and how the organisations planned for cyber incidents. The only aspect in the people domain showing zero trust implementation was case organisation 7 with their continuous training program and open communication about present threats. In the processes domain the major differences were between organisations 5 and organisations 1 and 7 due to the fact that organisation 5 had an external partner providing a SOC log monitoring and routine vulnerability checking. They had also implemented the principle of least privilege in their access control policies. Still, even though there were zero trust principles visible in the process domain, all organisations showed low maturity. The architecture domain also showed some heterogeneity between the three organisations, but all interviewees were similar in the fact that they were not IT-professionals. Thus, for example knowledge about encryption policies was

left vague. However, the organisations differed how they managed their endpoint devices and how they had implemented segmentation to their networks. All in all, the three small organisations with low zero trust maturity where heterogeneous on their approaches to secure their systems and their supply chains. The supply chain for these organisations doesn't present itself as a threat but as a necessity to continue their business, whether manufacturing or selling electricity.

5.1.2 High maturity large organisations (Case organisations 3, 4 and 9)

The three large organisations were very similar in terms of their security conduct event though as organisations they were very heterogeneous being from insurance, retail, and boat manufacturing industries. Also, the company structures differed significantly the first being its own organisation, second being the parent company for a group and the being the local operator of a large global corporate. Due to the large organisation size, cybersecurity management was mostly internal with all organisations, apart from the SOC that organisation 4 had outsourced. The size also affects the cyberattacks that the organisations face. Case organisation 4 reported facing only phishing attacks, but the other two explained that they are also facing identity fraud attempts, fraud attempts, malware, DoS, AI based attacks for case organisation 3 and CNC attacks for case organisation 9. These attacks also reflected to the perceived largest threats to the supply chains, which the organisations described followingly:

> Looking from my own position, the biggest threat is probably data breaches. Losing control of our data. Data falling into the wrong hands, leaking, and if it happens on a large scale, that's a significant threat at some point in the supply chain. (Case 3)

> The entire supply chain. -- Our top threats are phishing, identity threats, and supply chain cyberattacks, followed by system vulnerabilities. That is pretty much the top three that we are fighting against. (Case 4)

> A sabotage or breach targeting those (critical assets) would be the biggest threat. (Case 9)

From these answers a trend can be seen that the large organisations see the supply chain as a source of potential threats.

In the people domain all three organisations showed mature and comprehensive processes. They described their incident response planning followingly:

> We have a security incident process, of which I am the process owner. It is a standardized process from people, processes, and technology perspectives incidents are handled. It includes who handles them, how the process works, and what technologies are used. (Case 3)

> We have a 24/7 CSOC that the entire organisation is instructed to contact if any incidents are detected. Their contact information is also available to our key suppliers. (Case 4)

> Monitoring and management come from the parent company. When something is detected, they start investigating. They have CSIRT teams – involved. (Case 9)

Extensive processes are shown in these answers, which reflects to the size of the organisations, which enables them to have designated teams responsible for cyber incidents. The communication about these incidents seems to be more external than internal, which can be seen from the following quotes.

> We report security incidents regularly, monthly, as part of our reporting. When an incident is ongoing, certain things get specific attention. If it's a more critical incident, we inform certain management groups, like if there's a denial-of-service attack happening, we monitor the situation. (Case 3)

> It depends on the case. If only individual credentials are compromised, there's usually no communication. For larger incidents, we involve communications and, if necessary, the crisis management team (CMT) and IT leadership. (Case 4)

> Internally, yes. Since we have a two-person IT team, we get informed if there's any kind of breach or attempt. But what happens in the rest of the organisation or at the parent company's other locations doesn't really reach us. Of course, if a large third party sends out a mass phishing campaign across the parent company's organisations, we might get a warning. (Case 9)

It seems that the main focus of the communication is external and more reporting style communication rather than warning internal stakeholders that these kinds of threats are currently on. This might be caused by the reporting obligations coming from legislation and contracts, and the will to control the narrative about cyber incidents affecting the organisations, which would be harder if anyone from the organisation could comment on the situation.

The organisations had comprehensive ways on mitigating internal threats. Organisation 3 had included security screenings as part of their onboarding process. They, however, didn't have SOC monitoring like the Case organisation 4, which described their ways as follows:

> HR performs basic checks—identity verification, CV and certificate validation. We don't currently conduct formal security clearances (e.g., from the Finnish Security Intelligence Service), but it's under consideration for certain roles. (Case 4)

> Mainly it (referring to identifying internal threats) is through our network monitoring. The XDR agents collect vast telemetry from workstations. Suspicions are usually reported by colleagues or supervisors. (Case 4)

These promote two ways of identifying internal threats. Doing thorough background checks aims to eliminate bad apples from recruitment processes whereas SOC monitoring is more reactive way of identifying malicious acts in the network.

All three organisations also had invested in regular mandatory cybersecurity training. Organisations 3 and 4 utilised Hoxhunt phishing simulator to create awareness of phishing among employees. Organisation 3 had the most recurring training having micro-trainings every other month, organisation 9 had updates a few times in a year and organisation 4 had training once a year, but they were also looking for alternative more recurring alternatives. This shows a trend towards smaller more regular trainings, which can target specific issues or threats. The benefit from having training more regularly is also the awareness effect where the users are more likely to remember cybersecurity while doing their jobs. On top of those regular small micro-trainings, organisation 3 participated also to cybersecurity month in March, which includes real life examples of past attacks towards the organisation, which should increase the awareness effect since it can feel more personal to the participants.

The people domain in general showed relatively high zero trust maturity for all three organisations, which reflected the size of the organisations, and the possibilities larger resources bring.

The same trend of high maturity continues in the process domain. Procurement processes for all three organisations included cybersecurity assessments. The organisations described their processes followingly.

> Well, our procurement team makes contracts with vendors, and we've provided security requirements. Depending on the vendor and what they do for us, if it involves personal data, there are specific requirements in the data processing agreement. There are technical and process requirements. (Case 3)

> There is a multiphase process. We have a standard set of security requirements that we require for suppliers. All new suppliers or projects go through a data protection/security evaluation process. (Case 4)

> When contracts are made, everything has to go through the parent company's procedures including why they need access, what they'll access, and so on. It all has to be approved in Japan, so the process is long. (Case 9)

These demonstrate how the large organisations rely on processes where they check potential vendors for their security both technical and processual. This shows that the organisations require a certain level of security from their suppliers. This can mitigate the threats coming from the supply chain since at least the tier 1 suppliers and partners have been security vetted. Regarding the

procurement process, interestingly the organisations valued external certifications like ISO differently stating as follow:

> If some vendors have certifications like ISO 27000 or ISO 27018, if they handle personal information, it is OK. It is good that they have audited platforms, but we have our own definitions. (Case 3)

> We also gladly utilize and take into consideration certifications like ISO or SOC 2. Also, if the suppliers have security descriptions, we look into those. (Case 4)

Thus, case organisation 3 does not trust external certifications but rather relies on their own security checks but organisation 4 views certifications more positively placing trust on the certification itself.

The organisations mitigated software related risks through testing the software and by doing regular vulnerability scanning. Organisation 3 described their scanning and testing followingly:

> Yes, we constantly look for vulnerabilities. We have systems that do this daily. We also have a process for identifying issues with new applications or improvements that includes security assessments and vulnerability scanning. (Case 3)

Organisation 4 differed from organisation 3 by having more internal software production, which they described followingly:

> For Internally produced code, our digital development team includes two cybersecurity experts, that are also part of our cybersecurity team. Our responsibility is to drive DevSecOps. The two cybersecurity experts have a guidebook about secure coding practices and use automated code scanners to find vulnerabilities before production deployment. (Case 4)

They also conducted regular vulnerability scanning on their systems and explained that also some external parties are included in this by stating that:

> If they (suppliers) manage a public-facing portal, it’s included in our vulnerability scanning. (Case 4)

These show that the organisation treats both internally and externally produced software like they are vulnerable, thus checking for vulnerabilities regularly after launch and before in the development phase. Organisation 9 similarly to organisation 4 included also external partners to their proactive vulnerability management.

> We use Rapid7, which runs 24/7 and sends alerts about vulnerabilities. Our CSIRT and cybersecurity teams monitor CVEs and send alerts to relevant partners. (Case 9)

This indicates that the global organisation has registries, on what systems which external partners provide to the organisation, and thus are able to monitor both CVEs and regular vulnerability scans reaching also to external partners. These show that all these organisations are proactive when it comes to vulnerability management. Through regular vulnerability scanning and safe development methods the organisations are trying to mitigate the risks rising from software supply chain by implementing zero trust principles there.

Access control policies follow the same path as being heavily controlled by processes with all organisations. The organisations use centralised processes to manage the access control that often varies between roles but can also include dynamic or just-in-time accesses for users rarely needing certain information. This way the principle of least privilege is implemented, which follows zero trust by limiting the information users have access to only necessary.

> We use a role-based access model, granting access based on job duties. Some roles have just-in-time access meaning that the user has access only when those are needed, while others, like the claim's handler, need those accesses daily. It's a wide range. (Case 3)

> They come through group policies or similar mechanisms from the parent organisation. They're user-based, and roles are added as needed. (Case 9)

Having a centralised process for approving accesses also enables the organisations to also audit them, thus making sure that no unnecessary accesses are granted promoting traceability and thus zero trust.

> There's a centralized process for requesting and approving access, with records of who has approved the access and how often reviews are done to granted accesses. Sensitive systems with personal data require reviews twice a year to ensure access is correct. Other systems may have annual reviews. (Case 3)

> When an employee starts, their manager requests access and defines the systems based on their role. Changes in employment status change these access needs and trigger needs but these should also be reviewed regularly. (Case 4)

This shows that these large organisations have implemented zero trust principles into their access control policies but are still balancing between efficiency and security.

Apart from the access control approving logs, the organisations collected comprehensive security logs. These logs were analysed either with 24/7 SOC monitoring or by automated solutions that produced alarms if network traffic anomalies were detected.

> We have automation that processes the logs, normalizes them, and identifies relevant information for our security incident process. We have a product that processes the logs and brings up certain things related to our security incident process. If we need to

> investigate certain things, we can use the platform to investigate those issues. So, there are some manual tasks, but a lot is automated. (Case 3)
>
> Mostly what the XDR agent collects into our SIEM system, which is also used by C-SOC, so it is mainly security log information. (Case 4)

Case organisation 9 characterised their SOC services by stating that "if something happens, they send a message asking, "What's going on? Are you aware of this? Please check ASAP."", which shows how the SOC contacts the IT teams on a low threshold.

The reason organisations collected log details was to maintain their situational awareness and keep track on all current threats and mitigate those appropriately.

> We collect a lot of logs for situational awareness, so we can see what's happening. (Case 3)
>
> Our SOC operates in real-time using XDR and SIEM tools. And for that the tools are for, so that is how our base level SOC operates, so they have a real-time surveillance. (Case 4)

Having the situational awareness and real-time surveillance allows the organisations to implement a zero trust on all network traffic and treat everything as possibly malicious, thus assuming breach at all times.

To protect the critical resources in the supply chains the organisations have contingency and resilience plans. The responsibility of planning can be shared placed on those people using the resources or to central risk management organisations.

> Each platform ensures capacity and contingency planning considering resources. The starting point is that it's part of resilience planning. (Case 3)
>
> We have a continuity management organisation under risk management department, and our IT has its own continuity leads. (Case 4)
>
> Those (contingency plans) come from the Netherlands. The CSIRT team has created notification chains and assigned responsibilities. (Case 9)

These show that the organisations have plans for the critical resources and assets, but they can also approach supply chain related threats through extensive planning, which can include having incident processes in place to mitigate those attacks, communication obligations to suppliers or even playbooks and routine exercises for managing attacks coming from the supply chain.

> If a service provider experiences a security incident, we have a process for handling it. Our security incident process includes detection and response. Our vendors are

> contractually obligated to notify us of incidents. So, we have contingency measures at multiple levels. (Case 3)
>
> C-SERT has playbooks for certain events, but experience has taught us that, no two incidents are the same. Even though they might seem similar, it seems utopistic that you could have a concrete plan for all situations. We do have certain operation models. We conduct regular cyber exercises involving the security team, C-SERT, and IT leadership as a CMT role. These exercises simulate different systems. These exercises often reveal unexpected issues happen not covered in any playbooks. (Case 4)

These contingency plans regarding critical supply chain resources and plans on how to mitigate attacks coming from the supply chain are ways for organisations to implement zero trust principles on how external parties are managed and cooperated with to manage the threats in the supply chain.

