UNIVERSITY OF TURKU
Turku School of Economics

Sharing is Caring: Trust, Information Sharing, and Intelligence for Digital Supply Chain Cyber Threats

An empirical preliminary study on factors influencing digital supply chain cyber threat awareness in EU public and private organisations

Department of Management and Entrepreneurship: Information Systems Science

Master's thesis

Author(s):
Noah Spierings

Supervisor(s):
Prof. Dr. A.-F. Rutkowski

(version 1) 05.06.2026
Tilburg, The Netherlands

Student's statement regarding the use of Artificial Intelligence (AI) for preparing and/or writing this thesis:

☐ **I have not used any AI-based tools.**

☒ **I have used AI-based tools**. Their use is documented in Appendix G: Usage Log for External Tools and AI-Assisted Work. 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 System Sciences
Author(s): Noah Spierings
Title: Sharing is Caring: Trust, Information Sharing, and Intelligence for Digital Supply Chain Cyber Threats
Supervisor(s): Prof. Dr. A.-F. Rutkowski
Number of pages: 73 pages (+ appendices 16 pages, if any)
Date: 05.06.2026

Abstract

The digital age has introduced new forms of supply chains, namely digital supply chains. These chains are characterised by intertwined organisations using cloud services and software ecosystems that introduce new forms of cyber risks, threats and uncertainties regarding security objectives. Due to the distance of these services and the underlying structures underneath, organisations may depend more on cyber threat intelligence, inter-organisational information sharing between industry-peers and trust in information quality to improve awareness of cyber threats affecting their external digital dependencies. However, empirical evidence on how these factors jointly contribute to digital supply chain cyber threat awareness remains limited.

As such, this preliminary study investigates how cyber threat intelligence capability, inter-organisational cyber threat information sharing and information quality trust are associated with digital supply chain cyber threat awareness. It further explores whether differences exist between public and private organisations in terms of these constructs. The study is guided by Information Processing Theory, which conceptualises how organisations reduce uncertainty by acquiring and processing relevant (external) information.

A quantitative survey design was employed resulting in 31 usable responses (n = 31) from information security professionals, including CISOs, information security managers and -officers, amongst others. The data were analysed using reliability analysis (Cronbach's alpha), descriptive statistics, and Spearman correlation analysis. In addition, exploratory group comparison between public and private organisations were conducted using MANOVA, ANOVA and non-parametric Wilcoxon rank-sum tests.

The results suggest that cyber threat intelligence, inter-organisational cyber threat information sharing, and information quality trust are all positively associated with digital supply chain cyber threat awareness. The strongest associations were found for cyber threat intelligence capability and information quality trust, while information sharing showed weaker but still statistically significant relationship. Exploratory analysis suggests that public organisations reported higher levels of information sharing compared to private organisations, although overall awareness was reported comparable across. Due to the limited sample size, the findings should be interpreted as preliminary and exploratory, providing a foundation for future research in relation to the field of cyber supply chain risk management. The discussion was enhanced by an expert consultation session.

Keywords: Digital Supply Chains, Cyber Supply Chain Risk Management, Cyber Threat Information Sharing, Threat Intelligence Capability, Cyber Threat Awareness and Information Quality Trust.

TABLE OF CONTENTS

FIGURES

TABLES

1 Introduction

1.1 Background

Supply chains trace their origins to the early days of the Industrial Revolution, when the production, distribution, and sale of goods were common business models adopted by companies working together in unison. These companies - as nodes in a network (e.g., organisations, businesses, manufacturers) - build upon one another by creating additional layers of value in the so-called "chain," from start to finish. Originally, the Supply Chain Management (SCM) function was primarily concerned with achieving efficiency and improving customer value within the chain, particularly in logistics and manufacturing business areas (Habib, 2011). In broad terms, SCM can be defined as the management of the end-to-end process of creating, selling, consuming, and disposing of a product or service, and it is often intertwined with production, procurement, and other planning-related processes (Lu & Swaminathan, 2015).

However, the age of digitalisation has significantly stimulated innovation in SCM (Li et al., 2023). Technologies such as Big Data, Cloud Computing, the Internet of Things, and Augmented Reality have tremendously altered supply chains, as well as associated business models and value creation processes (Büyüközkan & Göçer, 2018; Wang et al., 2021). In terms of connectivity, technologies including wireless LAN, cellular networks, and other information systems utilising the internet have impacted the connectivity of nodes within supply chains (Lu & Swaminathan, 2015). This is particularly relevant, as the use of information systems that extend beyond organisational boundaries improves supply chain performance (Asamoah et al., 2020). As a result, information systems, networks, and information flows have expanded, evolved, or enabled the emergence of new supply chains and new approaches to managing them.

Unfortunately, the increased use of Information and Communications Technology (ICT) systems has also introduced new cybersecurity-related challenges. For example, in 2020, hackers conducted a supply-chain attack by secretly inserting malicious code into updates for SolarWinds' management software (hSO, 2020). These developments have increased the importance of Cyber Supply Chain Risk Management, which focuses on identifying, assessing, and mitigating cybersecurity risks arising between organisations and their chains. Consequently, securing cyber aspects within supply chains became a topic requiring further research attention (Linton et al., 2014).

In addition to academic attention, policymakers have increasingly signalled the importance of cybersecurity with supply chains. Within the European Union, regulatory frameworks such as the

NIS2 Directive. NIS2, the successor of NIS, was established to enable EU Member States to supervise and monitor the implementation of a legal framework for sectors with critical infrastructure, or those otherwise designated as critical. This framework aims to establish top-level accountability and strengthen cybersecurity functions to protect network and information systems (European Commission, 2023). Article 21 of the directive, which addresses cybersecurity risk-management measures, states that entities subject to the NIS2 Directive shall conduct risk-management activities to ensure appropriate and proportionate technical, operational, and organisational measures for network and information system security. In relation to cybersecurity in SCM, this article explicitly specifies the measure of "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers" (European Parliament, Council of the European Union, 2022, p. 127). Thus, cybersecurity in supply chains remains a topic of high importance to this day.

1.2 Problem Statement

The increasing digitalisation and interconnectivity of (digital) supply chains have expanded the cyber risk landscape faced by consumer organisations. Digital supply chains rely on interconnected information systems build on cloud infrastructures and held together by software, where data exchanges between multiple organisations occur. This results in cyber incidents affecting one organisations or actor within the chain, that can affect another within the same supply chain network. Despite growing academic attention and regulatory pressure, organisations often face difficulties in identifying cyber threats that originate from external partners, suppliers or service providers within digital supply chains.

As current literature states, inter-organisational cyber threat information sharing has been proposed as a mechanism to improve collective cyber situational awareness by enabling organisations to exchange threat information. Technical threat intelligence sharing, if timely and of quality, has been found to be useful. However, the inter-organisational and informal method of sharing cyber threat information and its association in creating awareness of digital supply chain cyber threats remains insufficiently understood. Moreover, organisations in public and private sectors could differ in their relationship with industry peers, for which the trust in information quality can also affect their effective awareness. Consequently, further research is required to understand how inter-organisational information sharing could support the awareness of cyber risks within digital supply chains.

Moreover, the researcher's hosting organisation benefits from a broad and qualitative insight on this matter to improve the quality of their consultancy practices for their broad portfolio of clients. Anecdotal evidence during projects have brought niche insights about industry peer inter-organisational information sharing practices, however the hosting organisations wishes to statistically test it on a broader scale.

1.3 Research Objectives and Questions

The objective of this study is to examine how inter-organisational information sharing contributes to organisation's ability to become aware of digital supply chain cyber threats. More specifically, this explorative preliminary study aims to contribute to academia by examining how inter-organisational cyber threat information sharing contributes to organisations' awareness of digital supply chain cyber threats that can affect themselves, while also analysing how this relationship is influenced by the organisations' internal threat intelligence capability, trust in information quality and how this could differ for private and public organisations.

As such, the following main research question was constructed for this research:

How are cyber threat intelligence capability, inter-organisational cyber threat information sharing and information quality trust associated with digital supply chain threat awareness among information security managers in European public and private organisations?

The following sub-research questions (RQ) have been made to support the main question:

RQ1: *How are cyber threat intelligence capability, inter-organisational cyber threat information sharing and trust in information quality associated with digital supply chain cyber threat awareness?*

RQ2: *To what extent do public and private organisations differ in cyber threat inter-organisational information sharing and information quality trust?*

RQ3: *To what extent do public and private organisations differ in digital supply chain threat awareness?*

1.4 Research Methodology and Scope

This study adopts a quantitative and exploratory research design to examine the association between inter-organisational cyber threat information sharing and digital supply chain cyber threat awareness. A semi-structured literature review was conducted to gather abstract and key articles to give context to the matter at hand, create a theoretical framework and to define the respective constructs. A survey was meticulously constructed and tested containing four primary constructs: Inter-organisational Cyber Threat Information Sharing (ICTIS), Cyber Threat Intelligence Capability (CTIC), Information Quality Trust (IQT), and Digital Supply Chain Cyber Threat Awareness (DSCCTA). These constructs were operationalised using multiple Likert-scale measurement items derived and adapted from existing literature on cyber threat intelligence, inter-organisational information sharing, trust, and supply chain cybersecurity. Afterwards, data was collected through an online survey targeting cybersecurity professionals involved in threat intelligence, security operations, governance, risk management, or related cybersecurity functions within organisations operating in the European Union. The target population primarily consists of organisations in the Netherlands operating within an information security management like roles. Considering the researchers' client network at the hosting organisation, specific organisations were chosen, such as insurance, banks and financial services, as well as care providers, hospitals and government service organisations, including other kinds of organisations. This to create a balanced split between private and public organisations.

Given the exploratory nature of the study and the relatively limited sample size, the analysis focused primarily on descriptive statistics, reliability assessment, correlation analyses, and exploratory group comparisons. Cronbach's alpha was used to assess internal consistency and reliability of the multi-item constructs. Spearman's correlation analyses were applied to examine the hypothesised relationships between the constructs. In addition, exploratory MANOVA and follow-up non-parametric analyses were conducted to examine potential differences between organisational groups, such as public and private sector organisations. Several practical limitations further constrained the scope of this research. The study was conducted individually during an internship period between February and June 2026, resulting in limitations in time, financial resources, and respondent accessibility. Consequently, the sample size remained relatively modest, which limits the generalisability of the findings and reinforces the exploratory character of the study. Although multiple measures were taken to support validity and reliability, including pilot survey testing, reliability assessment, and robustness checks, the possibility of unforeseen biases and methodological limitations cannot be fully excluded. Additional theoretical and methodological limitations are discussed in subsequent chapters. Expert consultation was performed to enhance the discussion.

1.5 Overview of Chapters

This thesis is structured into six main chapters, including the introduction. Chapter 2 presents the literature review, introducing the phenomenon of digital supply chains, the characteristics of cyber risks within these environments and transitions into the formulation of threats. Within this chapter, inter-organisational cyber threat information sharing, cyber threat intelligence and information quality trust are explored and made tangible utilising the theoretical lens Information Processing Theory. Based on the literature and this theoretical foundation, the conceptual model and hypotheses are developed.

Chapter 3 describes the research methodology, including the design, construct definitions and scopes, participant selection, data collection procedures and the statistical methods used to analyse the data. Considerations regarding validity and reliability are also discussed. Subsequently, Chapter 4 presents the empirical results. It starts with an overview of the sample characteristics and shows the reported data, followed by reliability and descriptive analyses, hypotheses testing, and exploratory analysis comparing organisation types (private vs public) and respondent roles.

Chapter 5 provides the conclusion by answering the sub-research questions, evaluating the hypotheses and summarising the study's main findings to fully answer the main research question. Afterwards, Chapter 6 goes into detail about discussion points in relation to the findings of existing literature and theories, outlines management implications, addresses the limitations of the study and provides recommendations for future research.

Finally, Chapter 7 contains the references, followed by the appendices which include the survey instrument, survey setup, data management plan and the scripts used for data sanitisation and statistical analysis.

1.6 Research Summary

Hereby a summary of the conducted research, by stating the questions, adhering methodology and associated findings.