The processes in these large organisations show mature zero trust implementations, even though there is always room for development and improvement. Importantly the risks coming from both software and physical supply chain were mitigated through checking both the suppliers and their software, collecting extensive logs that are used to detect attacks in real time.

The architecture domain containing mostly technical enterprise-wide solutions and configurations reflects the size of the organisations and their capabilities but also their needs to protect their environments. Network micro-segmentation was used to divide the networks of the organisations to mitigate the effects of possible breaches and to limit the access users had in the network. This was shown in policies like:

> Some services are micro-segmented even at the server level, others at the system or subnet levels with controls in between. Then there are larger networks, like office networks, which are not micro-segmented at the host level. (Case 3)
>
> There is segmentation, but more could be done. So, it is not fully micro segmented. Office, IoT, and device networks (e.g., payment terminals) are fully separated. There's less segmentation within the main office network. Suppliers have their own networks and inside there their own segmentations. (Case 4)

Thus, the organisations utilise micro-segmentation through a risk evaluation where less risky networks are not as segmented as the more critical networks. This shows the balance of efficiency, ease of implementation but also security. Micro-segmentation was also used to limit the possible consequences of supply chain related incidents since vendors only had access to their own segments containing the consequences in that specific segment.

Encryption practises also illustrated the capabilities of large organisations in both communication and storage. Following zero trust all communication and all data in storage should be encrypted to mitigate data breaches. These three case organisations utilised encryptions followingly:

> Starting from, encryption at rest, encryption in transit. It's part of Zero Trust, encrypting everything and authenticating everything. It's also a regulatory requirement. We have been under DORA legislation since January, which requires encrypted communication for both internal and external networks. (Case 3)

> It depends on the use case. Generally, all traffic is encrypted. All external traffic is encrypted. Data is encrypted based on demands. Data classification and personal data handling guidelines dictate encryption levels. (Case 4)

> Our endpoints are encrypted. USB drives are banned unless encrypted. If something goes wrong, your account is locked, VPN access is cut, and you're disconnected. In principle everything is encrypted in a way that you don't notice it unless something breaks. (Case 9)

Here the policies differ between case organisation 3 and the other two. Case organisation 3 follows zero trust principles and also legislation by encrypting all traffic and data whereas case organisation 4 follows a risk-based approach where all important and critical information are encrypted in communication and in storage. For case organisation 9 their parent companies are handling the encryptions, but at least external communication is encrypted for them due to the use of VPN.

Technical access control is the method the organisations use to identify and authenticate their users. This way the confidentiality of information can be secured since users accessing the information have been properly authenticated. The three top high maturity case organisations elaborated their policies followingly:

> Centralized. We have centralized identity providers for authentication and centralized access management that we discussed earlier, but centralized system. It (MFA) is mandatory for external access. (Case 3)

> We use both MFA and single sign-on. Everything goes through Microsoft Entra ID. MFA is enforced for all users, with risk-based rules depending on login context. (Case 4)

> MFA is required by the parent company. Some systems still require daily authentication, but Office can be set to not ask for 90 days. In some factory settings, shared accounts might not support MFA, but those are categorized as risks and acknowledged as there is no better way. For example, our ERP is accessed via Citrix which you can use to open the ERP. The portal logs you out after 15 minutes, and you need to re-authenticate with MFA. It depends; some systems are more annoying than others. (Case 9)

All these demonstrate centralised access management where however MFA is used differently. For all organisations external connections always required MFA but for case organisation 4, dynamic policies were used to determine when MFA was required. For case organisation 9 MFA usage was platform and system dependent. Thus, there were three different ways of utilising MFA.

Endpoint devices are often the source for cyberattacks into large organisations, thus making securing them critical for large organisations with thousands endpoint devices. To mitigate these risks these organisations had devices centrally managed, thus monitored in different ways.

> We have various security controls depending on the device: MacBook, iOS, Windows, Linux, and others. There are different requirements and controls to ensure the device, and its intended use are secure. (Case 3)
>
> All devices are managed by IT. Laptops and workstations have XDR agents installed, which are key tools for CSOC. (Case 4)
>
> We use Rapid7, Trend Micro, Zscaler, and firewalls. Rapid7 scans continuously. Phones can't access systems unless their IMEI, and serial number are sent to Japan and approved. Even then, access is limited to Intune-corporate portal which prevents data copying from your device to the company. There's zero trust to the devices. (Case 9)

These methods are used to support the real time SOC or automated log monitoring. Together these methods mean that the devices are kept updated and centrally managed, which enables containing possible incidents to small segments or only few devices.

Securing external access has a large effect on the security of organisations due to limiting attacks like eaves dropping or Man-in-the-middle attacks. Thus, these organisations have strict policies on how external access to the systems is done.

> All connections are encrypted and authenticated, the ways for encrypting are SSH, IPsec and TLS and MFA are used to authenticate users, but we aren't using IPsec for everything. We use also TLS and SSH encryptions. (Case 3)
>
> We use a partner VPN tunnel, opened per supplier and if there is need for access. Access is workstation-specific, purpose-limited and system limited. The access is carefully limited where each supplier is allowed in. (Case 4)
>
> The suppliers that have access use accounts with MFA managed by us. It is for logging these sign ins and possibly identifying if something out of the ordinary is happening there. (Case 4)
>
> Very few, if any, external users can access our network. The access is granted in segments, if someone needs ERP access, they get access through Citrix. For things like boat schematics, we whitelist IP addresses. Same for databases. (Case 9)

Securing external accesses, thus limiting the cyber supply chain threats, the organisations used encrypted communication channels to complement the micro-segmentation, monitoring log information, and access control policies. The architectures showed high maturity arching from large organisational policies regarding technology usage in network structure, encryptions, access control policies and securing the endpoint devices.

As a conclusion, these managerial, architectural, and processual solutions together are able to mitigate risks and possible damages caused by the cyber supply chain. From all three domains a high zero trust maturity could be seen, which reflects the higher demands that large organisations have for their cybersecurity but also their capabilities to invest in security.

5.2 Cross-group comparison

In this chapter a cross-group comparisons are conducted, first between small organisations with high or medium ZT maturity and those with low ZT maturity. Second comparison is between large organisations with high or medium ZT maturity are compared to large organisations with low ZT maturity, and finally comparison between large and small organisations in general is conducted.

5.2.1 Small organisations with high or medium zero trust maturity compared to those with low maturity

In the study two small organisations were found to have higher zero trust maturity than low. Case organisations 2 had high maturity whereas case organisation 6 had medium maturity. Case organisation 2 operates in logistics sector whereas organisation 6 operates in industrial manufacturing. Case organisation 2 was one of the smallest organisations with 25-50 employees and case organisation 6 was one of the largest small organisations with 400-500 employees. These represented both ends of the spectrum when it comes to number of employees in small organisations. Case organisation 2 had outsourced the technical security but handled management internally. Similarly, case organisation 7 had outsourced services like the CSOC but kept the management internal. All of this was very similar to the low performing, small organisations (1, 5 and 7). However, looking at the cyberattacks that the organisations had faced there was a difference. The two better performing case organisations described past cyberattacks followingly:

> We’ve had denial-of-service attacks, data leaks in the supply chain, and various minor incidents. (Case 2)

> We’ve had phishing and exploitation of vulnerabilities—those are the most common. (Case 6)

Whereas the three worse performing organisations reported only having phishing or no attacks at all. This shows that the better performing organisations also faced more, and more severe cyberattacks than the others, or at least they were aware of these attacks. This also reflected into the perceived largest threats to the organisations' supply chains, which the better performing organisations named to be low level Microsoft o365 attacks or leaked credentials giving access to digital environments, compared to the two of lower performing organisations naming physical threats like global shutdowns or material shortages as the greatest threats. Thus, the organisations with the higher zero trust maturity levels perceived digital threats as more dangerous than the lower performing organisations.

In the people domain, the differences regarding zero trust maturity were shown mainly through more extensive and updates security incident processes and more thorough background checks. On the other hand, all organisations had similar both internal and external communication about security incidents.

The better performing case organisations 2 and 6 elaborated their security incident processes followingly:

> We have a management model starting with process descriptions and policies, down to user guides and documentation forms. There are two levels of forms: one for end-user incident reporting and another for managing the incident itself, which also forms internal documentation automatically. (Case 2)

> We have a process in place. When a breach is identified, we classify its criticality and assess its severity. We aim to mitigate the issue as soon as possible, isolate it, and then investigate the root causes and how to prevent them in the future. (Case 6)

These present clear processes that for case organisation 2 demonstrate a top-down approach where the process is not only about handling the incident but also documenting it. Case organisation 6 on the other hand shows an in-depth process where documentation is also used to find the root causes, thus blocking similar attacks in the future.

The low performing organisations generally described their way of handling cyber incidents as more communication or law based:

> That, at least we communicate in the company that something like this happened and then we may inform also to the service provider 1 that there is something like this. (Case 1)

> According to the law. We've all been trained, and we have ongoing training, especially on GDPR. (Case 5)

This shows the different approach on handling cyber incidents in high and low performing organisations. The better performing organisations demonstrate zero trust maturity by having a clear process in place that show two goals. Firstly, mitigating the attack in hand, but secondly identifying root causes and producing documentation to improve the organisations security posture in the future. For the low performing organisations, the results reflect the fact that the knowledge on handling the incidents is not in the organisation and, thus the goals are more communicating or following the law.

Regarding background checks, organisation 2 being the only one having a high zero trust maturity, differed from the rest. They stated that: *"We conduct security clearances through the national security agency for anyone accessing critical systems."* (Case 2). Thus, all users have been formally checked allowing the organisation to protect themselves from internal threats, at least when hiring. The other small organisations stated that they aren't doing any background checks or only the basic checks to verify that users are what they claim they are.

The cybersecurity and awareness training showed very heterogeneous practises that ranged from case organisation 2's and 7's regular and extensive trainings to case organisation 1's almost non-existent training. Case organisation 5 had regular cybersecurity training but the focus on those trainings were more on legislation like GDPR and for case organisation 6, the training was annual and due to large time interval, the effect of the training can be lost during the year.

In the people domain the differences between high, medium, and low zero trust maturity were mainly the result of either robust security incident processes or background checks. The organisations were similar in terms of communicating about security incidents having both internal and external communication whereas their security and awareness training varied a lot.

The process domain showed more variety compared to the people domain with the differences being in procurement processes, log collection and analyse and vulnerability scanning. During the procurement process, performing security checks and scans, it is possible to identify possible vulnerabilities and "bad apples" in suppliers. Case organisation 2 approached this with software vendors by:

> Our ISO 9000 requires us to use a safety appendix in contracts. For significant suppliers, we require ISO 27000. The appendix allows for scanning and audits when needed. Regular audits haven't been done, but occasional checks have been done. (Case 2)

This shows certified processes in the case organisation itself guiding a documented way of evaluating suppliers. Having a contractual base to conduct security checks, enables the organisation to continuously monitor its suppliers and verify their security claims, thus demonstrating zero trust principles. With physical goods the organisation 2 elaborated further that *"but for smaller purchases, price often takes priority."* (Case 2), which shows that the process can be flexible with small purchases that only have a minor influence in security. The other small organisations described their procurement processes followingly:

> We assess the criticality of the system or service, both from availability of the system and the criticality of information the system houses. And depending on the level, if it's not significant, like buying a phone, no security assessment is done. For critical systems, we check certifications and if the vendor doesn't have them, we use our own security questionnaire to evaluate if our information security requirements are fulfilled. (Case 6)

> We try to ensure the vendor has proper processes and that the product is secure. We don't have a formal process like a security check, but we discuss these aspects during procurement process and ask vendors to provide a summary of how they ensure security of their products. It's one of the selection criteria, though not a very robust process. (Case 7)

> If we get new systems, our IT support—who provides those services—ensures their security because they also install them. (Case 5)

Case organisation 6 comes close to the organisation 2's level but lacks the auditing of the suppliers. However, they demonstrate a robust process where vendors of critical systems and physical components are either required to have certifications or to answer a security questionnaire, to determine their security protocols. For the case organisation 7 and 5, the process is either not robust or non-existent. This leaves the two organisations susceptible for possible vulnerabilities coming through the suppliers. Thus, the procurement process of case organisation 6 demonstrates medium level zero trust maturity and case organisations 5 and 7 show only low maturity.