Research Question(s)	Methodology	Key Findings
RQ1: How are cyber threat intelligence capability (CTIC) , inter-organisational cyber threat information sharing (ICTIS) and trust in information quality (IQT) associated with digital supply chain cyber threat awareness?	Quantitative survey (n = 31), reliability analysis, descriptive statistics, internal validity checks and two-sided Spearman correlation analysis.	All three constructs were positively associated with digital supply chain cyber threat awareness. H_1, H_2 and H_3 (alternative hypotheses) were supported. CTIC (rs = .73) and IQT (rs = .65) showed the strongest associations, while ICTIS (rs = .39) showed a weaker association. All were found to be statistically significant ($p < .05$).
RQ2: To what extent do public and private organisations differ in cyber threat inter-organisational information sharing and information quality trust?	Descriptive statistics, internal validity checks, MANOVA, ANOVA and Wilcoxon rank-sum tests.	Public organisations reported significantly higher levels of inter-organisational cyber threat information sharing than private organisations (H_{4a} supported). No significant differences were found for information quality trust (H_{4b} rejected).
RQ3: To what extent do public and private organisations differ in digital supply chain threat awareness?	Descriptive statistics, internal validity checks, MANOVA, ANOVA and Wilcoxon rank-sum test.	No statistically significant differences was found between public and private organisations regarding digital supply chain cyber threat awareness. H_5 was therefore rejected.

Ultimately to answer the main research question with this preliminary research, the findings suggest that digital supply chain cyber threat awareness is associated not only with the exchange of cyber threat information between industry-peer organisations, but also with the capability to process threat intelligence and trust placed in the quality of the exchanged information. While public organisations appear to engage more actively in cyber threat information sharing, both public and private organisations reported comparable levels of trust in information quality, capability and digital supply chain cyber threat awareness.

2 Literature Review

A literature review was conducted to identify and integrate relevant concepts, findings, and theories related to the scope of this research. To do so, existing knowledge on digital supply chain- and risk management, risk identification, threat intelligence and information sharing, have been systematically researched and synthesised. Furthermore, this review was used to develop a theoretically grounded framework for the empirical research phase of this study.

Methodologically, a semi-structured literature approach was employed. The review process was operationalised by systematically translating the sub-research questions into defined key search terms and or phrases. This structured operationalisation enhances transparency, scope control, and reproducibility. To ensure academic rigour, the AIS Senior Scholars' basket list of eleven Premier Journals[1] will serve as the primary benchmark. This basket contains the top journals in the field of information systems science. However, due to the interdisciplinary and emerging nature of cybersecurity in supply chains, additional relevant outlets (e.g., AIS Senior Scholars' special interest groups, university accepted cybersecurity and supply chain journals[2]) were included. Only peer-reviewed journal articles are considered, and the papers were carefully selected based on relevance and context. Publications from 2016 onwards are selected to reflect the rapidly evolving nature of cyber supply chain risks, media exposure and increased prominence of risk management regulatory developments (e.g., NIS-Directive, GDPR). Table 1 presents the key search terms used. Abstract and key articles from the results were selected and utilised from snowballing to further identify core/relevant literature. Any theoretical lenses or empirical tools (e.g., constructs or questions) came from related or relevant literature or were developed using the literature review.

Table 1: Key search terms used to research background literature

Conceptual domain	Key Search Terms / Phrases	Results	Chapter(s)
Cyber Supply Chain Risk Management for Digital Supply Chains	"Cyber* supply chain risk management" OR "Cyber* supply chain security" OR "Supply chain security" OR "ICT supply chain risk" OR "Cyber* supply chain attack" OR "Third-party cyber risk"	*90*	2.1 and 2.2
Cyber Risk identification / Awareness	("Cyber" OR "Cloud" OR "Software") AND ("Risk identification" OR "Risk sensing")	*58*	2.3
Information sharing and trust	"Cyber" AND "Risk" AND ("Information Sharing" OR "Collabora*")	*40*	2.4

[1] Senior Scholars Basket - Association for Information Systems (AIS).
[2] Key Journals & Proceedings - Cybersecurity - CMU LibGuides at Carnegie Mellon University; Key journals - Logistics and Supply Chain Management - Guides at Birmingham City University

2.1 Digital Supply Chains are Intertwined Software- and Cloud Supply Chains

Fundamentally, supply chains are recognized as ecosystems of processes, people, organisations, and distributors involved in the creation and delivery of final solutions or products, where there are a constant supplying and consuming effect (Beamon, 1998). Due to digitalisation, modern supply chains can also be seen as networks of organisations interconnected through (communication) technology, working together to utilise information and aiming to protect it (Closs et al., 2004). One new form of these modern supply chains has been named digital supply chains. Examples of such digital services include tax-accounting or financial services, multi-tenant asset monitoring, security operating centres, and supply chain services. For a broader interpretation, the European Union Agency for Cybersecurity (ENISA) defines a digital supply chain as: "the services and infrastructure that deliver or enable the delivery of a digital product used to establish, maintain, develop or restore an organisation's information management and information systems" (ENISA, 2023, p. 41).

2.1.1 Cloud Computing and Software

Cloud computing is a core enabler of these kinds of services. Consumers can participate in digital supply chains by 'connecting' with a provider of a digital service, also known as a cloud service provider. These providers offer computing capability services within the cloud – commonly referred to as Infrastructure-, Network-, Platform, and Software-as-a-Service (ENISA, 2023; Latsiou & Lambrinoudakis, 2026). However, cloud computing services are enabled by cloud supply chains. Akinrolabu et al. defines cloud supply chains as systems of two or more parties that work together to provide, develop, host, manage, monitor or use cloud service (2018). Depending on the service demands regarding security and scalability or performance requirements, cloud service consumers may use publicly shared (public), private - or a hybrid of these two - cloud infrastructure(s) (Durowoju et al., 2011).

The cloud supply chain can be identified by five cloud service-related elements: the cloud service provider, hosting infrastructure, delivery platform, cloud control system, and the cloud consumer (Akinrolabu et al., 2018). Each of these entities maintains its own supply chain. Infrastructure service providers depend on physical locations and ICT service management chains that provide installation, management and operational services, often collaborating with Managed (Security) Service Providers. Cloud Service Providers may depend on Internet Service Providers for connectivity and Application Programming Interfaces (API) providers for system integration (Akinrolabu et al., 2018; ENISA, 2023; Latsiou & Lambrinoudakis, 2026). The introduction of additional cloud-based software services further creates software dependencies (ENSIA, 2023). Software development,

deployment and integration of cloud-native applications have thus increasingly become points of vulnerability, as recent attacks demonstrate (Latsiou & Lambrinoudakis, 2026).

Digital services in the cloud are not created on their own, nor is the software that allows for the cloud supply chain to operate. Accordingly, software supply chains (security) concern the (security of) infrastructure used to build software, as well as software development and delivery processes, including external dependencies such as third-party packages and libraries (Reichert & Obelheiro, 2023). Third-party libraries are essential in modern software development but introduce vulnerabilities that may be difficult to detect due to obfuscation and other technical factors (Zhan et al., 2025). The widespread adoption of open-source software introduces additional governance challenges, requiring Software Composition Analysis measures (Shu et al., 2025). At a deeper technical level, vulnerability detection in binary programs is an important research area, requiring state-of-the-art detection tools (Wang et al., 2023).

2.1.2 Digital Supply Chain Roles

Taking from the existing literature and professional resources, digital supply chains can be understood as the result of intertwined cloud and software supply chains. As per the definition of ENISA, cloud supply chains are the delivering factor and software supply chains are the enabling factor of digital services: creating digital supply chains. These ecosystems consist of cloud-based services and software development activities layered across multiple actors, increasing structural and technical complexity (Reichert & Obelheiro, 2023). Synthesising these works, the following roles within Digital Supply Chains can be identified (see table 2). Up until the digital service consumer, every layer introduces a value provisioning and consuming effect.

Table 2: Distinct Roles that can be identified within Digital Supply Chains

Role	Description
Digital Service Consumer	The entity consuming the digital service through utilisation of the software and underlying information systems in the cloud.
Digital Service Provider	Responsible for delivering the digital service, ensuring Service Level Agreement, and sharing responsibility for compliance and security.
Cloud Service Provider	Hosts and manages cloud computing services enabling digital service delivery.
Infrastructure Provider	Providers hosting infrastructures (servers, routers, firewalls, power and cooling systems), often operating data centres enabling dynamic resource allocation (Kushida et al., 2015).
Software Developing	Develops software at application, platform, infrastructure and hardware layers.
Hardware Provider	Supplies hardware forming the physical cloud infrastructure.

Additional roles may emerge where technologies such as Internet of Things or Blockchains are integrated (Zhang et al., 2019; Islam, 2023). Furthermore, one organisation can possess multiple roles. For example, an organisation may not only provide digital services but also owns actual data centres and allows organisations to gain access to raw cloud computing resources (Microsoft, 2025). The link between traditional supply chains can be found the hardware provider level, where there is a dependency on the hardware manufacturers. These manufacturers are within their own logistical supply chains, most probably concerning the retrieval and processing raw materials.

2.2 Characteristics of Cyber Risks in Digital Supply Chains

As organisations increasingly share information and establish digital information flows across supply chains, risks increase that affect information accuracy, system security, operational continuity and information outsourcing (Tang & Nurmaya Musa, 2011). Organisations that integrate cloud computing into supply chain processes face inherent security risks (Jede & Teuteberg, 2015). For example, sensitive data such as financial records, customer information or supplier contracts stored in cloud environments require protection against unauthorized access (Yenugula et al., 2023). Recent applications of advanced technologies such as Internet of Things and Blockchain expand security concerns while also offering potential mitigation mechanisms (Zhang et al., 2019). For example, blockchain may provide a shared, distributed, transparent and immutable record of data, particularly where trust between supply chain partners is limited (Islam, 2023).

2.2.1 Uncertainty to Security Objectives

Ultimately, cyber- or information security risks in supply chains are probable events with (usually) a negative consequence that may lead to security incidents, such as data breaches or cyber-attacks (Bojanc & Jerman-Blažič, 2013; Latsiou & Lambrinoudakis, 2026). Risks arise when threats exploit vulnerabilities in assets, creating uncertainty regarding the achievement of information security objectives (ISO/IEC 27000, 2018; Boyens et al., 2022). These security objectives commonly aim to maintain the confidentiality, integrity and availability (CIA) of information and -systems (Boyens et al., 2022). As such, cyber risks create uncertainty in the organisations' ability to achieve these objectives.

2.2.2 Key Risks and Characteristic

Latsiou and Lambrinoudakis (2026) identified some key cyber risks regarding digital supply chains, namely: malicious open-source libraries, cloud provider misconfigurations, malicious hardware, phishing attacks and vendor compromises. These cyber risks clearly illustrate the overlap between cloud- and software supply chain complexities respectively, and how cybercriminals can exploit vulnerabilities within (organisations). A defining characteristic of cyber supply chain attacks is the combination of at least two cyber-attacks across two or more parties in the chain (ENISA, 2021). These cyber risks propagate across interconnected actors, rather than remaining isolated within a single organisation. Advanced cyber-attacks frequently exploit software vulnerabilities, and software underpins all layers of cloud services and according to ENISA (2021), 50% of reported supply chain attacks were attributed to known Advanced Persistent Threat groups. A vulnerability refers to a

weakness in an information system, organisation or security measure that can be exploited by one or more threats. Vulnerabilities in digital supply chains may exist at multiple levels: technical components, organisational processes, and implemented security controls.

2.2.3 Technical, Control and Organisational Vulnerabilities

Technical vulnerabilities include unpatched systems, misconfigurations, insecure APIs, embedded malicious code, and zero-day exploits. Unfortunately, structural economic incentives often disincentivize proactive security investments by software vendors that perhaps could have prevented these technical vulnerabilities (Anderson & Moore, 2006). These finding stresses risk identification in outsourced digital environments. Technical risk assessment frameworks emphasize structured asset identification, vulnerability extraction and mapping, and risk calculation (Shakibazad & Jabbar Rashidi, 2019). These approaches rely heavily on vulnerability knowledge repositories such as CVE and CVSS databases, which are supported by coordinated vulnerability disclosure processes that accelerate patch development (Arora et al., 2010). Control-based vulnerabilities may arise when implemented measures are poorly designed, implemented or monitored.

Given the distributed nature of digital supply chains, organisations often lack (direct) visibility into supplier controls. To combat this, organisations request assurance reports, such as System and Organisational Controls (SOC), to provide independently audited assurance regarding controls that ensure the functioning of security, availability, processing integrity, confidentiality, and privacy controls (Hampton et al., 2021). Organisational vulnerabilities include insufficient supplier oversight, inadequate contractual security clauses, and a lack of security awareness. As such, third-party security questionnaires and vendor audits may attempt to reduce information asymmetry regarding supplier risk posture (Latsiou & Lambrinoudakis, 2026).

2.3 Requiring Threat Information to Become Aware

Professional resources provide practices and guidelines for cyber supply chain risk management (Latsiou & Lambrinoudakis, 2026). The National Institute of Standards and Technology (NIST) defines cyber supply chain risk management as: “a systematic process for managing exposure to cybersecurity risks through the supply chain and developing appropriate response strategies, policies, processes, and procedures” (Boyens et al., 2022, p. 17). Risks stemming from supply chains can be accepted, avoided, transferred or mitigated. Cyber supply chain risk management is essential for protecting data and assets against cyber risks in digital supply chains (Shakibazad & Jabbar Rashidi, 2019; Latsiou & Lambrinoudakis, 2026).