Monitoring security log information is one key method for organisations to maintain situational awareness about their security. To be helpful these logs need to be gathered but also analysed in real time to enable identifying breaches proactively. Case organisations 5 and 6 used SOC services to monitor these logs whereas organisation 2 relied on automation to detect anomalies in the logs. Both of these are ways of identifying the network traffic anomalies that can be malicious, but the SOC service can be more costly since it requires personnel to be monitoring the traffic 24/7. Case organisations 1 and 7 differed from the rest by only logging some information and by not analysing it in real time. This allows the organisations to only reactively utilise the logging information to find

causes for security incidents, but they can't be used to stop the incidents from happening. Thus, the three first organisations show higher zero trust maturity when it comes to log information than the two latter.

Similarly to the log usage, the three organisations performing well there also did routine vulnerability checks whereas the case organisations 1 and 7 did not. Vulnerability scanning is an essential tool for organisations to proactively secure their networks because it allows organisations to find possible weak spots before they can be exploited by attackers. For organisations 6 and 7, the vulnerability scanning was part of their SOC service whereas organisation 2 performed the scanning themselves. Thus, both organisations that had higher than low zero trust maturity performed regular vulnerability scanning, which positively influenced their maturity level.

Access control policies in small organisations in general varied a lot. Generally being small organisations, given access was static, and role or person based. Organisations faced challenges due to broad roles or persons having multiple roles that was elaborated as *"though in a small organisation, one user might have multiple roles. "(*Case 7). For most organisations, granting access was tied to processes, like on- and off-boarding and changes in roles. These accesses were monitored and updated by organisations 2, 6 and 7 which described this followingly:

> Our systems have defined owners who are responsible for access management, which means that they need to know who has access to their systems and oversee it from there. We have an annual centralized review process. (Case 2)
>
> When someone joins, we define their access level. Changes are made through role updates and always require approval from their supervisor. If it is to a specially defined spaces, the spaces owner's approval is needed to establish access to that space. (Case 6)
>
> Firstly, our onboarding and offboarding processes are the most important. Role changes also trigger access updates. We're a small organisation, so we don't need extensive needs to maintain anything. We ensure access is granted, revoked, or modified as with role changes. (Case 7)

Thus, the organisations are monitoring their access and updating those in formal processes unlike case organisation 1, who described their access control policy management *"Access is granted to so large entities in a way that are then given to someone. So, someone who has been given access in them, it is then carefully considered so that it does not need to be changed."* (Case 1). This is a stark contrast to the others. It can be due to people having so broad roles, that they need large access, or that information is not classified enough, making following principle of least privilege hard.

Thus, in the process domain, the organisations with the higher maturity, had more robust processes that controlled procurement and access controls, but they also secured their networks with log analysing and with regular vulnerability scanning.

The architecture domain shows largest differences between the organisations with higher maturity (Cases 2 and 6) and the rest. Case organisation 2 stated that their network is micro-segmented whereas the other organisations described their network segmentations followingly:

> We're in the process of segmenting. Tomorrow, the office will be moved behind a separate firewall. (Case 5)
>
> It's segmented, but not micro segmented. Our segmentation is more based on usage. (Case 6)
>
> We've separated the factory and office networks. The factory runs in its own segment, and the office in another. (Case 7)

While segmented these organisations did not have micro-level segmentation and organisation 1 did not have practically any segmentation. This reflects the size of the organisations and their possibilities to have extensive micro-segmentation.

Encryption practises also differentiated case organisations 2 and 6 from the rest. They characterised their practises followingly:

> Our network to the data centre runs on private fibre, so no encryption at that level. Critical traffic is encrypted point-to-point with our own PKI and certificates. (Case 2)
>
> Generally critical data should be encrypted, but not all technologies support it, so it's not everywhere. Same (with communication), it's recommended in our guidelines that encrypt communication, but it is not always feasible everywhere. (Case 6)

These indicate that all traffic and data are generally encrypted, but with case organisation 6, not all systems are yet supporting it, but the general approach is that everything is encrypted. This mindset differs from the rest. Case organisation 7 didn't have the knowledge to explain their encryption practises whereas case organisation 5 characterised their practises followingly:

> Nothing is encrypted. If someone accesses a device, they can find everything. – (Communication is) mostly unencrypted. If we handle data that must be encrypted, then we do encrypt it. (Case 5)

This shows that either the interviewees didn't know about the encryption practises about their organisations, or their approach to encryption is motivated by legislation and only necessary data is encrypted.

To authenticate users, organisations utilised MFA varyingly. Case organisations 2 and 6 used dynamic policies for requiring MFA. This was also linked to a central access management solution, which enables more accurate access management for the organisations. This shows zero trust implementation due to always authenticating users. For case organisations 1 and 7 used MFA on only some systems. This reflects the size of the organisations, since their small size doesn't allow them to use only new software systems, which would allow MFA. Case organisation 5 only used password authentication, which is not ideal and brings possible vulnerabilities. Thus, the high and medium zero trust maturity organisations differed from the others through centrally controlled and dynamically authenticated logins.

Finally in the architecture domain the organisations used different methods for securing their endpoint devices. Case organisations 2, 5 and 6 used EDR solutions that were connected to their automated network anomaly detection systems or SOC services. This way all endpoint devices were constantly monitored, which showed zero trust implementation since the endpoint devices are not trusted and constantly monitored. Case organisations 1 and 7 used merely antivirus software on their centrally managed devices, but those devices were not managed actively.

Thus, it can be concluded that case organisations 1 and 6, which had high or medium zero trust maturity overall, differed from the low maturity organisations by having strong and robust processes in place, by having background checked and properly trained employees and through having a secured network with proactive surveillance.

5.2.2 Large organisations with high zero trust maturity compared to large organisations with medium maturity

In this study there were four large organisations, case organisations 3, 4, 8 and 9. Case organisation 8 was the only one of those having medium zero trust maturity, whereas the others had high maturity. Case organisation 8 was also clearly the smallest of the bunch, barely crossing the threshold of 500 employees to be considered a large organisation in this study. Case organisation 9 itself was a smaller company but because they were part of a large international corporation, they were considered to be a large organisation.

All four organisations handled the majority of cybersecurity management internally, with the most outsourced things being SOC for case 4, and network management and SIEM implementation for case 8. Thus, the smallest organisation had also the most outsourced, which reflects the capabilities of larger organisations that have cybersecurity teams that are able to take on these kinds of projects.

In the people domain the maturity becomes apparent from the start. When diving into how these large organisations handle incident response planning, heavy process dependency can be seen. The organisations disclosed their practises followingly:

> We have a security incident process, of which I am the process owner. It is a standardized process from people, processes, and technology perspectives incidents are handled. It includes who handles them, how the process works, and what technologies are used. (Case 3)

> We have a 24/7 C-SOC that the entire organisation is instructed to contact if any incidents are detected. Their contact information is also available to our key suppliers. (Case 4)

> We have a dedicated cybersecurity team. Depending on the nature of the breach, we also involve a few external experts. (Case 8)

> Monitoring and management come from the parent company. When something is detected, they start investigating. They start bombarding different departments and begin the investigation. (Case 9)

This shows that case organisations 3 and 8 are handling the incidents more internally compared to the other two, but for organisation 8, there seems to be a lack of knowledge for handling major incidents. This compared to the incident process in organisation 3, shows a lower maturity since there are no clear roles in the process due to some of them being external people. Case organisation 4 on the other hand relies in its SOC partner to detect and mitigate security incidents similarly as case organisation 9 relies on the parent organisations CSIRT teams. However, it is interesting to note that case organisation 4 also involves their external suppliers with their SOC by instructing the suppliers to contact the SOC in cases of incidents. This shows an effort of controlling the risks coming from the supply chain.

For mitigating internal threats case organisations 3, 4 and 8 conducted varying background checks or had the contractual base to conduct them and all of them used either SOC or automated IDS systems, which allowed them to mitigate the risks of internal threats. Regarding background checks the organisations stated that:

> Yes, it's part of the onboarding process. Different countries have different laws, as we operate in seven countries. We conduct background checks, sometimes through national security agencies, depending on the country's regulations. (Case 3)

> HR performs basic checks—identity verification, CV and certificate validation. We don’t currently conduct formal security clearances (e.g., from the Finnish Security Intelligence Service), but it’s under consideration for certain roles. (Case 4)

> Only if they receive higher-level admin credentials. It's stated in our contracts that background checks can be done. But our current staff has been with us long enough that we haven't seen the need to do it to them. (Case 8)

This highlights that case organisation 3 operating on the insurance field, thus handling more personal details, had the most robust background checks, whereas case organisation 4, operating in retail, checked mainly that the employees are who they say they are. They also recognised the possible benefit of formal background checks regarding critical positions. Case organisation 8 was one step behind the previous by only having the possibility to conduct background checks on employees that have higher level access. However, being the smallest organisation in this group, organisation 8, shows traits of those smaller organisations by having familiarity between employees and thus, trust.

All organisations had similar means of cybersecurity and awareness training. Training was included both in the onboarding process on top of regular mandatory trainings for all users. The following descriptions about these processes were given:

> Additionally, we conduct security awareness training annually, especially during Cyber Month in October. In the past couple of years, we've had sessions explaining the types of incidents we have faced, so everyone can learn to recognize those attacks. We train users awareness to both recognize and report attacks, and there are micro-trainings. We conduct phishing training -- for all employees. (Case 3)

> Through annual web-based training, which is a bit stiff, though we're exploring alternatives. We also continuously use Hoxhunt platform for phishing simulations. It simulates phishing messages that are sent to employees and then statistics are collected about how employees react to those. Some gamification and it can be used to share smaller awareness campaigns regarding cybersecurity. (Case 4)

> We run continuous phishing simulation training which is this data breach training that is ongoing for everyone, and it also includes these small information packages, related to information security. The awareness training is ongoing for everyone and then we have had some mandatory Teams trainings. Our onboarding trainings are mandatory for everyone. Employees must complete this security onboarding in order to receive a device like a phone. (Case 8)

> It comes all the way from Japan. There are a couple of hours of training when you start and then updates a few times a year. It's a lot, maybe too much if you're not into IT or don't know much about it. It can be an information overload. And there are tests afterward, so you can't just click through. It takes a couple of workdays to complete everything. (Case 9)

These demonstrate similar practises between organisations. All organisations conducted the trainings through internet and not in person. Similarly, between the organisations, the training included micro trainings around the year focusing on different information security aspects like

recognising phishing attacks. However, case organisation 3 differed from the others participating in the cybersecurity month in October and showing users real life examples of attacks targeting the organisation. This is likely to cause more awareness due to the fact the users see that their training has a purpose.

As a conclusion, all four organisations had very similar practises regarding the people domain. Even though they differed between internal and external incident management, they all had processes to follow. They also had controls in place to mitigate internal threats through background checks or network monitoring, and they all had regular and mandatory cybersecurity and awareness training for all users.

The differences between the three high maturity organisations and case organisation 8 with medium maturity are larger compared to the people domain. Starting from the procurement processes the three high maturity organisations described their processes as follows:

> Our procurement team makes contracts with vendors, and we've provided security requirements. Depending on the vendor and what they do for us, if it involves personal data, there are specific requirements in the data processing agreement. There are technical and process requirements. It depends vastly on the vendor. We have critical vendors with regular follow-ups and naturally more requirements. Then we have really small vendors, who only supply small things, so the requirements definition is a little smaller. But in general, it's a process with our own specifications. (Case 3)

> There is a multiphase process. We have a standard set of security requirements that we require for suppliers. All new suppliers or projects go through a data protection/security evaluation process. We use a template with specific questions for the purchasing party. (Case 4)

> When contracts are made, everything has to go through the parent company's procedures including why they need access, what they'll access, and so on. It all has to be approved in Japan, so the process is long. (Case 9)

These clarify that these organisations have defined requirements for vendors security practices, that either are same for all vendors or differ based on their criticality. Case organisation 3 has also included follow-ups with critical vendors, which show the implementation of zero trust principles since then those vendors' security practises are regularly checked, mitigating the supply chain risk. Case organisation 8, however described their process followingly:

> We rely on contracts and NDAs that need to be taken care of. It is a bit forming at the moment how we make contracts with suppliers since we're currently building an ISMS. (Case 8)

This, on the other hand shows that the process is not as rigorous, but the direction is towards a more robust process.

Case organisation 3 also differed from the rest by how certifications are considered in the procurement process. Case organisations 3 and 4 described it as follows.

> If some vendors have certifications like ISO 27000 or ISO 27018, if they handle personal information, it is OK. It is good that they have audited platforms, but we have our own definitions, where we receive different certifications from our vendors. (Case 3)

> We also gladly utilize and take into consideration certifications like ISO or SOC 2. Also, if the suppliers have security descriptions, we look into those. However, if none are available, and the purchasing party is adamant that we need to choose that vendor, we conduct interviews with the supplier about how they maintain cybersecurity. (Case 4)

This difference where case organisation 3 does not trust the fact that organisations are certified and rather conducts their own security checks to possible vendors shows a more zero trust way compared to case organisation 4, which accepts the certifications and if those are non-existing, they conduct their own checks, thus implicating zero trust since no trust is placed on external parties.