Past studies indicate that effective cyber supply chain risk management requires both strong organisational oversight and proper technical measures (Latsiou & Lambrinoudakis, 2026). Given complex inter-organisational relationships involving trust, power and commitment, the demand for effective Cyber supply chain risk management has increased (Hampton et al., 2021). In digital supply chains, the process of managing cyber risks becomes complex due to layered software dependencies, cloud-service outsourcing, and multi-tier supplier ecosystems. Risks may originate not only within the organisation, but across interconnected cloud infrastructures and software. Accordingly, insight into all the possible vulnerabilities and threats within cloud and digital solutions is critical to understand risks (Yenugula et al., 2023). However, the effectiveness of mitigation measures depends on the specific risk that has been identified.

2.3.1 Identification Requires Awareness, which requires Information

Identifying and evaluating risks is usually a systematic practice in cyber supply chain risk management, where appropriate security measures are selected based on acceptable security levels (Bojanc & Jerman-Blažič, 2013). Risk identification refers to the systematic process of finding, recognizing and describing risks by analysing their sources, causes, events and potential consequences (ISO/IEC 27000, 2018). In information system security, this involves identifying critical assets, potential threats, exploitable vulnerabilities, existing controls, and possible impacts.

Risk identification can be qualitative or quantitative, static or dynamic, and increasingly hybrid in digital environments (ISO/IEC 27000, 2018; Shakibazad & Jabbar Rashidi, 2019). However, due to resource constraints and limited historical data, risk assessments are usually done qualitatively, relying on experience and professional knowledge and awareness of relevant risks (Wheeler, 2011). As explored before, digital supply chains represent highly uncertain environments regarding the

achievement of security objectives. Organisations rely on multiple external service providers, software components, and interconnected – sometimes cross international border – infrastructures, while having limited information into the security practices and vulnerabilities of external partners (Yenugula et al., 2023), to identify risks.

According to the European Union Agency for Cybersecurity (ENISA), cybersecurity risks in supply chains should be monitored using internal and external sources of information, and on findings from suppliers' performance monitoring and reviews (ENISA, 2021). However, static vulnerability databases alone do not provide complete information into a dynamic threat landscape, as it is argued that threat intelligence complements the ability to identify vulnerabilities to further improve assessing of risks (Chismon & Ruks, 2015; Shakibazad & Jabbar Rashidi, 2019).

2.3.2 Threat Intelligence to Process Information for Awareness

A cyber threat consists of a potential and unwanted incident that can harm an information (system) caused by an actor, such as a hacker or another incident from the supply chain (Nishat Faisal et al., 2007; Abdelmagid et al., 2025). Common digital supply chain threats, as explored before, include malware infections, phishing attacks and social engineering, ransomware, embedded malicious code or poor-quality products/services (Latsiou & Lambrinoudakis, 2026). Cyber Threat Intelligence (CTI) enhances risk identification by transforming raw threat data into actionable knowledge that supports decision-making (McMillan, 2013). Rather than focusing solely on known vulnerabilities, CTI aims to anticipate and interpret emerging threats, thereby reducing the window between compromise and detection (Chismon & Ruks, 2015). The threat intelligence cycle typically consists of *1)* Requirements definition; *2)* Collection from diverse formal and informal sources; *3)* Analysis and contextualisation; *4)* Dissemination and finally *5)* Evaluation.

This cyclical process enables organisations to move from "unknown unknowns" to actionable threat landscape insight. (Chismon & Ruks, 2015). Adequate threat intelligence information should be relevant, actionable and valuable (Dalziel, 2015). Relevant assumes that the information relates to or potentially relates to the organisation, industry, network or other relational factor. Actionable states the ability to respond, change, act or make decisions with the information, and valuable means that there should be a useful business outcome.

Threat information is most often tactical or technical in nature (Chismon & Ruks, 2015). Technical threat intelligence focuses on indicators of compromise (IoCs), such as malicious IP addresses, file hashes, malicious libraries, and anomalous network behaviours (Dalziel, 2015; Ray, 2015). IoCs can

also be created by learning from past incidents (Dalziel, 2015). Tactical Threat Intelligence provides insights into adversarial tactics, techniques, and procedures (TTPs), often structured through frameworks such as MITRE ATT&CK (The MITRA Corporation, 2015). Operational and strategic threat intelligence tend to be less present in non-governmental organizations due to complexity in information gathering (Tang & Musa, 2011). Additionally, organisations should invest in incident response and individual threat analysis capabilities (Ring, 2014).

Threat information or intelligence can be gathered formally and informally, where the difference is mostly the source it comes from (Ahrend et al., 2016). For example, a published incident report or vendor services that gathers, analyses and produces threat intelligence may be considered formal. On the other hand, informal gathering entails informal reports, conversations with defenders or investigators on the nature of attacks and trends in methodologies or communicating with peers. As such, the value of collecting from human sources should not be underestimated as the ability to 'catch-up' with a peer can be highly valuable (Chismon & Ruks, 2015).

In digital supply chains, where risks may propagate across interdependent systems, threat intelligence complements vulnerability identification by contextualising how vulnerabilities are actively exploited (Shakibazad & Jabbar Rashidi, 2019). Recent analysis of supply chain incidents demonstrates that integrating threat intelligence frameworks such as MITRA ATT&CK improves systematic identification of exploitation pathways across suppliers (Kampourakis et al., 2025). However, while technical standards and intelligence repositories provide structured knowledge, effective risk identification ultimately depends on the organisation's ability to process, integrate, and interpret externally sourced information, including that of threat information.

2.3.3 Information Processing Theory Applied to Cyber Threat Intelligence

The threatening nature of cyber threats amplify uncertainty on organisations' ability to achieve their security objectives. Naseer et al. (2021) has applied Information Processing Theory to explain the uncertainty effect of cyber threat environments and found that utilising business analytics to process threat information enhances an organisations' awareness of cyber threats. Information Processing Theory (IPT) conceptualises organisations as systems that must process information to cope with environmental uncertainty (Galbraith, 1974; Tushman & Nadler, 1978). Uncertainty arises when the information required to perform organisational tasks exceeds the information available to the organisation, or in other words the absence of information. To manage uncertainty, organisations must either reduce information processing requirements or seek and acquire more information to

reduce uncertainty (Zack, 2007). To link the relationship between needing, acquiring and processing threat information, the theoretical framework (see figure 1) is proposed.

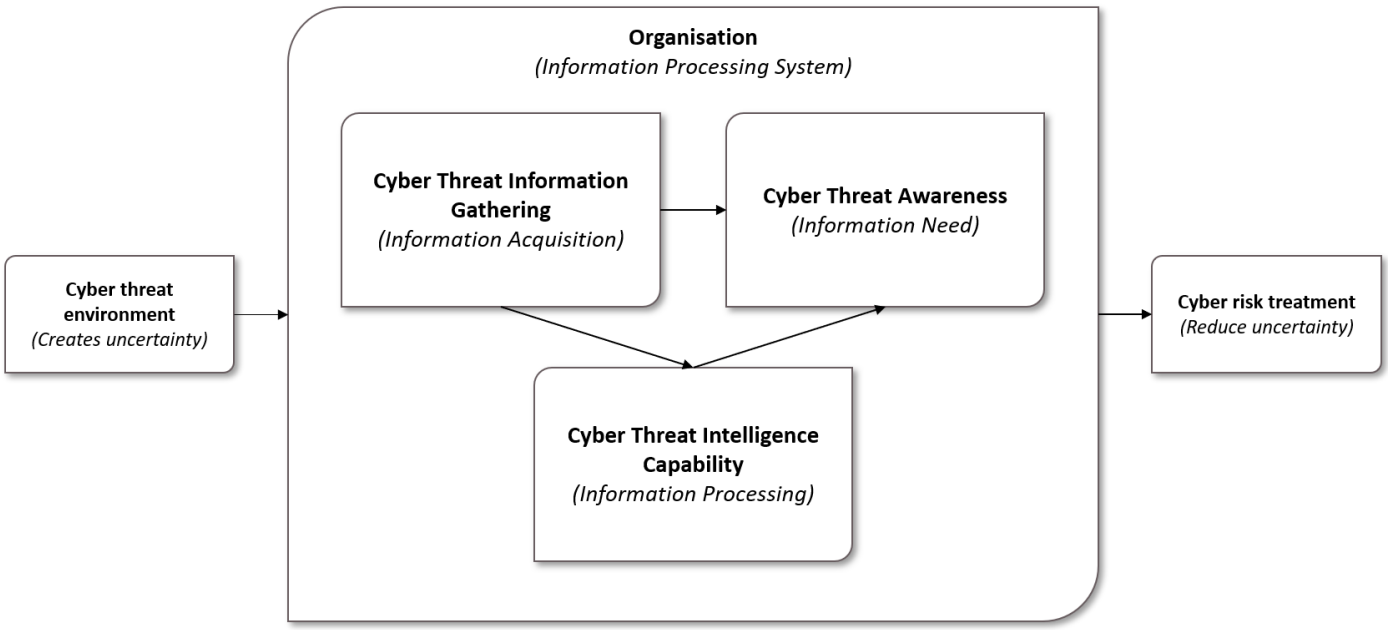

Figure 1: Theoretical framework illustrating Cyber Threat Intelligence in the Context of Information Processing Theory

Information Processing Theory explains and links the need for cyber threat information to become aware and identify risks following mitigation to reduce uncertainty. As found by Naseer et al (2021), organisations use analytical information to enhance their cybersecurity awareness to proactively with dynamic cyber threat environments. As using business analytics, vendors services or chatting with other professional, cyber threat information or data can be gathered formally or informally (Chismon & Ruks, 2015; Ahrend et al., 2016). Depending on whether the information/data is (already) of quality, additional a cyber threat intelligence capability is required to analyse, process and report findings for evaluation. Having gained or gathered cyber threat information, organisations can fill in the historical information gaps or create the opportunity to benefit from professional knowledge to create awareness and identify risks (Wheeler, 2011; Naseer et al, 2021). Moreover, organisations that find it challenging to gather cyber threat data can benefit from formally or informally but externally gathered cyber threat information to create awareness (Ring, 2014).

Considering the literature and theoretical lens, the first hypothesis is proposed on the association of cyber threat intelligence capability in relation to digital supply chain cyber threat awareness to answer the first sub-research question (*RQ1*):

> H_1: *Cyber Threat Intelligence Capability is positively associated with Digital Supply Chain Cyber Threat Awareness.*

2.4 Sharing Cyber Threat Information and the Role of Trust

The increasing interconnectedness of digital supply chains has intensified the need for organisations to exchange cyber threat information beyond their organisational boundaries. Guidance from NIST emphasizes close collaboration with key suppliers and partners, including information communication channels, to support the identification and management of cybersecurity risks (Boyens et al., 2021). In digitally interdependent environments, organisations often lack full awareness and information about vulnerabilities and threat exposure affecting upstream of downstream partners. External cyber threat information sharing therefore can become an important mechanism for extending organisational insight beyond internal systems.

2.4.1 Sharing Threat Information Can Improve Awareness

Organisations are encouraged to share technical details extracted from known attack methods, including IoCs, adversarial tactics, and vulnerability disclosures, to strengthen security measures such as intrusion detection and prevention systems (Delvecchio et al., 2025). These technologies depend on knowledge of known threats and are therefore enhanced by timely and high-quality intelligence (Tounsi & Rais, 2018). Big data, (open source) threat intelligence tools and communication standards can enable these conditions. Access to shared threat intelligence enables organisations to anticipate emerging attack patterns, prevent operational disruptions, and improve overall security posture (Preuveneers & Joosen, 2023). Furthermore, shared intelligence contributes to more efficient network risk assessment and security hardening processes (Qamar et al., 2017).

Beyond structured vulnerability disclosure tools and automated feeds, tactical threat intelligence is frequently exchanged through voluntary and information collaboration among organisations. Such exchanges may involve sharing knowledge of past incidents, threat actor behaviour, defensive strategies, or mitigation practices. Public–private information sharing initiatives have been argued to accelerate the identification and detection of cyber threats (Peretti, 2014), as Governmental agencies tend to have a higher threat intelligence capability (Tang & Musa, 2011). Participation in such exchanges may also be cost-effective, particularly for organisations with limited internal threat intelligence capabilities, as it allows them to benefit from collective expertise and shared analytical resources (Ring, 2014).

Sector-specific information sharing arrangements are often recommended, as organisations operating within similar industries tend to face comparable threat landscapes and risk profiles, which could lead to better situational awareness and deeper understanding of the threat landscape (Zheng & Lewis,

2015). This idea has been approved in a survey, where 700~ IT and -security practitioners agreed that exchanging cyber threat intelligence can improve security posture and situational awareness (Ponemon, 2015). In many cases, these organisations are also embedded within overlapping or connected supply chains, further increasing the relevance of shared intelligence. Through these mechanisms, external cyber threat information sharing can expand the informational boundaries of organisations, thereby enhancing their awareness into cyber threats that may propagate across digitally interconnected supply chain networks.

However, despite normative recommendations advocating increased collaboration, empirical evidence remains limited regarding the practical effectiveness of information cyber threat information sharing (Tounsi & Rais, 2018; Preuveneers & Joosen, 2023). Limited research has examined how such external exchanges contribute specifically to digital supply chain threat awareness, not general cyber risks. In regard to the IPT-framework proposed (see Figure 1), inter-organisational cyber threat information sharing can be seen as a method of gathering threat intelligence, and as such, in combination with past research, this study proposes the following second hypothesis that also supplements the answer of the first sub-research question (*RQ1*):

> H_2: *Inter-organisational Cyber Threat Information Sharing is positively associated with Digital Supply Chain Cyber Threat Awareness.*

The emphasis here is on peer-industry inter-organisational sharing. Where similarities in threat landscape are also expected to result in a positive association with awareness.

2.4.2 Organisational and Information Quality Trust Manifestations

When exchanging between organisations, trust can mainly manifest itself in two ways. Trust in the quality of information exchanged, and trust in the organisation(s) that participate in the information exchange. Empirical findings suggest that organizations are more willing to engage in information sharing when they trust the platform or community and perceive the exchanged information as relevant, accurate, and timely (Zibak et al., 2022). As previously discussed, these are similar aspects of qualitative cyber threat intelligence (Dalziel, 2015), and this makes sense as organisations need quality information to deal with uncertainty and improve their decision-making according to IPT (Galbraith, 1974). Moreover, inaccuracies, incompleteness and out-of-date (actionable) are perceived problems with cyber threat information that could lower the trust in information quality (Ring, 2014). When the perceived information quality is low, the utilisation of said information received when participating in information exchange may lead to less awareness. As such, a higher perceived trustworthiness of the externally exchanged cyber threat information may increase awareness, including that of cyber threats in digital supply chains. Accordingly, the third and last hypothesis is proposed to fully answer the first sub-research question (*RQ1*):

> H_3: *Information Quality Trust is positively associated with Digital Supply Chain Cyber Threat Awareness.*

Furthermore, if reciprocity is uncertain, participation levels may decline as organizations evaluate the potential benefits of sharing against associated risks. When perceived gains - such as reciprocal access to intelligence, improved collective defence, or enhanced preparedness - outweigh privacy, reputational, or legal concerns, organizations may reach a threshold at which sharing becomes more likely (Ezhei & Tork Ladani, 2017).

Although the benefits of external cyber threat information sharing are acknowledged, organisations often hesitate to disclose sensitive information. Effective information sharing requires alignment across legal, regulatory, technological, and organisation dimensions (Skopik et al., 2016). Differences in regulatory frameworks, data protection obligations, and liability concerns may create uncertainty regarding the permissibility and consequences of sharing threat-related information. Confidentiality and reputational considerations further influence organizational behaviour. Firms may fear that disclosing incidents or vulnerabilities could lead to negative publicity, loss of customer trust, or competitive disadvantage (Peretti, 2014; Tounsi & Rais, 2018). As Chismon and Ruks state (2015), informally exchanging threat information should not lead to the exposure of business plans to competitors.

Additionally, organizations may be concerned that locally collected cyber threat intelligence could be misused or weaponized if shared inappropriately. However, modern threat intelligence platforms attempt to address some of these concerns through anonymization and privacy-preserving mechanisms (Preuveneers & Joosen, 2023). Although private-public information sharing is argued to improve identification of threats, private-private information sharing could be less prevalent as compared to public-public information sharing, due to these factors creating an inherent lack of trust amongst competing organisations.

Similarly, the perceived trust in information quality for private-private sharing organisations can differ from that of public-public sharing. If there is an association between information sharing and trust in information quality, this could perhaps adjust the digital supply chain cyber threat awareness. As such, the final two hypotheses are proposed that make up the second and third sub-research questions *(RQ2 & RQ3*):

> H_4: *Public and private organisations differ significantly in inter-organisational information sharing and/or trust in information quality.*
>
> H_5: *Public and private organisations differ significantly in digital supply chain cyber threat awareness.*

3 Research Methodology

3.1 Research Design

In order to address the main question of this preliminary research – "How are inter-organisational cyber threat information sharing and information quality trust associated with digital supply chain threat awareness among information security managers in European public and private organisations?" – three sub-research questions were formulated to structure the research process: 1) How are cyber threat intelligence, information sharing and information quality trust associated with digital supply chain cyber threat awareness?; 2) To what extent do public and private organisations differ in information sharing and trust?; And lastly, 3) To what extent do public and private organisations differ in digital supply chain cyber threat awareness? By synthesising existing key literature and utilising Information Processing Theory as a lens, a theoretical framework was proposed, which was the basis for the hypotheses that are linked to each sub-research question.

This study adopts a quantitative survey-based research design to explore statistical associations and differences to the respective study variables: cyber threat intelligence capability, inter-organisational cyber threat information sharing (in the context of public-public and private-private), trust in information quality and their respective associations with digital supply chain cyber threat awareness among information security managing roles in digital service consuming organisations. A qualitative interview-based approach was not selected for this study as the primary objective was not to explore perceptions or experiences in depth, but to test theoretically derived hypotheses regarding the study variables. According to Sekaran and Bougie (2019), quantitative research is appropriate when researchers seek to measure concepts systematically and analyse relationships between using statistical techniques to test hypotheses. Although interviews could have provided richer contextual insight, extensive literature including qualitative data is present, which – in combination with the interest of the supporting organisation of the researcher – prioritised the statistical analysis to conclude at a broader scale.

The research is deductive in nature, drawing on established literature which has previously examined (1) the general role of cyber threat information sharing in improving organisational cyber threat awareness, and (2) the role of trust as an antecedent and mechanism in inter-organisational information exchange. However, this study extends existing work by providing a preliminary empirical examination of how these associations manifest specifically within the context of digital supply chain cyber threat awareness, particularly from the perspective of information security

managers that communicate with industry peers; as public-private sharing has already been understood to be effective. To the best of the researcher's knowledge, limited empirical work has focused on modelling trust and information sharing in relation to digital supply chain cyber threat awareness at the level of digital service-consuming organisations.

Given the evolving and underexplored nature of this domain, particularly in the context of increasingly interconnected digital ecosystems, this study is positioned as an initial exploratory step toward understanding how inter-organisational information flows may contribute to closing awareness gaps that cannot be addressed through internal capabilities alone. Furthermore, additional exploratory analyses were conducted to examine potential differences between public and private organisations across the study variables.

3.1.1 Construct Definitions and Scopes

Based on the reviewed literature and applied theoretical lens (IPT), this study operationalises four primary constructs (see table 3) in the context of this research reflecting information acquisition, information processing capability, and the need to gain cyber threat awareness ultimately to reduce uncertainty from digital supply chain threats.

Table 3: Defined Construct using Information Processing Theory

Construct	Definition and scope	Reference(s)
Inter-organisational Cyber Threat Information Sharing (*independent*)	The voluntary participation in exchanging informal cyber threat information between industry peers and sector-specific communities (*Information Acquiring*). Includes indicators of compromises (IoCs), adversarial tactics and techniques (TTPs), vulnerability disclosure, incident experience and threat intelligence insights obtained.	Chismon & Ruks, 2015; Ahrend et al., 2016; Delvecchio et al., 2025; Kampourakis et al., 2025.
Cyber Threat Intelligence Capability (*independent*)	An organisations' internal capability to collect, analyse, contextualise and operationalise quality cyber threat information (*Information Processing*). Includes dedicated intelligence analysts, analytical tools, intelligence platforms, correlation mechanisms and processes that transform raw information into technical or tactical intelligence.	Chismon & Ruks, 2015; Shakibazad & Jabbar Rashidi, 2019;
Information Quality Trust (*independent*)	The perceived trust in quality of information regarding acquired shared cyber threat information. Includes the perception of relevant, accurate and actionable information that can be trusted and is perceived to be of quality.	Ring, 2014; Dalziel, 2015; Zibak et al., 2022.
Digital Supply Chain Cyber Threat Awareness (*dependent*)	Perceived extent to which an organisation processes knowledge of cyber threats affecting entities/systems within its digital supply chain(s) that threatens own information systems (*Information Need*). Reflects awareness of emerging threat actors, attack techniques, exploited vulnerabilities, and potential threat propagation paths across interconnected supply chain partners that can threaten its own information systems.	Wheeler, 2011; Ring, 2014; Dalziel, 2015; Naseer et al., 2021.

Furthermore, this study aims to explore some descriptive information regarding what digital services are used by organisations, the possible impact of recent incidents on awareness, commonly perceived technical incident causes and nature of incidents regarding digital supply chains. Additionally, whether the organisation operates publicly or privately has also been captured in this study as it is of interest to explore the differences in between. Besides acting as the more explorative part of this research, the European Union Agency for Cybersecurity (ENISA) maintains a database with likewise data for the latter two. This will create an opportunity to compare results and further add context to data and thus results.

3.1.2 Conceptual Model and Hypotheses

Drawing from the reviewed literature, proposed IPT cyber threat intelligence and answers from the previous sub-questions, the following conceptual model (see figure 2) was constructed using the definitions and scope from the constructs and utilised to perform the quantitative research.

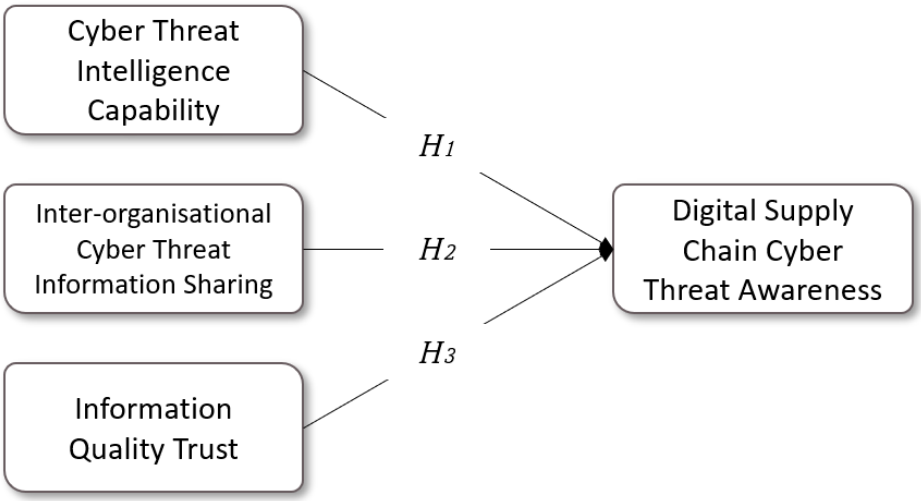

Figure 2: Conceptual Model

This conceptual model outlines the focus of this research, namely the first sub-question (*RQ1*): How are cyber threat intelligence, information sharing and trust in information quality associated with digital supply chain cyber threat awareness? The variables in the conceptual model will thus be in the examining scope of this research.

In relation to IPT, Inter-organisational cyber threat information sharing (ICTIS) acts as the information gathering and acquiring elements and aims to measure the perceived participation in information sharing. Directly, or due to threat intelligence processing, this information sharing contributes to the awareness of digital supply chain cyber threats (DSCCTA) as perceived by information security managers. In this model, the perceived trust in information quality (IQT) of the acquired cyber threat information is speculated to influence the relationship between sharing and gaining awareness.

Table 4 contains the hypotheses that were derived from the literature review section, each with their respective null-variant. These hypotheses help understanding the associations and aims to provide context to and answer the sub-questions at hand. This includes the exploratory part of this thesis, which comes down to examining the potential differences between organisational type and the respective study variables. As such, hypothesis 1-3 relate to the main constructs and assumed associations in this study, as seen in the conceptual model.