Internal software production also showed some differences how organisations approached the security of self-made software. Case organisation 4 and 8 described their process followingly:

> For Internally produced code, our digital development team includes two cybersecurity experts, that are also part of our cybersecurity team. Our responsibility is to drive DevSecOps. The two cybersecurity experts have a guidebook about secure coding practices and use automated code scanners to find vulnerabilities before production deployment. (Case 4)

> … our subsidiary does automation software for OT environments -- It is a marginal part of our business, but yes, we do have some internal software development. -- In them the security testing is mostly functional, and cybersecurity doesn't hold a major role there. (Case 8)

This shows the clear difference between secure developing methods, which implement at least some level of zero trust into self-made software as compared to software that has tested only to test functionalities of the software, overlooking the cybersecurity testing leaving possibilities for vulnerabilities.

All four organisations collected comprehensive log details that they all analysed proactively. The difference between these organisations was that case organisations 3 and 8 relied on automated IDS system producing alarms of network anomalies whereas the other two had implemented either

internal or external SOC service, which increases the zero trust maturity due to constant monitoring. This reflects well the size of the organisations since their vast resources enable proactivity and comprehensive logging.

Similarly, all organisations conducted regular vulnerability scanning. This allows organisations proactively find vulnerabilities, thus placing no trust in them. These scans were done daily for most organisations, and they were also expanded to external actors as well. The organisations described this followingly:

> Yes, we constantly look for vulnerabilities. We have systems that do this daily. (Case 3)
>
> If they (Suppliers) manage a public-facing portal, it's included in our vulnerability scanning. (Case 4)
>
> We try to find vulnerabilities in our own systems by vulnerability scanning. We've done some checks on key partners using public sources and IP scans. (Case 8)
>
> We use Rapid7, which runs 24/7 and sends alerts about vulnerabilities. Our CSIRT and cybersecurity teams monitor CVEs and send alerts to relevant partners. (Case 9)

This shows that the scans are done daily and also expanded outside of the organisations themselves. This increases zero trust maturity because no systems, own or vendor, are trusted to be secure and thus are proactively checked for possible vulnerabilities.

The access control policies of the organisations showed some differences, but generally all four organisations relied on role-based access control policies that were tied to processes like on- and off-boarding and changes in roles. Most of the organisations used a central management system and single sign-on to verify users. The organisations described their policies followingly:

> Centrally, with approval processes. As an example, for business systems, there's a centralized process for requesting and approving access, with records of who has approved the access and how often reviews are done to granted accesses. Sensitive systems with personal data require reviews twice a year to ensure access is correct. Other systems may have annual reviews. We use a role-based access model, granting access based on job duties. Some roles have just-in-time access meaning that the user has access only when those are needed (Case 3)
>
> We have a dedicated IAM team with a centralized tool for managing and monitoring access. -- It is role-based. When an employee starts, their manager requests access and defines the systems based on their role. Changes in employment status change these access needs and trigger needs but these should also be reviewed regularly. (Case 4)
>
> (We manage access) Through Intra ID, managed by our internal staff. The starting point is role-based access. (Case 8)

> We have a two-person IT team, so most of it (access controls) comes from the *parent organisation*. They're user-based, and roles are added as needed. If we have an issue, we send a message saying something is missing or needs access. (Case 9)

These demonstrate central management that is used to control the access controls. The central access management allows monitoring who has access and who has granted that access. This allows for better zero trust implementation since all access should have a reason behind them and log trails are being audited regularly. For most organisations, the starting point is role-based access, but for case organisation 3, there is also usage of just-in-time accesses. This increases the zero trust maturity since it can be used to allow access to information strictly based on the information needs, especially in critical systems and with rare information needs. Thus, the centrally managed access controls allow monitoring, thus showing some level of zero trust, but it can be further increased by using for example just-in-time accesses.

The organisations had varying means of maintaining continuity and security of critical components in their supply chains and protecting themselves from attacks targeting the supply chain.

> Each platform ensures capacity and contingency planning considering resources. The starting point is that it's part of resilience planning. (Case 3)

> If a service provider experiences a security incident, we have a process for handling it. Our security incident process includes detection and response. Our vendors are contractually obligated to notify us of incidents. So, we have contingency measures at multiple levels. (Case 3)

> Yes, we have a continuity management organisation under risk management department, and our IT has its own continuity leads. (Case 4)

> C-SERT has playbooks for certain events. We conduct regular cyber exercises involving the security team, C-SERT, and IT leadership as a CMT role. These exercises simulate different systems. These exercises often reveal unexpected issues happen not covered in any playbooks. (Case 4)

> We have listed them, and the most critical ones are known, but the work is ongoing. We have to do a contingency plan especially for backups and such. Plans are being developed. (Case 8)

> We have some plans for incident management, but they're still in progress. In our IT systems supply chain, many things can happen. In our production supply chain, if something goes wrong, we usually just cut off access to our environment if misuse is detected. (Case 8)

> (Contingency plans) come from the Netherlands. The CSIRT team has created notification chains and assigned responsibilities. (Case 9)

> It's quite difficult for anything to reach us that way. Access is very restricted. Even if someone has credentials, they can't access the internal network without our device. So, the chances of a third party breaching our systems are very limited. (Case 9)

These quotes show that organisations 3 and 4 have identified critical resources in their supply chains and have created contingency plans for them. For organisation 3, the responsibility and accountability of that planning is decentralised to the different platforms, whereas in organisation 4 there is a risk management department that handles most of the planning with some done by IT continuity leads. Organisations 8 and 9 have improved their planning due to NIS-2 implementation and thus especially for organisation 8, the work is still in progress. The organisations viewed the external threats a bit differently. Organisation 3 used their security incident process that includes also threats coming from the supply chain, whereas organisation 4 has a playbook with some protocols for attacks targeting the supply chain. The also performed yearly exercises to practise protecting these resources. Organisation 9 differed from this by trusting their tight access controls ranging to the external systems, thus trusting that they are secure enough. Thus, it can be said that organisations 3 and 4 have taken the contingency planning and securing critical supply chain resources further than the latter two.

The process domain showed some differences between the organisations especially with the procurement of IT systems and with secure development practises. The processes did reflect the size of the organisations, which was shown with centralised controls like access management and with mature services for security log analysing and vulnerability scanning. The key differences separating organisation 8 from the rest were the procurement processes, secure development and securing critical supply chain resources.

The architecture domain showed the least differences between the three organisations. One of the key differences was with micro-segmentation, which showed differences between organisations 3 and 4 compared to organisation 8.

> Some services are micro-segmented even at the server level, others at the system or subnet levels with controls in between. Then there are larger networks, like office networks, which are not micro-segmented at the host level. (Case 3)

> There is segmentation, but more could be done. So, it is not fully micro segmented. Office, IoT, and device networks (e.g., payment terminals) are fully separated. There's less segmentation within the main office network. Suppliers have their own networks and inside there their own segmentations. (Case 4)

> Building network systems are on separate networks, and we have a dedicated backup network for our production environment. (Case 8)

This shows that even though their systems are not fully micro-segmented, all critical systems for organisations 3 and 4 have been micro-segmented, unlike with organisation 8, which has only segmentation for building networks and operational production equipment. Micro-segmentation can be used to implement zero trust by limiting the areas users are permitted, thus mitigating consequences of possible attacks.

Organisation 8 differed also from other large organisations trough their encryption policies.

> Well, we're currently classifying data. All communication channels are encrypted, and backups are encrypted. All endpoint device hard drives are encrypted. Encrypted messaging is mainly used by the data protection team, but we're continuously moving towards having encryptions in also other file formats and data. (Case 8)

> Starting from, encryption at rest, encryption in transit. It's part of Zero Trust, encrypting everything and authenticating everything. It's also a regulatory requirement. We have been under DORA legislation since January, which requires encrypted communication for both internal and external networks. (Case 3)

Even though they have the capabilities to encrypt messaging, but all data is yet to be encrypted. This separates them from the other organisations whose baseline is to encrypt everything whether in transit or in storage.

Securing endpoint devices didn't show large differences with organisation 8 compared to the others.

> Even phones are under our control via Microsoft Intune, so we can wipe them remotely. Endpoint devices use BitLocker, Windows Hello and MFA. On top of those they also have antivirus, browsing protection, firewalls, and XDR services. (Case 8)

> All devices are managed by IT. Laptops and workstations have XDR agents installed, which are key tools for C-SOC. (Case 4)

This shows that the organisations were similar by having centralised endpoint device management and used XDR tools to monitor anomalies in them, thus showing zero trust implementation with no trust to the device itself.

To authenticate users, organisation 8 used MFA, but the methods differed from the others like organisation 4, since those organisations utilised more dynamic controls, which determine the methods for authentication.

> MFA is the de facto. Trusted devices are recognized, but generally, MFA is used for every login. (Case 8)

> We use both MFA and single sign-on. Everything goes through Microsoft Entra ID. MFA is enforced for all users, with risk-based rules depending on login context. (Case 4)

Thus, the dynamic access control policies show more zero trust implementation because with dynamic access control rules, no device is automatically trusted, but it depends on multiple variables.

To secure external access to systems, organisation 8 utilised limited access to information through MFA authentication, thus making it possible for them to keep logs of external accesses. This was similar to case organisation 3 who also required MFA and limited the places external users can access.

> The access is carefully limited where each supplier is allowed in. And well. The suppliers that have access use accounts with MFA managed by us. It is for logging these sign ins and possibly identifying if something out of the ordinary is happening there. (Case 8)

> We have defined methods for providing public services meaning how we identify users, of course MFA is used and to what resources the access is granted. (Case 3)

Thus, in general the key differences between organisation 8 and other large organisations within the architecture domain lied in the network segmentation, encryption policies, and access control. However, there were also many similarities like in external access and with securing endpoint devices.

As a conclusion the key differences separating case organisation 8 from the high maturity large organisations in the people domain were in incident handling, in the process domain in procurement and software development processes and in the architecture domain with network segmentation, encryption and access control.

5.2.3 Large organisations compared to small organisations

In general, as shown in figure 6, large organisations had higher zero trust maturity than smaller organisations, with then only exception being the small organisation 2 with high maturity that was higher or equal than the large organisations. This is probably caused by lack of resources for cybersecurity or IT in the smaller organisations leading to more outsourced approach and thus, less capabilities inside the organisations themselves.

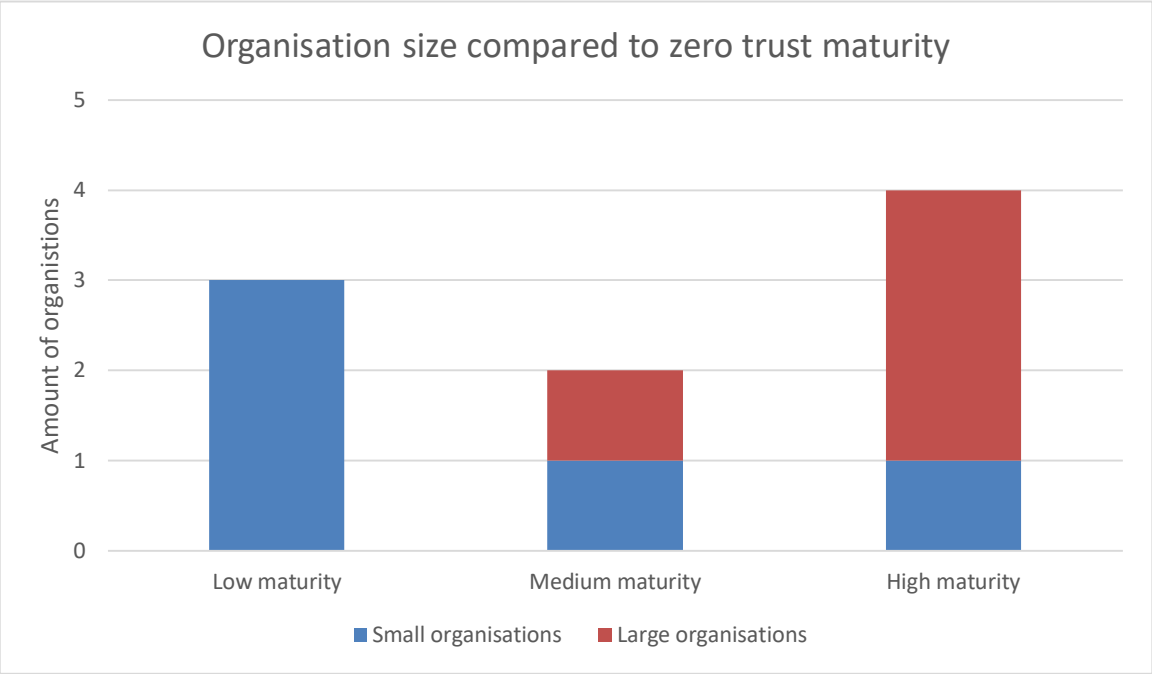

Figure 6 Organisation size compared to ZT maturity

In the people domain the large organisations had more robust processes for handling cybersecurity incidents, whereas with smaller organisations they relied on external professionals and focused on communication, which can be seen for example from the following citations.