Table 4: Defined hypotheses

H	Hypothesis (H_n)	Null hypothesis (H_0)	RQ
H_1	Cyber Threat Intelligence Capability is positively associated with Digital Supply Chain Cyber Threat Awareness.	Cyber Threat Intelligence Capability is not significantly positively associated with Digital Supply Chain Cyber Threat Awareness.	*RQ1*
H_2	Inter-organisational Cyber Threat Information Sharing is positively associated with Digital Supply Chain Cyber Threat Awareness.	Inter-organisational Cyber Threat Information Sharing is not significantly positively associated with Digital Supply Chain Cyber Threat Awareness.	*RQ1*
H_3	Information Quality Trust is positively associated with Digital Supply Chain Cyber Threat Awareness.	Information Quality Trust is not significantly positively associated with Digital Supply Chain Cyber Threat Awareness.	*RQ1*
H_{4a}	There is a significant difference in Inter-organisational Information Sharing between public and private organisations.	There is no significant difference in Inter-organisational Information Sharing between public and private organisations.	*RQ2*
H_{4b}	There is a significant difference in Information Quality Trust between public and private organisations.	There is no significant difference in Information Quality Trust between public and private organisations.	*RQ2*
H_5	There is a significant difference in Digital Supply Chain Cyber Threat Awareness between public and private organisations.	There is no significant difference in Digital Supply Chain Cyber Threat Awareness between public and private organisations.	*RQ3*

Afterwards, hypotheses H_{4a}, H_{4b} and H_5 will be tested as these are complementary to examine the potential differences between public and private organisations; which will help answering the second and third sub-research questions: To what extent do public and private organisations differ in sharing and trust? And to what extent do public and private organisations differ in digital supply chain cyber threat awareness?

Besides the organisational type, other variables were included for descriptive and exploratory subgroup analysis:

| *number of employees* (organisation size): Larger organisations tend to have more information system related capabilities, including security and threat intelligence capabilities.

| *number of digital services*: Supply chain complexity, size and amounts connected to can influence the perceived awareness, but this is very cognitively taxing to ask and difficult to measure. The number of digital services will act as a proxy that the more services an organisation has can negatively influence the perceived awareness.

| *Significant security incident occurrence*: Questions the occurrence of a significant incident in its digital supply chain within the last 12 months. This could influence the awareness of threats in digital supply chain(s).

Lastly, the participants' role and amount of experience will be examined, as well as what digital services are used, and the commonly perceived incident natures and causes. The above mentioned variables, and the roles and digital services have been defined using the experience of the researchers' supervisor at the hosting organisation and . The incident natures and causes have been extracted from ENISA (2023b) incident reports.

3.2 Research Participants and Sample Selection

The research participants of this study consist of information security managers, as these roles are directly involved in overseeing and managing the security of information and -systems within their organisation. Given that the aim of the study is to generate insights relevant for governance and policy development, these professionals were considered the most appropriate respondents due to their strategy and operational involvement in cyber risk management and information security decision-making. The following roles have been selected to match the information security manager role: CISO / Head of Information Security, Information Security Manager, Cybersecurity Manager, Information Security Officer and IT Risk Manager.

The sample selection focused on organisations operating within the European Union, with a specific emphasis on the Netherlands due to data collection feasibility and contextual relevance. This geographic focus is also relevant considering the NIS2 Directive, which strengthens cybersecurity requirements and introduces obligations related to cyber threat information sharing for entities operating within critical and important sectors. To ensure variation across organisational contexts, both public and private organisations were included in the sample. Targeted sectors included insurance companies, banks, portfolio management and financial services, as well as hospitals, care providers, and government and public administration organisations. These sectors were selected because they are generally covered under the NIS2 Directive and are therefore more likely to be engaged in structured cybersecurity governance and, to some extent, cyber threat information sharing practices. However, participation was not strictly limited to these sectors, and respondents from other relevant organisations were also allowed to participate in cases where response rates were limited.

It should be noted that no formal registry exists that accurately quantifies the total number of individuals occupying information security management roles within the Netherlands. As a result, the sample was obtained using non-probability sampling methods, which limits the ability to determine response rate and affects the generalisability of the findings.

3.3 Research Process

3.3.1 Survey Preparation

Ironically, a cloud-based survey service was purchased for the creation and deployment of the survey[3]. The configuration of this survey service left all the collected data to be completely confidential and anonymous at both personal and organisational level, which was considered essential to increase the likelihood of participation.

The survey was constructed that - amongst other measurements - contained the measures of constructs to operationalise the data collection phase. The defined constructs and scope in Table 3 were translated into multiple (5-6) measures of constructs leaning on similar construct sentence statements (Appendix A: Survey Measures of Constructs). Due to the relative sensitive nature of this data, the researcher has chosen to use a European based survey software solution to avoid geopolitical tensions and ensure full organisational and personal anonymity. A welcome page was made that contains a summary of the research objective, survey effort summary, anonymity statement, mention on where the data will be located and a statement of consent by continuing the survey (Appendix B: Survey Setup). The measure of construct elements was quantified using the Likert-scale method, ranging from 1 = strongly disagree to 7 = strongly agree. This scale transforms subjective attitudes and opinions into quantitative data that will be used for statistical testing. This design choice ensures that a quantitative statistical analysis is possible. The participant was informed about the research and the respective objectives, data storing method including anonymity and was asked for consent by continuing to participate and thanked at the end of the survey.

3.3.2 Data Collection

The data was collected between the by 22nd of April until the 30th of May. As the main headquarters of the organisation the researcher worked at during the time of this research was in the Netherlands, mainly Dutch professionals were targeted. Expert non-probability sampling was used due to the need of expert knowledge on the individuals of interest in this research in combination with an unknow population size – other than the approximation. Non-probability sample methods were used to contact the information security managers, mainly because of their difficulties in reachability. Participation invites were sent via e-mails to clients that fell within the targeted population extracted from a client list. Furthermore, the networks of colleague's and classmates were used to contact information

[3] LimeSurvey, a software that offers secure survey deployment and anonymous data hosting on German servers – considering the geopolitical tensions – which negates the American Clarifying Lawful Overseas Use of Data (Cloud) Act.

security managers directly via e-mail or by telephone. LinkedIn, the social media platform, was also employed to reach information security managers. Direct messages were sent to the professionals that fit the selected organisations and defined roles. Additionally, a post was made asking professionals to participate in the research. The researcher ensured in personal contact that the same organisation or legal entity were not requested to participate twice. As stated before, the survey service offers complete personal and organisational anonymity. No IP-addresses or other identifiable information were collected. The researcher hoped this encouraged the willingness of (potential) participants to participate and respond truthfully.

3.3.3 Data Processing and Analysis Methods

The results from survey were exported into a .csv file format and stored in line with the data management plan (Appendix C: Data Management Plan). This allowed the researcher to normalise, structure and sanitise the data using python, specifically the Pandas dataset management library (Appendix D: Python Data Sanitisation Script). Column names were changed for adequate analysis, and a python script was created and used to filter out any incomplete and unusable data, including respondents that did not pass the screening question. The organisation size variable was also split into high-low sections based, including the number of digital services. The middle point was used to make this separation, specifically for organisation size followed that >250 employees and 20-50 digital services and onwards were considered high.

The software R was subsequently used to further sanity-check the data and perform the statistical analysis required (Appendix E: R Descriptive Analysis and Statistical Testing Code (polished)). A straight-lining detection module was used to examine the number of unthoughtful answers.Descriptive statistics were used to summarize and understand the characteristics of the sample data, including respondent role, organisation size and type, amongst other data. The variables of this study (CTIC, ICTIS, IQT and DSCCTA) were assessed for internal consistency and reliability using Cronbach's alpha. Furthermore, the Central Limit Theorem and normality assumptions were assessed by inspecting distributional characteristics (mean, standard deviation, skewness and kurtosis), as well as visually using boxplots and histograms.

Before executing the hypothesis testing, additional statistical assumptions were evaluated. For correlation analyses, monotonicity was assessed visually using scatterplots. For group comparisons, assumptions underlying MANOVA were examined, including homogeneity of covariance matrices using Box's M test and inspection of distributional properties. Although examining the differences in cyber threat intelligence capability between public and private organisations is not of interest in this

research, it will be considered when executing the multivariate assumptions due to its possible effect when combined in the analysis.

Due to the limiting sample size and violations, the Spearman's correlation test was applied. Furthermore, given violations of multivariate assumptions for some grouping variables, Pillai's Trace was used as the primary multivariate test due to its robustness. In addition, non-parametric testing (Wilcoxon rank-sum test) was applied as a robustness check for key group differences. For all statistical tests, a significance (p-value) of <0.05 (α) was used as a threshold. Where relevant, the tests were performed bidirectionally (two-tailed).

3.3.4 Validity and Reliability

Responses failing the screening question or containing excessive missing data will be excluded from the analysis. Straight-lining testing was done to preserve data quality. Construct validity was addressed by grounding all constructs in the existing literature, applying the before used theoretical lens Information Processing Theory, and operationalising them using multiple survey items. In addition, findings from ENISA (2023b) incident reports were used as an external benchmark to support construct relevance and ensure that the measurement of DSCCTA reflects current and realistic threat environments. ENISA data from 2020–2024, aligned with NIS2 sector classifications, indicate that most incidents in digital services and digital infrastructure contexts are caused by malicious actions and system failures, with common attack types including DDoS, malware, and ransomware. These insights informed the conceptual grounding of the DSCCTA construct and aimed to ensure alignment between survey items and real-world cyber threat conditions.

A pilot survey test was conducted to assess clarity and face validity of the survey items, ensuring that questions were interpreted consistently by respondents. During the pilot, the survey items were reviewed by two IT security and risk management consultants to ensure clarity, relevance, and interpretability prior to data collection. Their respective feedback was processed where deemed necessary.

Internal consistency and reliability were assessed using Cronbach's alpha, with all multi-item constructs exceeding the acceptable threshold of 0.68 as these are new constructs. To assess statistical assumptions underlying the analysis, distributional properties per the Central Limit Theorem and normality were examined using descriptive statistics (mean, standard deviation, skewness, and kurtosis) and visual inspection through boxplots. For group comparisons, homogeneity of covariance matrices was assessed using Box's M test, and where violations were observed, Pillai's Trace was

used as a robust multivariate test statistic. In addition, non-parametric testing (Wilcoxon rank-sum test) was applied as a robustness check for key group differences.

To reduce common method bias, respondent anonymity was ensured to minimise evaluation apprehension and social desirability effects. In addition, item ordering was varied to reduce systematic response patterns by breaking up the responding to Likert-scale based questions.

3.3.5 Reporting and Concluding

The results section contains all the descriptive, assumption test and hypotheses and group distinction testing results, including a summary of the sample and its descriptive variables. The results were interpreted, conclusions were made, as well as recommendations, implications and discussion points and proposals for further research.

Following the completion of the statistical analysis, two Chief Information Security Officers from a public and private organisation were consulted during an Expert Consultation Session (Appendix F: Expert Consultation Session). The purpose of the session was to discuss and contextualise the findings of the study, discuss potential explanations for the observed results, and identify practical implications. The session was not part of the formal data collection process and was therefore solely used to support the interpretation of the findings relevant and add to/change the existing discussion points.

4 Results

4.1 Characteristics of Respondents in Sample

The survey yielded a total of 38 responses during the data collection phase, whereof six were empty and thus not usable. Furthermore, the confirmation of operating within an Information Security Management role left out another response. In total, the collection phase resulted in 31 usable responses ($n = 31$). Table 5 shows the characteristics of the sample size.

Table 5: Overview of Sample Organisational Characteristics

Characteristic	*Private* N = 14[1]	*Public* N = 17[1]
Size		
<50	3 (21%)	0 (0%)
50-249	4 (29%)	1 (5.9%)
250-1000	1 (7.1%)	4 (24%)
>1000	6 (43%)	12 (71%)
Organisation		
Banking	0 (0%)	1 (5.9%)
Insurance	3 (21%)	0 (0%)
Portfolio management/financial services	4 (29%)	0 (0%)
Care providing	0 (0%)	3 (18%)
Government services / public administration	0 (0%)	8 (47%)
Hospital	0 (0%)	3 (18%)
Other	7 (50%)	2 (12%)
Role		
CISO / Head of Information Security	6 (43%)	7 (41%)
Cybersecurity Manager	0 (0%)	1 (5.9%)
Information Security Manager	1 (7.1%)	1 (5.9%)
Information Security Officer	5 (36%)	7 (41%)
IT Risk Manager	2 (14%)	1 (5.9%)
Experience		
<2 years	2 (14%)	1 (5.9%)
2-5 years	6 (43%)	8 (47%)
>5 years	6 (43%)	8 (47%)

[1]n = 31

As stated, the final sample consisted of 31 respondents, including 14 respondents from private and 17 from public organisations. Most participants were from large organisations with more than 1.000 employees (>1000), representing 43% of the private organisations and 71% of the public organisations. Smaller organisations with fewer than 50 employees were only represented within the private sector sample (21%). Medium-sized organisations operating between 250 and 1.000

employees accounted for 7.1% of the private organisations and 24% of public organisations, while organisations with 50-249 employees represented 29% of private organisations and 5.9% of public. Sectoral differences can be observed between the public and private organisation groups. Public sector respondents primarily represented government services and public administration organisations (47%), followed by hospitals (18%) and care-providing organisations (18%). In contrast, private sector respondents mainly represented organisations classified as “other” (50%), insurance organisations (21%), and portfolio management or financial services organisations (29%). The only banking organisation is part of the public organisation group (5.9%). As for the respondent roles, most participants occupied senior information security management positions (CISO, -managers).

Among private organizations, 43% of respondents held the role of Chief Information Security Officer or Head of Information Security, while 36% were Information Security Officers. Similarly, the public organisations group holds mostly CISOs and Information Security Officers. Cybersecurity managers were only represented within the public organisations group (5.9%), whereas IT Risk Managers accounted for 14% of private respondents and 5.9% of public respondents. Most respondents reported holding experiences on the higher ends. Within both the private and public organisation groups, 43-47% of respondents reported between two and five years of experience, while an additional 43-47% reported more than 5 years of experience. Respondents with fewer than two years of experience represented a relatively small proportion of the sample.

Table 6 shows an overview of the organisation size and the respective number of digital services consumed.

Table 6: Overview of Sample Number of Services to Organisation Size

Characteristic	*<50* *N = 3[1]*	*50-249* *N = 5[1]*	*250-1000* *N = 5[1]*	*>1000* *N = 18[1]*
Number of Digital Services				
0-5	1 (33%)	0 (0%)	0 (0%)	1 (5.6%)
6-10	0 (0%)	0 (0%)	0 (0%)	0 (0%)
11-20	2 (67%)	2 (40%)	0 (0%)	0 (0%)
20-50	0 (0%)	3 (60%)	0 (0%)	5 (28%)
50-100	0 (0%)	0 (0%)	3 (60%)	3 (17%)
>100	0 (0%)	0 (0%)	2 (40%)	9 (50%)

[1]n = 31

Smaller organisations with fewer than 50 employees were primarily characterised by consuming between 11 and 20 digital services (67%), with one organisation reporting between 0-5. Among organisations holding 50-249 employees, the majority consumed between 20-50 (60%0, while the remaining organisations within this size reported consuming between 11-20 digital services (40%). Organisations with a size of 250-1000 employees and above reported higher levels of digital service consumption overall. Within the 250-1000 category, 60% reported consuming between 50-100 digital services, while 40% reported consuming more than 100 digital services. As for the largest organisation size by employees (>1000), respondents reported the highest levels of digital service consumption. Half of these organisations more than 100, while 28% consumed between 20 and 50 digital services. Furthermore, 17% of this group reported 50-100 digital services, and only one organisation reported consuming between 0-5 digital services (5.6%).

Out of the sample size, only four (12.9%, out of n = 31) organisations reported having experienced a significant security incident within the last 12 months. This includes two hospitals, one care providing organisation and “other” organisation that reported to be an organisation operating within public safety. The latter is the only private organisation.

The distribution of commonly experienced technical causes of incidents in digital supply chain(s) vary across private and public organisations (see Figure 3).

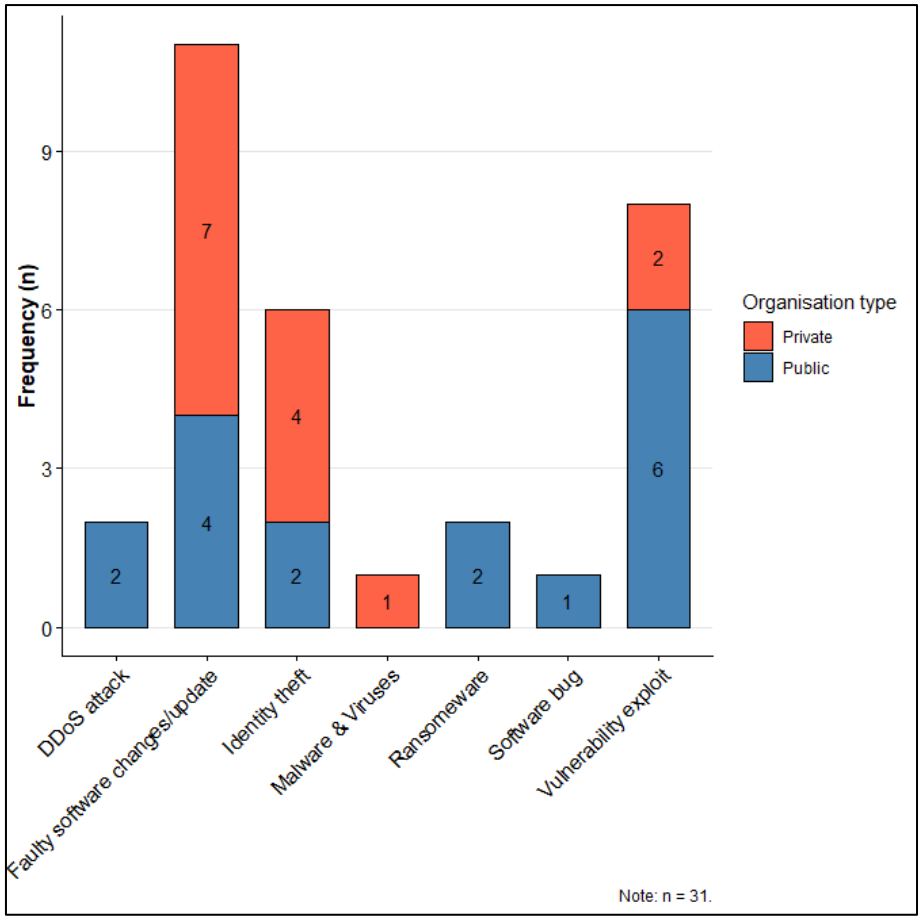

Figure 3: Reported commonly experienced technical causes of incidents in digital supply chain(s)

In private organisations, the most frequently reported technical cause was faulty software or updates (50%), followed by identity theft (29%). Vulnerability exploits were reported by two respondents, while malware and viruses count one. No private sector organisation respondents reported DDoS attacks or ransomware, or software bugs, as commonly experienced cause of security incidents in digital supply chain(s). In public organisations, vulnerability exploits were the most frequently reported technical cause (6), followed by faulty software changes or updates (24%). Both DDoS attacks and ransomware were reported by two respondents in the public sector group. Software bug was reported once, while malware and viruses were not reported. In their reporting dashboard from 2020-2024, ENISA (2023b) reports that, besides the "other" category, DDoS Attacks and Malware & viruses are most prevalent technical causes of incidents in the defined digital supply chain categories. The results from the respondents in the sample size indicate a mirrored experienced technical cause of incidents in their respective digital supply chain.

The nature of security incidents experienced in digital supply chain(s) shows some similarities and variation between public and private organisations (see Figure 4). In both private and public organisations, human error was the dominant perceived nature of security incidents. Public organisations perceive more malicious action(s) as the nature, including one reporting natural phenomena(s), compared to private organisations.

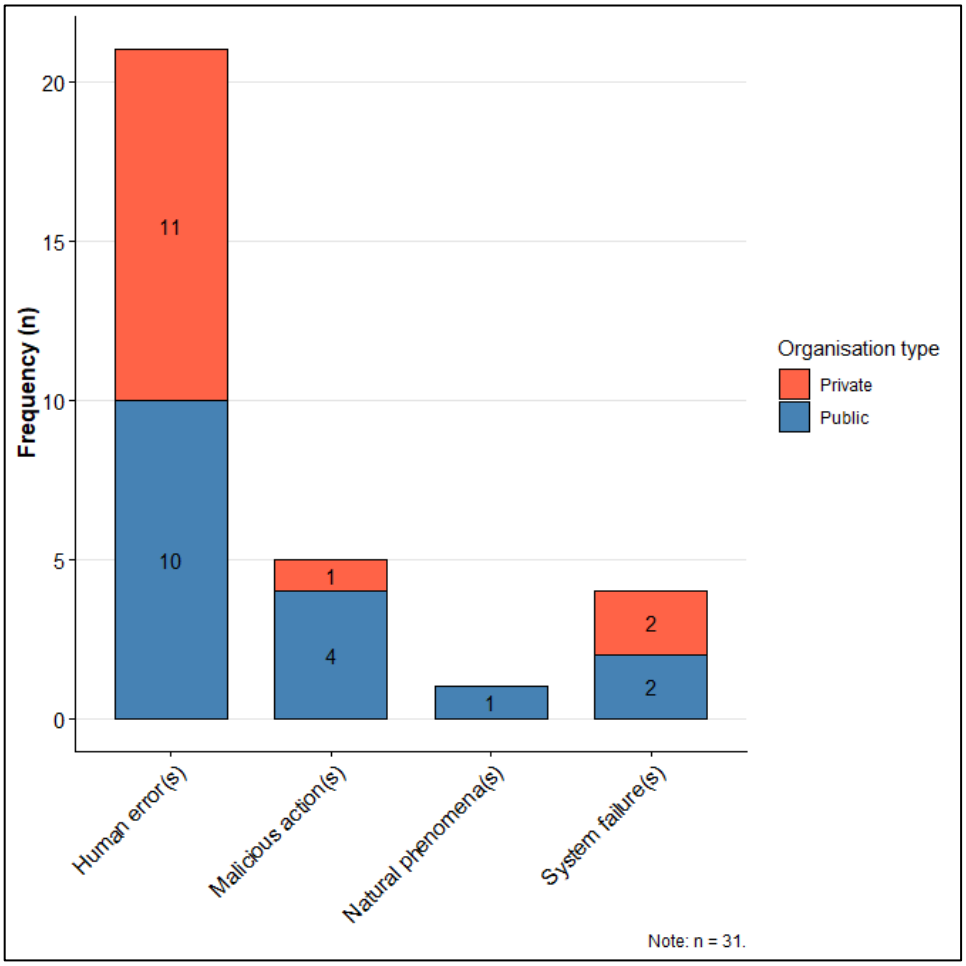

Figure 4: Reported commonly experienced nature of incidents in digital supply chain(s)

Nevertheless, the difference in group size for public and private sector organisations influence the frequency of reported technical cause and nature of security incidents in digital supply chain(s). Similarly, here, the data from ENISA (2023b) from 2020-2024 report that system failures (49%) and malicious actions (40%) are amongst the two highest natures of incidents at the defined digital supply chains, instead of human error(s). Likewise, however, natural phenomena(s) remain low.

The participants of the survey also reported the types of digital services their organisations used (see figure 5).

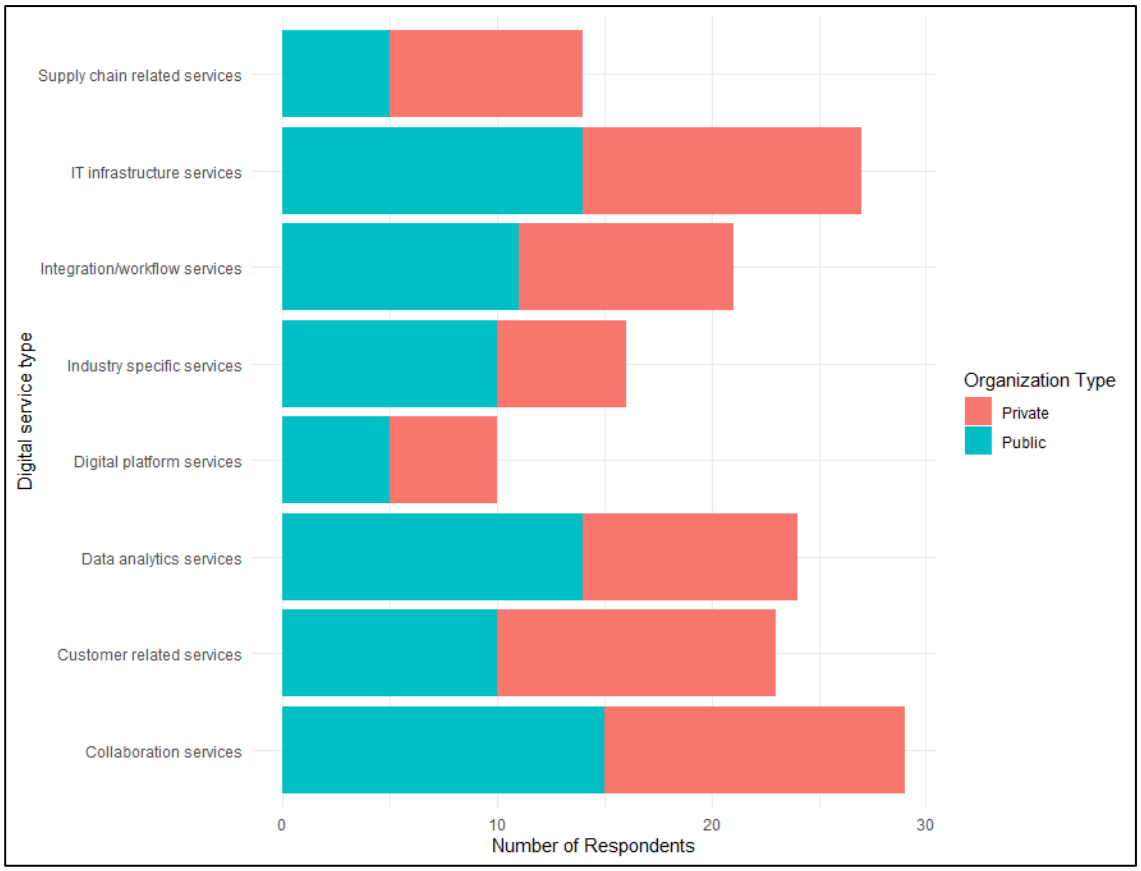

Figure 5: Kinds of Digital Services used by Private and Public Organisations

From the various available digital service types that the respondents could have chosen, only the supply chain related services show a more pronounced distinction between public and private organisations. Collaboration and IT infrastructure services seem to be the most prominent digital service variant reported in the sample. On the opposite side, supply chain related and digital platform services have been reported the lowest.