> Well, it depends on the case a little bit, what kind it is. That, at least we communicate in the company that something like this happened and then we may inform also to the *service provider 1* that there is something like this. (Case 1)

> We have a security incident process, of which I am the process owner. It is a standardized process from people, processes, and technology perspectives incidents are handled. (Case 3)

This shows the robustness of processes in large organisations and the dependency of external knowhow. However, the communication that the small organisations performed differs a lot from the large organisations since for small organisations the communication is more internal whereas large organisations mainly discussed about external communication and reporting. This was shown as follows:

> …at least we communicate in the company that something like this happened. (Case 1)

> We report security incidents regularly, monthly, as part of our reporting. When an incident is ongoing, certain things get specific attention. If it's a more critical incident, we inform certain management groups. -- Our process is documented, so any of our employees can see the general overview. (Case 3)

> If only individual credentials are compromised, there's usually no communication. For larger incidents, we involve communications and, if necessary, the crisis management team and IT leadership but the communication is always there in larger cases. (Case 4)
>
> There is a clear process for handling breaches—we try to identify root causes and communicate openly with any external parties that might be affected. We aim to communicate as fast and as openly as possible. If there are concrete examples, we try to share them openly, so people stay aware of current threats. (Case 7)

This demonstrates that small organisation (1 and 7) had more internal communication compared to the large organisations (3 and 4), which showed that users can read about how incidents are handled but they aren't necessarily as aware of present threats as in small organisations. This can be due to many reasons. It is possible that the volume of attacks in large organisations is so high, that informing users about them is not feasible or the large organisations want to contain information about possible attacks to control the external communication only through proper channels, thus controlling the external narrative. By informing the users about present threats, the small organisations are able to raise awareness of present threat landscape, thus helping their users recognize attacks and make their systems more secure. Large organisations on the other hand approach user cybersecurity awareness through more formal training that might include also real-life examples of attacks targeting their organisation.

In general, large organisations were more worried about internal threats than smaller organisations again with the exception of organisation 2. This was shown by the fact that 75% of the large organisations conducted or had the possibility of conducting background checks for all users of users with higher level accounts and 50 % used or considered using formal intelligence agency security clearances. For smaller organisations, only organisation 2 conducted formal security clearances and only 20% overall did background checks to verify their employees. To further mitigate risks of internal threats all large organisations and 60% of the small organisations conducted some level of log monitoring to identify malicious network traffic. Thus, large organisations in general had a more mature zero trust approach to internal threats than small organisations. One reason why background checks might not be done is that organisations feel that they can trust their employees stating, *"We trust our employees."* (Case 5) or "*But our current staff has been with us long enough that we haven't seen the need to do it to them (background checks)."* (case 8). This shows that organisations tend to trust long staying employees, even in larger organisations, which can lead to increased risks of internal threats.

Lastly in the people domain, the employee cybersecurity and awareness training differed between small and large organisations through regularity and focus. One of the small organisations had no

regular training for their users, and only 40% had regular cybersecurity focused training for their users. The remaining two organisations had either training that was more focused on legislation like GDPR or NIS-2, or training that was regular but with large time intervals between trainings. All large organisations conducted regular cybersecurity focused training and one of them also had a cybersecurity month with additional training. Thus, large organisations are able to offer better training for their employees, which helps them identify possibly malicious low-level attacks like phishing.

The processes domain showed larger differences between small and large organisations. In general, the procurement processes showed that larger organisations validated their vendors more carefully. 75 % of the large organisations validated all vendors with their own processes and 25% still considered cybersecurity aspects in the procurement process. In comparison only one small organisation conducted formal validation processes on their vendors, and another validated only major vendors formally, leaving 60% only to take the security aspects into consideration in the procurement processes. This is a stark difference between the small and large organisations demonstrating the capabilities of large organisations to validate vendors but also their market power that gives them more options in choosing their vendors.

Log collection and analyse also showed a difference between small and large organisations although the difference was not as large compared to the procurement processes. All large organisations collected comprehensive logs and used either SOC (75%) or automation (25%) to monitor for network anomalies. For small organisation 40% used a SOC service to monitor their logs whereas 20% used automation to find anomalies. This left 40% with only some log collection and no proactive or real time log analyse. Thus, large organisations were more likely to have real time log analysing to find network anomalies creating capabilities to identify possible attacks when they happen.

Vulnerability scanning told a similar story as log collection with all large organisations conducting regular vulnerability scan to their own networks, and in majority of the large organisation also to vendors systems. This demonstrates that large organisations have implemented a zero trust approach where they are constantly searching for weak spots in their own networks but also with their major vendors, indicating zero trust in them. For small organisations 60% conducted regular vulnerability scans to their own networks and 40% did no regular scans. Thus, large organisations were again more likely to conduct vulnerability scanning to proactively find vulnerabilities showing a more mature zero trust approach.

Access control policy management showed differences between large and small organisations even though across all organisations a role-based approach was used by the majority of the organisations. However, despite having a role-based access control model, small organisations faced difficulties with users having multiple roles, leading to a more person-based model. Large organisations utilised also role-based access in majority of cases with one also using just-in-time access for some roles. However, the difference between large and small organisations is caused by regular reviewing of accesses in large organisations. Majority of the large organisations stated that they review access for every system regularly to maintain least privilege access, showing a more zero trust approach to role-based access control, even though just-in-time or by case approved accesses would show even greater zero trust maturity. In comparison smaller organisations handled the access controls more based on HR processes, and thus role changes affected the access controls. This maintains some level of principle of least privilege, but with users having multiple roles, it is possible that users have more accesses that they need, thus not following the principle of least privilege.

Contingency planning presented differences between large and small organisations. 75% of the large organisations had formal and regularly updated continuity and contingency plans for their suppliers with the remaining organisation 8 only having reserve suppliers. However, since organisation 8 is part of a large international organisation, many of the most critical systems are provided by the parent organisation and the cybersecurity organisation is centralised, which leave only little planning to the organisation 8 itself. On the contrary, only one small organisation had formal and regularly updated contingency plans whereas most small organisations had their contingency plans only regarding major vendors or acts of nature. Thus, large organisations were more likely to have formal and up to date plans for their supply chains than smaller organisations.

Thus, the process domain generally showed the difference between small and large organisations where the latter had more formal processes allowing them to implement a more zero trust approach to many parts of their organisation.

In the architecture domain there were differences small and large organisations, although there were differences. 50% of large organisations had extensive micro-segmentation between different systems, networks, and devices. They also had separate segments for different vendors. One large organisation only had segmentation of office, production and building networks and the last wasn’t aware of their segmentation policies. On the other hand, only one small organisation had extensive micro-segmentation in their networks, with 60% having only some segmentation between networks and one with no segmentation in their network. This shows that large organisations have more

capabilities and resources but also more to protect leading to more micro-segmentation in their systems.

Similarly, all large organisations used encryptions both in their communication and stored data, one stating: *"Starting from, encryption at rest, encryption in transit."* (Case 3). On the contrary, only two small organisations claimed to be encrypting all communication and their data. Organisation 7 stated that they only encrypt external communication, whereas organisation 5 stated that they only encrypt personal information in both communication and in storage, but otherwise there were no encryption. This shows that smaller organisations utilise less encryptions than large organisations. Multiple of them stated that they use encryptions where possible, but many of their systems didn't support encryptions and thus, encryption was not utilised in those systems. Due to having less resources small organisations are not able to upgrade to newer systems with encryption capabilities leading to this gap between small and large organisations in general.

Organisations used different methods for user authentication with all large organisations utilising dynamic rules in using MFA in user authentication. Thus, these organisations didn't trust devices only based on their location or the device itself but utilised dynamic rulesets to determine if MFA was required. Two small organisations utilised same dynamic rules in their authentication policies, with two organisations requiring MFA only for some systems. One small organisation didn't use MFA at all for their authentication. Thus, large organisations are more likely to implement dynamic authentication policies allowing both efficiency and security whereas smaller organisations might have systems not supporting MFA implementation or they aren't seeing the benefits of using MFA.

To secure endpoint devices organisations used EDR solutions or antivirus software. All large organisations and 60% of small organisations had EDR software installed to protect their endpoint devices. This software collects logs from the devices and allows SOC or automation to analyse those logs to identify possible attacks. Only 40% of the small organisations had no real time surveillance for their endpoint devices and they relied on an antivirus software to protect the devices. Thus, endpoint devices were seen as a threat by majority of the organisations since they had invested into real time monitoring of those devices.

External access to organisations' systems were protected by usage of VPN and MFA. All large organisation and 40% of small organisations only allowed external access using VPN or IPsec tunnels and requiring MFA authentication. This left 60% of small organisations that required VPN connections to their systems, but they didn't utilise MFA. However, one of these small organisations used their size and close locational presence to their advantage by blocking all

connections from outside of Finland and opening those blocks only if an employee was abroad. These limits greatly possible attacks since most of them are coming from outside of Finland. This is a way that small organisations can use their size for their advantage unlike large organisations.

In general, large organisations showed high maturity in the architecture domain, but also many smaller organisations showed signs of high maturity with micro-segmentation showing the largest differences. Thus, the architecture domain showed the most similarities between small and large organisations. As a conclusion, larger organisations had a higher zero trust maturity compared to the smaller organisations, but even small organisations can have a high ZT maturity like organisation 2.

This study found that a larger organisation size generally led to a higher zero trust maturity due to larger requirements for supply chain security but also due to larger capabilities. Smaller organisations had more heterogeneity in their security practises and the practises across all domains were generally low. Differences between low and higher zero trust maturities in small organisations were mostly due to more mature processes and more secure architecture. On the other hand, large organisations had less variation in them because most of them relied on industry standard software containing zero trust elements, and more robust processes, leading to a higher zero trust maturity.

6 Discussion

6.1 Answers to research questions

In this chapter results from within-case and cross-group comparisons are synthesized to answer the research questions. There were four key findings, first of which was that threat focus diverges by size since small organisations prioritised their physical operations by seeing supply chain disruptions as greatest threats to their supply chains. Large organisations on the other hand emphasised data confidentiality, software supply chain risks, and low-level attacks to their organisation. Second finding was that the level or maturity of zero trust adoption correlates to the perceived risk of organisations. The organisations that valued their data confidentiality had more mature zero trust controls such as background checks, dynamic access control, or network micro-segmentation. Third key finding was that the most common zero trust elements to be implemented were the use of MFA, role-based access control, and VPN for external connections. Fourth, and last, key finding was that large organisations in general had a higher zero trust maturity compared to smaller organisations.

6.1.1 RQ1A: What are the largest cybersecurity risks for cyber supply chains?

Existing literature identified that supply chains are vulnerable for multiple attack vectors including social engineering such as phishing (ENISA, 2024), compromises in the software supply chain with cascading effect inside supply chains (Kangas, 2024; X. Wang, 2021), cyberattacks such as (D)DoS, malware, ransomware, and man-in-the-middle attacks (Ghadge et al., 2019; Yeboah-Ofori & Opoku-Akyea, 2019) and insider threats (Urciuoli & Hintsa, 2017). There are also many threat actors that have motives to target supply chains in their attacks. Nation-state actors can seek to cause wider disruptions by targeting large supply chains while cybercrime groups can target weaker links in the supply chain to gain access to large organisations. Competing organisations might utilise PSOAs to commit corporate espionage to gain advantages in markets and hacktivists might target supply chains to please attention to large corporations. (Boyes, 2015; ENISA, 2024). These risks were amplified by complexity and heterogeneity in supply chain systems. Legacy systems, weak supplier assurance, and lack of visibility reduce control of supply chains, thus making it harder to manage the risks. (Tanriverdi et al., 2024; Widjaja & Gregory, 2020). The consequences of attacks often cascade to other parts of the supply chain via outages, data breaches, quality issues or legal issues (Barron et al., 2016; Lis & Mendel, 2019; Soikkeli et al., 2023).

Top threats identified in this study's interviews, shown in table 11, were low level phishing attacks, malware, data breaches, and issues in the physical supply chain like material shortages. Smaller organisations found the threats like material shortages or global shutdowns to be the largest while data breaches were identified as the top threat by larger and more data-centric organisations. Ransomware and malware were also mentioned in many cases. Amplifiers noted from the interviews included flat networks, legacy systems, and limited vulnerability management especially in low-maturity organisations.

Table 11 Largest threats to supply chains perceived by interviewees

Case	Largest threat to their supply chain
1	Global shutdown, where components can't be sourced
2	Microsoft o365 attacks
3	Big data breach to confidential information
4	Phishing, identity threats, and supply chain attacks
5	Cyberattack to software service provider
6	Leaked credentials giving access to digital environments
7	Material shortage
8	Malware entering information systems through trusted suppliers or customers
9	Lack of demand for the products or a sabotage / breach targeting critical assets

In people domain results of this study followed the existing literature with the emphasis on social engineering and insider risks, that were identified by most cases. Also following the literature, organisations with lower zero trust maturity, placed more trust on their employees and partners, whereas larger organisations used automated tools to monitor network traffic for anomalies, placing no trust on network actors.

In process domain the existing literature emphasized software supply chain and third-party assurance as critical risk mitigation controls, which this study concurs since organisations with higher zero trust maturity generally had strict policies for vendor vetting and securing software supply chain. Smaller organisations and organisations that didn't see data as a critical asset, didn't follow the literatures recommendations on formal supplier audits or secure software supply chains, leading to their lower zero trust maturity.

In architecture domain the literature emphasises micro-segmentation to prevent lateral movements in networks and using MFA and encryption to limit exposure. This study converged with the literature by showing that data-centric and generally larger organisations utilise these controls to

secure their data whereas smaller, less data-centric organisations didn't use such controls in their environments. Especially encryption policies in smaller organisations where limited to only personal data or usage of VPN.

From a socio-technical perspective, the cybersecurity risks related to the human component and its interaction with machine components are critical. Social engineering cyberattacks, such as phishing, target these components to exploit the weaknesses in them. The results of this study highlight this by showing that organisations perceive these low-level attacks as one of the largest threats to their organisations supply chain. Thus, maturity models like the EZTMM by Tokerud et. al (2023) that focus more on these socio-technical factors can be more suited to evaluate how these risks are measured and mitigated.

Based on the existing literature and this study the largest risks to cyber supply chains depend on organisation size and their data-centricity. For larger and more data-centric organisations the largest threats are social engineering, software supply chain, malware, and malicious insiders that result in data breaches that might cascade through the supply chain. These threats are amplified by complexity, and lack of visibility and control in supply chains, thus creating a hard to manage risk. For smaller organisations, the largest threats are related to their physical operations like material shortages or global shutdowns. This is a larger problem for them since they might not handle a lot of data, and their business models can be built more around manufacturing. Thus, the threats rising from the cyber supply chain depend on the organisations size, position in markets and the supply chain data itself.

6.1.2 RQ1B: How can zero trust be implemented in cyber supply chains?

Existing literature identifies zero trust approaches as viable solutions for mitigating threats in the cyber supply chain. The two mantras built into zero trust, "assume breach" and "never trust, always verify", guide organisations to enforce least-privilege, per request, dynamic access controls (Buck et al., 2021; Kindervag, 2010a). Implementation of zero trust is guided by several tenets, of which the key ones for cyber supply chains environments, are dynamic access control policies, per-session access, continuous monitoring, data protection in transit and at rest, and strict authentication and authorisation. These should be applied to all components, both human and machine, in the environment. (Rose et al., 2020).

Zero trust architecture can be implemented in three ways. *Enhanced identity governance* uses policies that are based on the identities and attributes of actors requesting access to resources.

Micro-segmentation separates networks into small segments limiting exposure in possible breaches. Third way to implement ZTA is using *network infrastructure* where agents and resource gateways to control access to resources. (Rose et al., 2020). The implementation of zero trust can be governed through zero trust maturity models that help organisations to assess their environments and current socio-technical capabilities (Tokerud et al., 2023). Thus, organisations can implement zero trust tenets to their cyber supply chains through a few routes. This should be guided by a zero trust maturity model, to help the organisation observe their weaknesses and strengths.

6.1.3 RQ1: What zero trust elements have organisations implemented to mitigate risks of cyberattacks to their cyber supply chain?

In this study several patterns that converged with the literature were observed. The interviewed organisations were categorised to have low, medium, or high zero trust maturity based on their interview answers. This study found that generally larger organisations had higher zero trust maturity, but it wasn't the only relevant factor. It was found that organisations that identified system or data breaches, or attacks to critical assets, as the largest threat to their supply chain, had a higher zero trust maturity than the organisations that identified material shortages or other supply chain issues as the largest threat like illustrated by figure 7.

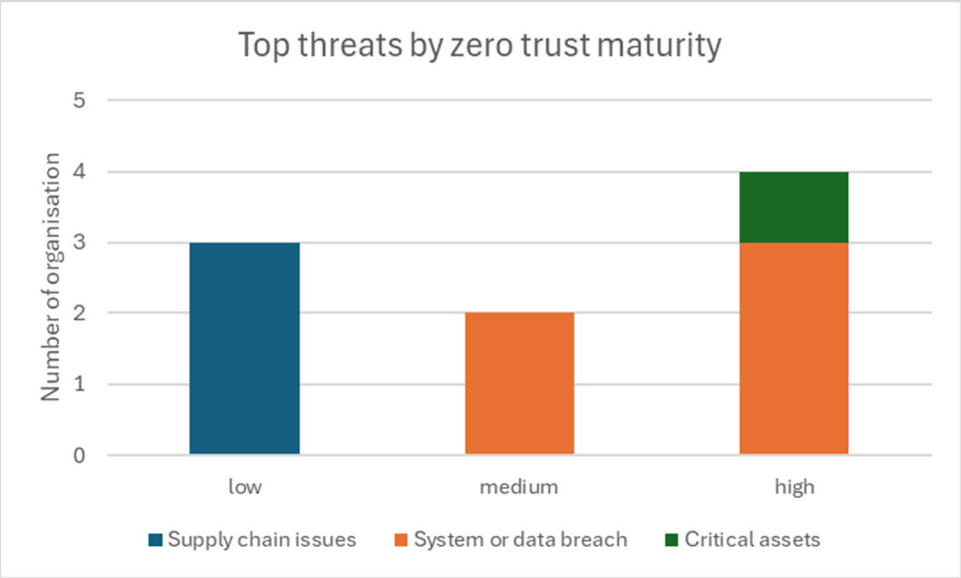

Figure 7 Largest threats to supply chains compared to observed zero trust maturity

Overall, zero trust implementations were found on all three domains. In the people domain, most commonly implemented tenets were regular cybersecurity training and incident communication whereas background checks were conducted only in high maturity organisations. In the process

domain, role-based access controls backed with MFA were commonly implemented whereas supplier audits and software supply chain scanning were only implemented by high maturity organisations. Network monitoring was commonly done through outsourced SOC services, but some larger organisations had either an automated SIEM solutions or internal SOC teams. In the architecture domain MFA for encrypted remote connections was most common to be implemented while micro-segmentation was only found in high maturity organisations.

In the people domain existing literature emphasizes documented incident processes, employee background checks, and mandatory frequent training. This study observed that organisations that identified cybersecurity risks high utilised proper background checks, whereas organisations that viewed other risks like material shortage more serious for their supply chains didn't perform such checks. Almost all organisations conducted some cybersecurity training for their employees, but higher maturity organisations used more frequent and encaging trainings than the lower performing organisations.

In process domain, this study found that data centric organisations followed literature with centralised identity-access-management, vulnerability scanning, and supplier requirements. But smaller and less data-centric organisations tend to overlook these recommendations. There was also a gap between the literature and this study where hunting proactively for vulnerabilities was seen mostly only on high performing data centric organisations whereas the lower performing organisations didn't look for these vulnerabilities.

In the architecture domain literature calls for micro-segmentation, MFA and dynamic access control, which high maturity organisations had implemented well. For smaller organisations and less data-centric organisations legacy systems that didn't support MFA, SSO logins or encryptions hindered zero trust adoption. Similarly micro-segmentation separated data-centric organisations from the rest since they had extensive segmentation that followed the literature compared to other organisations that had broader segmentation if any.

Extending the zero trust implementation to include more socio-technical elements can have positive influence on mitigating risks that are related to the human component and its interactions. Including socio-technical components was mentioned by most interviewed organisation. The observed methods for mitigating the risks created by the human component and its interactions in this study, can be divided into social and technical. The social methods were related to seeking to have the most secure workforce as possible meaning that the people in the organisation are more unlikely to fall victim of attacks targeting them like phishing. Most organisations had implemented a user

training program to educate users to detect attacks, while some also tested this regularly with phishing simulations. Conducting background checks was the second method organisations used to control risks related to their employees. Thirdly, open communication about previous and current attacks can increase awareness and awaken users to think and notice these threats. All of these methods were proactive methods to lessen the risks created by the human component. The technical methods this study identified mitigated the risk created by the human component through automation and monitoring. Monitoring network traffic through a SOC or with automatic threat detection aims to detect breaches or other malicious traffic while it happens, thus stopping the attacks early preventing damage. This way for example a malicious login with stolen user credentials could be stopped early. Conditional access control was another method for controlling the risk created by the human component, since requiring MFA can increase the security since a stolen password might still not grant access to systems. The social findings in this study concur with the EZTMM by Tokerud et al. (2023) that implemented a socio-technical approach to zero trust maturity model where the human component was evaluated through the people domain. The technical findings concur with the CISA ZTMM where the technical domains are more centred about how to secure an environment and not about the causes of the risks. Thus, the risks created by the human component are mitigated through the domains Identity and Network because those include controls like MFA or network traffic monitoring. Even though maturity models like the ZTMM don't have an explicit human or people domain, they control the risks that caused by humans through more technological solutions whereas the EZTMM approaches them more holistically by including the human element. Thus, the results of this study aren't fully captured in the CISA ZTMM but are on the other hand strongly aligned with the EZTMM by Tokerud et. al (2023).

This study also showed that the people domain controls were implemented in more low and medium maturity organisations compared to process or architecture domain controls. This indicates that the people centric controls can be more suited for less mature zero trust implementations than more technical controls. This however doesn't mean that a higher zero trust maturity implementation should overlook these controls. It means that in the lower maturity stages, organisations might find it easier or more achievable to improve their security posture by focusing on their human resources through training, communication, and background checks.

As a conclusion this study largely confirms patterns identified by existing literature while showing difference in implementation between different organisations. Both existing literature and this study agree that largest threats to cyber supply chains are low level attacks such as phishing that lead to

identity compromises and data breaches, software supply chain attacks, and insider threats. These risks are amplified by the complex nature of supply chain environments and limited control of suppliers. Zero trust literature consistently presents themes or tenets like principle of least privilege, continuous verification, micro-segmentation, and strong encryptions as effective means to mitigate the risks for cyber supply chains. However, the results show that the implementation of some of the tenets was uneven. Foundational elements like MFA, external VPN connections or endpoint security were widely implemented among the organisations that had medium or high zero trust maturity, but tenets like just-in-time access, secure development of software or systematic supplier audits were implemented in only high maturity organisations. This study also found that smaller organisations tended to have a lower zero trust maturity on average, but a small size didn't prohibit an organisation from having a high zero trust maturity, like shown by organisation 2. This follows the results from the report by the National Emergency Supply Agency of Finland, where they reported that small and medium sized organisations are more represented in the lower and medium maturity stages, but still some smaller organisations have a high security maturity. (Huoltovarmuuskeskus, 2026). From a socio-technical perspective it was noted that to holistically mitigate risks created by the human component, a socio-technical approach can produce more holistic results. Also, it was noted that the people domain controls were more represented in low and medium maturity organisations compared to process and architecture domain control.

Next, in these final chapters theoretical contributions of this study are visited and recommendations to organisations about zero trust implementations will be given. The goal is to help organisations improve their cyber supply chains security through implementing zero trust principles. Lastly limitations of this study as well as future research recommendations will be visited.

6.2 Theoretical contributions

This study contributes to the existing literature by providing understanding on how zero trust is adopted in real organisations, thus bridging the gap between conceptual frameworks and real-life supply chains through empirical evidence. Existing literature builds on theoretical models that create a holistic approach to securing environments, but in this study, zero trust was studied specifically in cyber supply chain context contributing to both zero trust and supply chain security literature.