4.2 Reliability and Validity Analysis

Cronbach's alpha was used to evaluate the internal consistency of the defined items for each of the constructs. Cronbach's alpha determines whether multiple designed questions measure the same concept to produce consistent and reliable results.

Table 7: Cronbach's alpha

Variable	*If dropped*	*Cronbach's alpha*
Cyber Threat Intelligence Capability (CTIC)		0.89
CTIC1	0.88	
CTIC2	0.87	
CTIC3	0.86	
CTIC4	0.85	
CTIC5	0.90	
CTIC6	0.88	
Inter-organisational Cyber Threat Information Sharing (ICTIS)		0.95
ICTIS1	0.95	
ICTIS2	0.94	
ICTIS3	0.94	
ICTIS4	0.93	
ICTIS5	0.94	
ICTIS6	0.95	
Information Quality Trust (IQT)		0.89
IQT1	0.84	
IQT2	0.86	
IQT3	0.88	
IQT4	0.84	
IQT5	0.89	
Digital Supply Chain Cyber Threat Awareness (DSCCTA)		0.88
DSCCTA1	0.87	
DSCCTA2	0.84	
DSCCTA3	0.88	
DSCCTA4	0.87	
DSCCTA5	0.84	
DSCCTA6	0.85	

n = 31

As table 7 shows, all Likert-scales items for the defined constructs demonstrated good ($\alpha > 0.80$) or above internal consistency. The CTIC scale showed good reliability ($\alpha = .89$, 95% CI [.082, .94]), as did the DSCCTA scale ($\alpha = .88$, 95% CI [.80, .93]) and the IQT scale ($\alpha = .89$, 95% CI [.81, .94]). The ICTIS scale indicates the strongest internal consistency using the Cronbach Alpha's test ($\alpha = .95$, 95% CI [.92, .97]). Corrected item-total correlations were acceptable to strong across all measures.

The survey respondents were analysed for straight-lining using 'longstring'. One respondent reported the highest level of straight lining, however the removal of it did not substantially impact the results of the Cronbach's Alpha tests. Considering the low sample size, it was decided to include this respondent. All the construct items were collected and parsed into averages, creating average scale variables for each of the four variables, each logically named …-Average.

Table 8 shows the descriptive statistics of these variables, indicating the mean, median, standard deviation, skewness and kurtosis; used to assess assumptions about the data's normality considering the Central Limit Theorem.

Table 8: Descriptive Statistics full Dataset

Measure	*n*	*Mean*	*Median*	*Std. deviation*	*Skewness*	*Kurtosis*
CTICAverage	31	4.88	5	1.15	-0.31	-0.9
ICTISAverage	31	4.42	4.5	1.7	-0.33	-1.24
IQTAverage	31	5.13	5.4	0.9	-1.18	0.87
DSCCTAAverage	31	5.5	5.67	0.83	-1.08	1.3

The average scale of CTIC showed a mean of 4.88 (SD = 1.15) and a median of 5.00. A mild tendency towards higher scores is indicated by a slightly negative skewness (-0.31), while the negative kurtosis (-0.90) indicates a flatter distribution compared to normality. IQT reported the highest mean of 5.13 (SD = 0.90) and a median of 5.40. The distribution was moderately negatively skewed (-1.18), with a slightly stronger Kurtosis distribution (0.87) that indicates a concentration above the mean. DSCCTA showed the highest mean score at 5.50 (SD = 0.83) and a median of 5.67. Its distribution was also negatively skewed (-1.08) and moderately concentrated (1.30), also suggesting a concentration around the mean. ICTIS had a mean of 4.42 (SD = 1.70) and a median of 4.50. It showed the highest variability among the variables. Its distribution is slightly negatively skewed (-0.33), and its kurtosis (-1.24) indicate a flatter distribution.

Inspecting the histogram of variable ICTISAverage uncovers that it has a bimodal distribution due to it having two peaks (see figure 6).

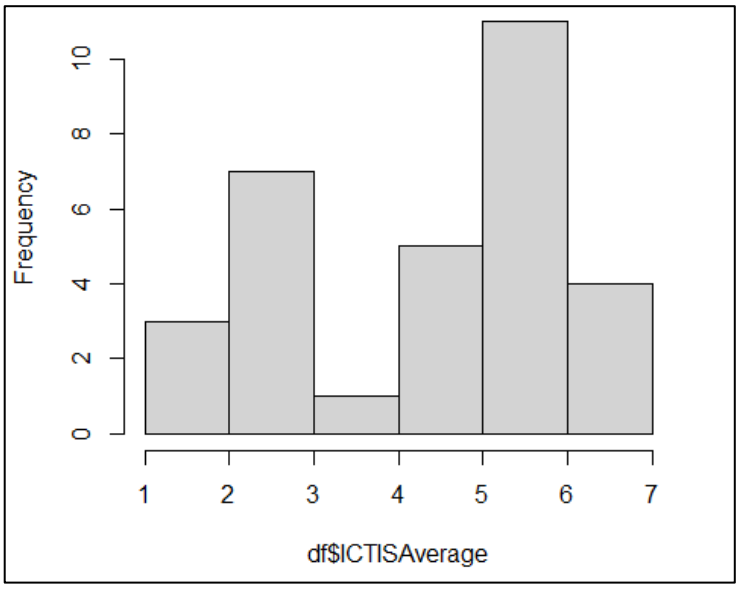

Figure 6: Inter-organisational Cyber Threat Information Sharing has a bimodal distribution

The histogram indicates that the sample contains two different groups that report different levels of inter-organisational cyber threat information sharing. Nevertheless, none of the variables follow a strict normal distribution, and considering the small sample size non-parametric methods were deduced to be more appropriate and thus selected.

4.3 Hypotheses Testing: Spearman Correlation Analysis

All three hypotheses in the conceptual model were tested using one-sided Spearman correlation tests. Before that however, the monotonicity was inspected between the study variable combinations of interest.

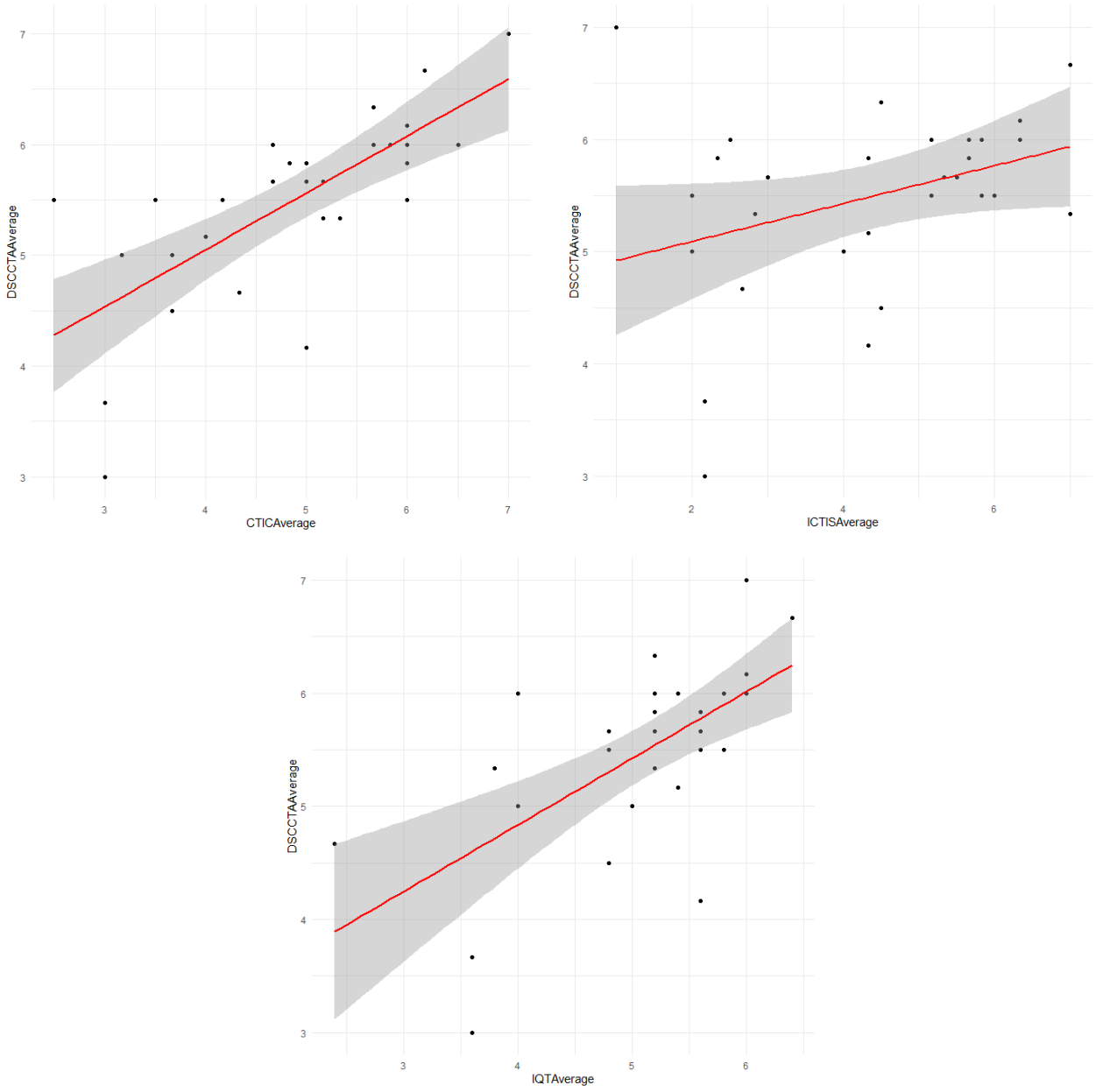

Figure 7: Monotonicity Visualised in Scatterplots

The first scatterplot in Figure 7 shows a relatively clear monotonic association between CTIC and DSCCTA averages. It appears that as CTIC increases, DSCCTA generally increases as well, and this pattern is relatively constant across the range of values. Second to it, the scatterplot shows a weaker and more dispersed monotonic association between ICTIS and DSSCTA. While there seems to be a general upwards trend in the fitted line, the spread of observations is much wider resulting in a line

that's less steep; considerably noise and variability. As for the third scatterplot, a more upwards trend seems to be present for IQT and DSCCTA. Similar to the first scatterplot, here it seems that as IQT increases, DSCCTA generally increases as well. However, there appears to be a concentration around the upper ends of the trend-line and more variability. Given the weaker monotonic characteristics of the plots, including the appearance of noise and variability, a spearman correlation test was selected.

A Spearman's correlation test was thus used to test the hypotheses (see Table 9), which include speculated positive associations between CTIC, ICTIS, IQT and DSCCTA.

Table 9: Spearman Correlation Matrix

			Spearman		
			rho	*CI*	*p*
CTICAverage	-	DSCCTAAverage	0.73	[.51, .86]	<.001
ICTISAverage	-	DSCCTAAverage	0.39	[.05, .66]	.028
IQTAverage	-	DSCCTAAverage	0.65	[.38, .81]	<.001

df = 29

First, the analysis indicates a strong positive association between CTIC and DSSCTA (r_s = .73, p <.001, 95 % CI [.51, .86]), which indicates that organisations reporting higher cyber threat intelligence capability also tend to report higher levels of digital supply chain cyber threat awareness. The strength and significance of the association provide support for the proposed association between CTIC and DSSCTA. Since the p-value is below .05 and the association is in the hypothesised positive direction, the null hypothesis is rejected and H_1 is supported.