In this study a socio-technical approach through people, process and architecture theoretical framework was taken to address cyber supply chains holistically. Prior literature tended to lean on the technical side emphasizing technology-centric controls, this study also emphasised people and

process controls by combining several zero trust maturity models to better gain a holistic view of the case organisations, thus extending existing socio-technical zero trust literature. However, in this study it was also noted that mitigating risks caused by the social component in systems can be done through a socio-technical approach, which combines the technical controls such as network monitoring found in more technical maturity models like ZTMM with the social controls like security and awareness training found in EZTMM. The results of this study show that these people domain controls can be equally as important in reducing risks in cyber supply chains. Thus, to address the complex risks created by users and their interaction with technical systems, a socio-technical approach can yield more holistic results that are address the risks both proactively and during attacks.

This study also provided empirical validation of existing literature about perceived threats to supply chains, but also about zero trust implementations in existing supply chain environments. It was found that organisations found both security related threats but also standard supply chain risks, such as material shortages to be top threats to their cyber supply chains. This extends the existing literature by showing that all organisations didn't consider cybersecurity as critical for their supply chains operations. This study also showed that some zero trust elements were more adopted than others. Technologies like MFA and VPN were widely used but processual elements like secure development processes or supplier audits like some human elements such as background checks were not as widely implemented. Also, many technological solutions like micro-segmentation were found in only some cases. Thus, this study provided validation to the existing literature and identified gaps between literature recommendations and real-life implementations.

As a conclusion, this study contributed to the existing literature by applying a holistic socio-technical approach to zero trust implementations in supply chains and it provided empirical validation to existing literature while identifying gaps between literature recommendations and real-life adoptions.

6.3 Recommendations to organisations

This study revealed that organisations have implemented varying levels of security controls to secure their cyber supply chains. Foundational controls like MFA and external VPN connections were implemented in many organisations, but gaps with recommendations were still left in all three domains.

In people domain, organisations should firstly invest in efficient security awareness and training. Beyond basic yearly compliance modules, more regular and concrete trainings such as phishing simulators can be an efficient way of educating users, thus protecting organisations from low level attacks. Secondly, insider risk management through background checks can help mitigate risks related to malicious insiders or corporate espionage. Even though the checks wouldn't be formal done by security agencies, basic checks to validate user's backgrounds can help to spot bad apples from potential applicants. Thirdly, communicating openly within the organisation and with stakeholders about experienced attacks can reduce the likelihood of similar attacks being successful in the future. It can also reduce the risk of cascading effects inside the supply chain.

In the process domain, the first recommendation for organisations is to integrate more formal supplier assurance processes before and during relationships. These can be achieved by asking for certifications or audits before signing contracts and during the relationship holding regular audits. Obligations about disclosing vulnerabilities or security incidents are also recommended to be included in contracts. Secondly, risks related to software should be mitigated by implementing secure programming practices and proactive vulnerability scanning of all critical applications. Thirdly, implementing central identity and access control through IAM solutions can enables easier and stricter access controls or even in best case scenarios only granting just-in-time or per case access to resources.

In architecture domain, organisations can firstly improve their security posture by implementing micro-segmentation for internal users but also for external users like vendors to their own vendor specific segments. This can greatly limit breaches to specific segments and limit lateral movement during breaches. Secondly, increasing the usage of encryptions both in transit and in storage across all systems. If legacy systems won't support encryption, capsulating them can help to mitigate the risk they pose. Thirdly, implementing continuous monitoring of network traffic through a SOC or by automated solutions and collecting all security logs into a SIEM. This enables organisations to better detect breaches when they happen and investigate already happened breaches to find root causes.

From a socio-technical perspective organisations should consider implementing human centric controls such as employee security and awareness training, active communication, or background checks because they can increase the organisations security posture easier than implementing new systems or investing in SOC monitoring. Organisations with a higher maturity should still not overlook these controls since they together with more technical controls from process and

architecture domains crate a more holistic solution were controls from each domain complement each other. An example, even an expensive SOC system won't protect the organisation from a user writing notes on paper and forgetting those on a table.

All in all, organisations should invest in a holistic security solutions covering all three domains. The security of a supply chain is only as strong as its weakest link, which means that by educating users, mitigating risks by proactively scanning for vulnerabilities and by creating capabilities to respond to incidents, organisations can protect themselves from the threats rising from the cyber supply chain.

6.4 Limitations

In this chapter, the limitations of this study are visited. These limitations of this study are linked to the data collection and the research method itself. Firstly, the case organisations for this study were chosen with a convenience sampling, which may have affected the results of this study. This means that organisations that are parts of critical infrastructure can be prohibited on disclosing their security practises leaving possible top performers out of the scope of this study. On the other hand, it is possible that there are more low performing organisations that were not chosen for this study. To add to this limitation, all the organisations operated in Finland, which is why this study only represents results of Finnish organisations. Thus, the organisations chosen to this study create both geographical and organisational limitations that may have impacted the results of this study.

Secondly, the interviewees that participated in the interviews were the people responsible for cybersecurity in their organisations. Their roles and backgrounds differed from each other's because some of them were clearly from business side and some from the technical side. Thus, the knowledge they had about their organisations' capabilities and processes might be limited to their roles, their knowledge, and their interest in cybersecurity. Thus, it is possible that the interviewees didn't have complete knowledge of their organisations, which may have reflected the results of this study.

Thirdly, this study was conducted during a period, where new regulatory changes like NIS-2 have been implemented, which may have changed organisational priorities. Changing threat landscapes and changes to the legislation may affect how organisations see the threats and risks related to their cyber supply chains, which may affect the applicability of this study in the future.

6.5 Recommendations for future research

In the future it would be beneficial to conduct a wider study about using zero trust in securing cyber supply chains through a more horizontally and vertically spread study. It would be beneficial to know how zero trust is seen in different parts of the cyber supply chain and how it impacts the operations of different actors in the chain. Similarly, it would be beneficial to study how the results would vary in different countries or continents due to for example cultural and legislative differences.

This study focused on if zero trust components were used to secure cyber supply chains, but in the future, it would be beneficial to study how outsourcing and external management of cybersecurity and zero trust affect the organisations capabilities and attitudes towards cybersecurity. This would be interesting to research because outsourcing cybersecurity can cause deep relations to external parties, thus exposing the organisation for threats in the future if the relationship with the service provider would be cut.

Some critical infrastructure was included in this study, but to more deeply study the possibilities of a full zero trust implementation in an organisation, a wider range of critical infrastructure organisations, or a more comprehensive study of a single organisation, could be fruitful to understand how far zero trust can be taken to secure an organisations environment, including the cyber supply chain.

Finally, it would be interesting to see how NIS-2 directive has influenced cybersecurity of supply chains. NIS-2 includes more organisations than previous legislations and poses requirements on cybersecurity management and incident reporting for these organisations. Thus, it would be interesting to study how this new legislation has influenced organisations conduct on securing their supply chains.

References

Al-Ansari, A. O., & Alsubait, T. M. (2022). Predicting Cyber Threats Using Machine Learning for Improving Cyber Supply Chain Security. *2022 Fifth National Conference of Saudi Computers Colleges (NCCC)*, 123–130. https://doi.org/10.1109/NCCC57165.2022.10067692

Barron, S., Cho, Y. M., Hua, A., Norcross, W., Voigt, J., & Haimes, Y. (2016). Systems-based cyber security in the supply chain. *2016 IEEE Systems and Information Engineering Design Symposium (SIEDS)*, 20–25. https://doi.org/10.1109/SIEDS.2016.7489299

Bateman, J. (2020). *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*. CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE.

Becker, J., Knackstedt, R., & Pöppelbuß, J. (2009). Developing Maturity Models for IT Management: A Procedure Model and its Application. *Business & Information Systems Engineering*, *1*(3), 213–222. https://doi.org/10.1007/s12599-009-0044-5

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386. https://doi.org/10.2307/248684

Bilge, L., & Dumitraş, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 833–844. https://doi.org/10.1145/2382196.2382284

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*.

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

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*, 102436. https://doi.org/10.1016/j.cose.2021.102436

Charles C. Poirier. (2002). *The Supply Chain Manager's Problem-Solver*.

Chen, Y., Hu, H., & Cheng, G. (2019). Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. *Frontiers of Information Technology & Electronic Engineering*, *20*(2), 238–252. https://doi.org/10.1631/FITEE.1800516

CISA. (2023). *CISA Zero Trust Maturity Model*. https://www.cisa.gov/zero-trust-maturity-model

Collier, Z. A., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, *59*(11), 3430–3445. https://doi.org/10.1080/00207543.2021.1884311

Corbet, S., & Gurdgiev, C. (2020). An Incentives-Based Mechanism for Corporate Cyber Governance Enforcement and Regulation. In *Ecological, Societal, and Technological Risks and the Financial Sector*. Springer International Publishing AG.

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, *27*(1), 30–53. https://doi.org/10.1108/SCM-02-2020-0073

Cyber-Attacks Against Critical Infrastructure. (2022). In M. Lehto, *Cyber Security: Critical Infrastructure Protection*. Springer International Publishing AG.

Do Amaral, T. M. S., & Gondim, J. J. C. (2021). Integrating Zero Trust in the cyber supply chain security. *2021 Workshop on Communication Networks and Power Systems (WCNPS)*, 1–6. https://doi.org/10.1109/WCNPS53648.2021.9626299

Dunwoodie, K., Macaulay, L., & Newman, A. (2023). Qualitative interviewing in the field of work and organisational psychology: Benefits, challenges and guidelines for researchers and reviewers. *Applied Psychology*, *72*(2), 863–889. https://doi.org/10.1111/apps.12414

Durugbo, C. M., & Al-Balushi, Z. (2024). Supply chain management in times of crisis: A multi-case study. *Production Planning & Control*, 1–29. https://doi.org/10.1080/09537287.2024.2386431

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, *14*(4), 532–550. https://doi.org/10.2307/258557

ENISA. (2024). *ENISA threat landscape 2024: July 2023 to June 2024.* Publications Office. https://data.europa.eu/doi/10.2824/0710888

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

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

Ghanbari, H., Koskinen, K., & Wei, Y. (2024). From SolarWinds to Kaseya: The rise of supply chain attacks in a digital world. *Journal of Information Technology Teaching Cases*, 20438869241299823. https://doi.org/10.1177/20438869241299823

Holm, H., Sommestad, T., Almroth, J., & Persson, M. (2011). A quantitative evaluation of vulnerability scanning. *Information Management & Computer Security*, *19*(4), 231–247. https://doi.org/10.1108/09685221111173058

Huoltovarmuuskeskus. (2026). *Kyberkypsyys toimialoilla 2025*. Huoltovarmuuskeskus.

Huong Tran, T. T., Childerhouse, P., & Deakins, E. (2016). Supply chain information sharing: Challenges and risk mitigation strategies. *Journal of Manufacturing Technology Management*, *27*(8), 1102–1126. https://doi.org/10.1108/JMTM-03-2016-0033

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kangas, L. (2024, December 20). Valio oli hyökkääjälle ”huippu-uhri”, sanoo tietoturva-asiantuntija. *Yle.Fi*. https://yle.fi/a/74-20133016

Kaur, H., Gupta, M., & Singh, S. P. (2024). Integrated model to optimize supplier selection and investments for cyber resilience in digital supply chains. *International Journal of Production Economics*, *275*, 109338. https://doi.org/10.1016/j.ijpe.2024.109338

Khandewal, A., & Mahato, D. P. (2024). Zero-Day Exploits Framework of Supply Chain Networks. In: Verma, A., Verma, P., Pattanaik, K.K., Dhurandher, S.K., Woungang, I. (eds). In *Advanced Network Technologies and Intelligent Computing. ANTIC 2023. Communications in Computer and Information Science, vol 2090. Springer, Cham.* (pp. 319–335). Springer Nature Switzerland. https://link.springer.com/10.1007/978-3-031-64076-6

Kindervag, J. (2010a). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture*.

Kindervag, J. (2010b). *No More Chewy Centers: Introducing The Zero Trust Model Of Information Security*.

König, W. (1994). *Profil der Wirtschaftsinformatik. Ausführungen der Wissenschaftlichen Kommission der Wirtschaftsinformatik.* 80.

Kshetri, N., & Voas, J. (2019). Supply Chain Trust. *IT Professional*, *21*(2), 6–10. https://doi.org/10.1109/MITP.2019.2895423

Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *JOURNAL OF INTERNATIONAL STUDIES*, *17*(2), 220–239. https://doi.org/10.14254/2071-8330.2024/17-2/12

Lambert, J. H., Keisler, J. M., Wheeler, W. E., Collier, Z. A., & Linkov, I. (2013). Multiscale approach to the security of hardware supply chains for energy systems. *Environment Systems and Decisions*, *33*(3), 326–334. https://doi.org/10.1007/s10669-013-9465-2

Lis, P., & Mendel, J. (2019). Cyberattacks on Critical Infrastructure: An Economic Perspective. *Economics and Business Review*, *5*(2), 24–47. https://doi.org/10.18559/ebr.2019.2.2

McAlaney, J., Frumkin, L. A., & Benson, V. (Eds). (2018). *Psychological and Behavioral Examinations in Cyber Security:* IGI Global. https://doi.org/10.4018/978-1-5225-4053-3

Mitchell, B. (2020). CORPORATE CYBERESPIONAGE: IDENTIFICATION AND PREVENTION PART 1. *EDPACS*, *62*(5), 1–14. https://doi.org/10.1080/07366981.2020.1798594

Osman, R., & El-Gendy, S. (2024). Interconnected and resilient: A CGE analysis of AI-driven cyberattacks in global trade. *Risk Analysis*, risa.14321. https://doi.org/10.1111/risa.14321

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

Papastergiou, S., & Polemi, N. (2018). MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology. In X.-S. Yang, A. K. Nagar, & A. Joshi (Eds), *Smart Trends in Systems, Security and Sustainability* (Vol. 18, pp. 1–9). Springer Singapore. https://doi.org/10.1007/978-981-10-6916-1_1

Paul, B., & Rao, M. (2022). Zero-Trust Model for Smart Manufacturing Industry. *Applied Sciences*, *13*(1), 221. https://doi.org/10.3390/app13010221

Paul, S., Ding, F., Utkarsh, K., Liu, W., O'Malley, M. J., & Barnett, J. (2022). On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review. *IEEE Systems Journal*, *16*(2), 2367–2378. https://doi.org/10.1109/JSYST.2021.3123904

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. https://doi.org/10.1007/s10111-021-00683-y

Pöppelbuß, J., & Röglinger, M. (2010). *WHAT MAKES A USEFUL MATURITY MODEL? A FRAMEWORK OF GENERAL DESIGN PRINCIPLES FOR MATURITY MODELS AND ITS DEMONSTRATION IN BUSINESS PROCESS MANAGEMENT*.

Prathyusha, J. R. V. S. L. P., Jyothi, V. E., Jhansi, V., Chowdary, N. S., Madhuri, A., & Sindhura, S. (2023). Securing the Cyber Supply Chain: A Risk-based Approach to Threat Assessment and Mitigation. *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 508–513. https://doi.org/10.1109/ICESC57686.2023.10193255

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sabbagh, B. A., & Kowalski, S. (2015). A Socio-technical Framework for Threat Modeling a Software Supply Chain. *IEEE Security & Privacy*, *13*(4), 30–39. https://doi.org/10.1109/MSP.2015.72

Sawik, T. (2022). Balancing cybersecurity in a supply chain under direct and indirect cyber risks. *International Journal of Production Research*, *60*(2), 766–782. https://doi.org/10.1080/00207543.2021.1914356

Schlackl, F., Link, N., & Hoehle, H. (2022). Antecedents and consequences of data breaches: A systematic review. *Information & Management*, *59*(4), 103638. https://doi.org/10.1016/j.im.2022.103638

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world.* WW Norton & Company.

Schneier, B., & Vance, A. (2025). "Complexity Is the Worst Enemy of Security": Studying Cybersecurity Through the Lens Of Organizational Complexity. *MIS Quarterly*, *49*(1), 205–210. https://doi.org/10.25300/MISQ/2025/49.1.075

Sena, J. (2022, November 16). SolarWinds Agrees to $26 Million Payout Over Massive Data Breach. *ISS Insights*. https://insights.issgovernance.com/posts/solarwinds-agrees-to-26-million-payout-over-massive-data-breach/

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*(1), 161–171. https://doi.org/10.1016/j.ejor.2019.09.017

Soikkeli, J., Casale, G., Muñoz-González, L., & Lupu, E. C. (2023). Redundancy Planning for Cost Efficient Resilience to Cyber Attacks. *IEEE Transactions on Dependable and Secure Computing*, *20*(2), 1154–1168. https://doi.org/10.1109/TDSC.2022.3151462

Stewart, J. (2012). Multiple-case Study Methods in Governance-related Research. *Public Management Review*, *14*(1), 67–82. https://doi.org/10.1080/14719037.2011.589618

Subramani, S., Kavitha, A. R., & Rukshana Safrin, A. (2025). Zero trust network architecture for modern enterprise environments. *2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI)*, 1–6. https://doi.org/10.1109/ICDSAAI65575.2025.11011897

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, *10*, 57143–57179. https://doi.org/10.1109/access.2022.3174679

Tanriverdi, H., Kwon, J., & Im, G. (2024). Taming Complexity in the Cybersecurity of Multihospital Systems: The Role of Enterprise-Wide Data Analytics Platforms. *MIS Quarterly*, *49*(1), 243–274. https://doi.org/10.25300/MISQ/2024/17752

The National Counterintelligence and Security Center (NCSC). (2018). *Foreign Economic Espionage in Cyberspace*. NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER.

Tokerud, S., Jansen, J., Niemimaa, M., & Järveläinen, J. (2023). *Designing Extended Zero Trust Maturity Model – From Technical to Socio-Technical*.

Urciuoli, L. (2015). Cyber-Resilience: A Strategic Approach for Supply Chain Management. *Technology Innovation Management Review*.

Urciuoli, L., & Hintsa, J. (2017). Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement. *International Journal of Logistics Research and Applications*, *20*(3), 276–295. https://doi.org/10.1080/13675567.2016.1219703

Wang, X. (2021). On the Feasibility of Detecting Software Supply Chain Attacks. *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, 458–463. https://doi.org/10.1109/MILCOM52596.2021.9652901

Wang, Y., & Pettit, S. (Eds). (2022). *Digital supply chain transformation: Emerging technologies for sustainable growth*. Cardiff University Press. https://doi.org/10.18573/book8

Widjaja, T., & Gregory, R. (2020). Monitoring the Complexity of IT Architectures: Design Principles and an IT Artifact. *Journal of the Association for Information Systems*, *21*(3), 664–694. https://doi.org/10.17705/1jais.00616

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

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Yeboah-Ofori, A., & Islam, S. (2019). Cyber Security Threat Modeling for Supply Chain Organizational Environments. *Future Internet*, *11*(3), 63. https://doi.org/10.3390/fi11030063

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. *IEEE Access*, *9*, 94318–94337. https://doi.org/10.1109/ACCESS.2021.3087109

Yeboah-Ofori, A., Islam, S., & Yeboah-Boateng, E. (2019). Cyber Threat Intelligence for Improving Cyber Supply Chain Security. *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 28–33. https://doi.org/10.1109/ICSIoT47925.2019.00012

Yeboah-Ofori, A., & Opoku-Akyea, D. (2019). Mitigating Cyber Supply Chain Risks in Cyber Physical Systems Organizational Landscape. *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)*, 74–81. https://doi.org/10.1109/ICSIoT47925.2019.00020

Appendices

Appendix 1 Data Management Plan

Research data management plan for students

This document will help you plan how to manage your research data. More detailed instructions for each section are available online in the Research Data Management Guide for Students.

1. Research data

Research data refers to all the material with which the analysis and results of the research can be verified and reproduced. It may be, for example, various measurement results, data from surveys or interviews, recordings or videos, notes, software, source codes, biological samples, text samples, or collection data.

In the table below, list all the research data you use in your research. Note that the data may consist of several different types of data, so please remember to list all the different data types. List both digital and physical research data.

Research data type	**Contains personal details/information***	**I will gather/produce the data myself**	**Someone else has gathered/produced the data**	**Other notes**
Interview records	x	x		Interview records saved in case of loss of data, saved on organisations cloud
Interview transcripts		x		Transcripts don't contain personal information. They are saved on the researchers' personal computer.

* Personal details/information are all information based on which a person can be identified directly or indirectly, for example by connecting a specific piece of data to another, which makes identification possible. For more information about what data is considered personal go to the Office of the Finnish Data Protection Ombudsman's website

2. Processing personal data in research

I will prepare a Data Protection Notice** and give it to the research participants before collecting data ☒

The controller** for the personal details is the student themself ☒ the university ☐

My data does not contain any personal data ☐

** More information at the university's intranet page, Data Protection Guideline for Thesis Research

3. Permissions and rights related to the use of data

Find out what permissions and rights are involved in the use of the data. Consult your thesis supervisor, if necessary. Describe the use permissions and rights for each data type. You can add more data types to the list, if necessary.

3.1 Self collected data

Data type 1: Participation to research is voluntary. Permission to record the interview is asked verbally in the beginning of the interview from the participants.

Data type 2: Permission to use transcripts is asked verbally from the participants at the beginning of the interview.

4. Storing the data during the research process

Where will you store your data during the research process?

In the university's network drive ☒
In the university-provided Seafile Cloud Service ☒
Other location, researcher's personal computer: ☒

The university's data storage services will take care of data security and backup files automatically. If you choose to store your data somewhere other than in the services provided by the university, please specify how you will ensure data security and file backups. Remember to make sure you know every time where you are saving the edited/modified data.

If you are using a smartphone to record anything, please check in advance where the audio or video will be saved. If you are using commercial cloud services (iCloud, Dropbox, Google Drive, etc.) and your data contains personal data, make sure the information you provide in the Data Protection Notice about data migration matches your device settings. The use of commercial cloud services means the data will be transferred to third countries outside the EU.

5. Documenting the data and metadata

5.1 Data documentation

Can you describe what has happened to your research data during the research process? Data documentation is essential when you try to track any changes made to the data.

To document the data, I will use:

A field/research journal ☐
A separate document where I will record the main points of the data, such as changes made, phases of analysis, and significance of variables ☒
A readme file linked to the data that describes the main points of the data ☐
Other, please specify: ☐

5.2 Data arrangement and integrity

How will you keep your data in order and intact, as well as prevent any accidental changes to it?

I will keep the original data files separate from the data I am using in the research process, so that I can always revert back to the original, if need be. ☒

Version control: I will plan before starting the research how I will name the different data versions and I will adhere to the plan consistently. ☐

I recognise the life span of the data from the beginning of the research and am already prepared for situations, where the data can alter unnoticed, for example while recording, transcribing, downloading, or in data conversions from one file format to another, etc. ☒

5.3 Metadata

I will save my data into an archive or a repository that will take care of the metadata for me. ☐

I will have to create the metadata myself, because the archive/repository where I am uploading the data requires it. ☐

I will not store my data into a public archive/repository, and therefore I will not need to create any metadata. ☒

6. Data after completing the research

Interview recordings are saved for one year.

Transcriptions are cleaned of any personal data and will be deleted after five years after the publication of the research.

Appendix 2 Declaration on the Use of Generative Artificial Intelligence

In this appendix the use of AI will be reviewed. The tools used and their purpose has been explained in detail below. I confirm that I have used AI tools and tools with AI components meticulously and carefully and I have fully brought up their use according to policies of University of Turku. I take full responsibility of all material used in this study.

1. Microsoft Copilot (Private instance of University of Turku)

Microsoft Copilot was used first in formulating ideas for the thesis and after that helping to find suitable methods and theoretical frameworks. After conducting interviews, Copilot was used to help translating the anonymised transcriptions. While conducting the literature review Copilot was used to help me understand hard or complex topics. In the later stages of the thesis process, Copilot was used to check for grammatical mistakes. This was done by asking for recommendations for edits, which were evaluated by the researcher and if deemed suitable, edited in the text. To ensure quality and control of material, no text was straight used from the tool, and the transcripts were examined word by word by the researcher to ensure that the contents of the interview didn't change.

2. ChatGPT (GPT-4)

ChatGPT was used in the early stages of the thesis process to formulate ideas for the thesis and identify possible research gaps.

3. Scopus AI and Volter AI

Scopus AI and Volter AI were used throughout the study to explain complex topics and find possible sources. The sources given by the AI agents were not trusted inherently, and their quality was checked from the JuFo-portal to ensure the scientific quality. The explanations from the tools were often compared to each other to ensure the quality of explanations. No text was copied from the tools to the thesis, leaving the control of the text to the researcher.

4. Microsoft Teams

Microsoft Teams uses AI to generate transcriptions from meeting recordings. The interviews in this study were conducted using the Teams and transcriptions created by the tool were used. These transcriptions were checked by the researcher line by line to ensure correct transcriptions. The account used in the interviews was the researchers UTU-account, meaning that the recordings and transcriptions were stored in the University of Turku's Microsoft environment.