Second from this sample data, ICTIS demonstrates a moderate positive association with DSCCTA (r_s = .39, p = .028, 95% CI [.05, .66]), the direction and significance of the association suggest a potential associating between reported inter-organisational cyber threat information sharing and cyber threat awareness of the consumed digital supply chains. Based on the p-value being below .05 and the effect being in the predicted direction, the null hypothesis is rejected and H_2 is supported. Nevertheless, including the visual screening of the scatterplot, the association is weaker compared to H_1 and H_3.

Lastly, as the latter suggests, IQT also showed a strong positive association with DSSCTA (r_s = .64, p < .001, 95% CI [.38, .81]). This suggests that similarly to CTIC that higher levels of trust in information quality regarding externally exchanges cyber threat intelligence are associated with higher levels of digital supply chain cyber threat awareness. This result is significant and in the hypothesised direction, therefore the null hypothesis is rejected and the H_3 is supported.

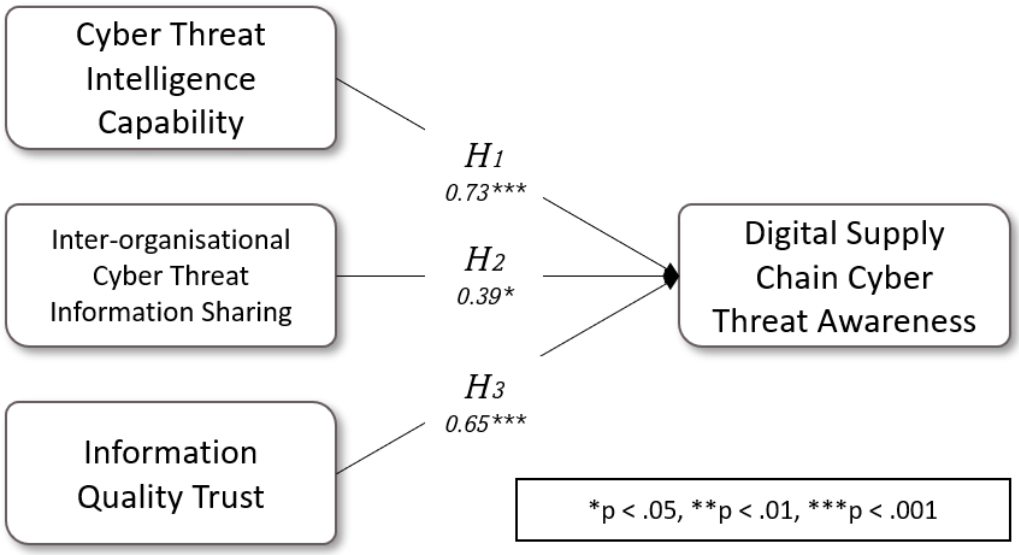

Figure 8: Results One-Sided Spearman Correlation Tests

As figure 8 illustrates, all three positive associations hypotheses have met the required significant level threshold (p <.05).

4.4 Exploratory Analysis: Organisation Type and Role

Table 10 shows the descriptive statistics of the variables separating the dataset by public and private organisations, indicating the mean, median, standard deviation, skewness and kurtosis; used to assess assumptions about the data's normality considering the Central Limit Theorem.

Table 10: Descriptive Statistics Public and Private

Public	*N*	*Mean*	*Median*	*Std. deviation*	*Skewness*	*Kurtosis*
CTICAverage	17	4.8	4.67	0.96	-0.2	-1.32
ICTISAverage	17	4.93	5.67	1.54	-0.65	-1.12
IQTAverage	17	5.16	5.4	0.96	-1.49	1.51
DSCCTAAverage	17	5.61	5.67	0.44	-0.57	-0.98
Private	*N*	*Mean*	*Median*	*Std. deviation*	*Skewness*	*Kurtosis*
CTICAverage	14	4.96	5.08	1.42	-0.4	-1.29
ICTISAverage	14	3.8	4.33	1.72	0.07	-1.24
IQTAverage	14	5.09	5.2	0.85	-0.5	-0.94
DSCCTAAverage	14	5.37	5.67	1.15	-0.6	-0.78

Both groups report broadly similar central tendencies CTIC. Public organisations show a mean of 4.80 (SD = 0.96) and a median of 4.67, while private organisations report a slightly higher mean of 4.96 (SD = 1.42) and a median of 5.08, indicating broadly comparable perceived capability across sectors.

For ICTIS, a clearer difference is observed. Public organisations report a higher mean of 4.93 (SD = 1.54) compared to 3.80 (SD = 1.72) in private organisations, with medians of 5.67 and 4.33 respectively, indicating lower reported sharing levels in the private sector. IQT is similarly high in both groups, with means of 5.16 (SD = 0.96) for public organisations and 5.09 (SD = 0.85) for private organisations, and closely aligned medians (5.4 and 5.2), suggesting comparable levels across sectors.

As for DSCCTA, both groups report high levels, with a slightly higher mean in the public sector (5.61, SD = 0.44) compared to the private sector (5.37, SD = 1.15). Median values are identical at 5.67. Inspecting the histograms of each variable in the respective separate datasets uncovers various bimodal distributions. Considering all, these reported values do not follow normal distribution assumptions.

In order to assess the assumption of homogeneity of covariance matrices, Box's M test was conducted for the variables across public and private organisation types. The results indicated a statistically significant violation of this assumption $\chi^2(10) = 26.29$, $p = .003$. As such, to explore whether organisational type (public vs private sector) was associated with differences across the study variables, a one-way multivariate analysis of variance was conducted using Pillai's Trace because the data violates assumptions like homogeneity of variances and has unequal sample sizes (see table 11).

Table 11: MANOVA and ANOVA on difference Public and Private

Effect (MANOVA)	*Pillai's V*	*f*	*df1*	*df2*	*p*
Type	0.260	2.28	4	26	.088

ANOVA	*F*	*df1*	*df2*	*p*
CTICAverage	0.15	1	29	.706
ICTISAverage	3.74	1	29	.063
IQTAverage	0.06	1	29	.813
DSCCTAAverage	0.63	1	29	.435

The MANOVA revealed no statistically significant multivariate effect of organisational type of the combined variables, Pillai's Trace = .260, $F(4, 26) = 2.28$, $p = .088$. Although the result did not reach the significance threshold of $p < .05$, it indicated a weak multivariate trend.

Follow-up univariate ANOVAs were conducted to examine the individual variables in relation to the organisational type. The analysis indicated no statistically significant differences between public and private organisations for CTIC, $F(1, 29) = 0.15$, $p = .706$, IQT, $F(1, 29) = 0.06$, $p = .813$, or DSCCTA, $F(1, 29) = 0.63$, $p = .435$. However, ICTIS demonstrated a marginal effect of organizational type, $F(1, 29) = 3.74$, $p = .063$.

As reported earlier, descriptive statistics indicate differences between public and private organisations across the variables, where the largest differences were reported on inter-organisational cyber threat information sharing. Visual inspection of the boxplots (see figure 9) further supports this trend, as the distributions for public and private organisations appeared separate for ICTISAverage. Although some overlap between groups remained, the plots suggested a distinction for ICTISAverage that for the other variables.

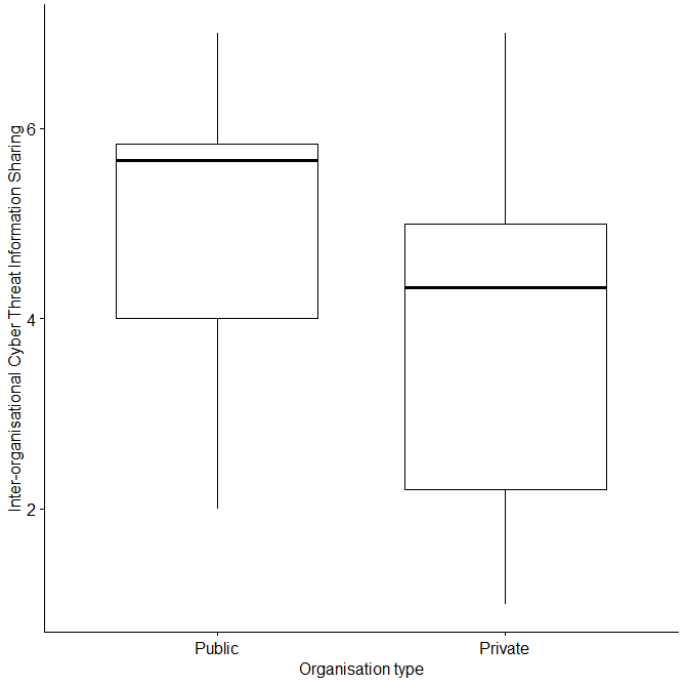

Figure 9: Boxplot Organisation Type on Inter-organisational Cyber Threat Information Sharing

To further examine differences between ICTIS between public and private organisations, a non-parametric Wilcoxon rank-sum test was conducted considering the violations of assumptions. The results indicate a statistically significant difference in ICTISAverage between the two groups ($W = 67$, $p = 0.038$). Due to the significance of this result, the null hypothesis is rejected and H_{4b} is supported when not considering the other study variables. This suggests that the distribution of ICTIS scores differs between public and private organisations, where inter-organisation information sharing of cyber threat information is reported higher for public organisations. This finding is consistent with the earlier descriptive statistics and univariate analyses, which indicated higher ICTISAverage scores in public organizations compared to private organizations.

As for H_{4a}, the null hypothesis is supported by the results of the MANOVA and follow-up test. The same is true for H_5, lacking a significant result from the MANOVA and follow-up test, supporting the null hypothesis.

During the exploratory analysis phase, the difference between reported data from management and non-management respondents was also examined. The table below shows the descriptive statistics between the two groups.

Table 12: Descriptive Statistics Management and Non-management

Management	*N*	*Mean*	*Median*	*Std. deviation*	*Skewness*	*Kurtosis*
CTICAverage	19	5.05	5	1.04	-0.48	0.05
ICTISAverage	19	4.31	4.5	1.72	-0.3	-1.3
IQTAverage	19	5.35	5.6	0.83	-2.21	5.72
DSCCTAAverage	19	5.81	5.83	0.52	0.22	0.19
Non-management	*N*	*Mean*	*Median*	*Std. deviation*	*Skewness*	*Kurtosis*
CTICAverage	12	4.6	4.58	1.29	0.04	-1.79
ICTISAverage	12	4.6	4.83	1.73	-0.35	-1.44
IQTAverage	12	4.78	4.9	0.94	-0.05	-1.86
DSCCTAAverage	12	5.01	5.17	1	-0.61	-1.01

CTIC in the management respondents (n = 19) reported a mean of 5.05 (SD = 1.04) and a median of 5.00. In the non-management respondents (n = 12), CTIC was reported with a mean of 4.60 (SD = 1.29) and a median of 4.58. For Inter-organisational ICTIS, management respondents reported a mean of 4.31 (SD = 1.72) and a median of 4.50, while non-management respondents reported a mean of 4.60 (SD = 1.73) and a median of 4.83.

As for IQT, management respondents reported a mean of 5.35 (SD = 0.83) and a median of 5.60, while non-management respondents reported a mean of 4.78 (SD = 0.94) and a median of 4.90.

Finally, for DSCCTA, management respondents reported a mean of 5.81 (SD = 0.52) and a median of 5.83, while non-management respondents reported a mean of 5.01 (SD = 1.00) and a median of 5.17. Following a boxplot comparison of ICTISAverage, the management group contains an outlier that pushes the mean towards the lower side of the scale. These characteristics, in combination with some bimodal distributions, violate the normal distribution assumptions.

Box's M test again was conducted for the dependent variables across role levels, The result was not statistically significant, $\chi^2(10) = 15.98$, $p = .100$, indicating that the covariance matrices did not significantly differ between groups. This suggests that the assumption of homogeneity of covariance matrices was reasonably met for the MANOVA. Nevertheless, Pallai's test was again used for the test for stability reasons, despite the assumption of homogeneity of covariances being met. The sample size and violations of distribution assumptions require a more robust test (see table 13).

Table 13: MANOVA and ANOVA on difference Management and Non-management

Effect (MANOVA)	*Pillai's V*	*f*	*df1*	*df2*	*p*
Type	0.318	3.03	4	26	.036

ANOVA	*F*	*df1*	*df2*	*p*
CTICAverage	1.16	1	29	.289
ICTISAverage	0.21	1	29	.650
IQTAverage	3.09	1	29	.098
DSCCTAAverage	8.36	1	29	.007

The overall multivariate effect was statistically significant (Pillai's V = 0.318, F(4, 26) = 3.03, p = .036), indicating that management level is associated with differences within the study variables. Subsequent univariate analysis was conducted to examine each construct separately.

For CTIC, no statistically significant difference was observed between management and non-management respondents (F(1, 29) = 1.16, p = .289). Similarly, Inter-organisational ICTIS did not show a significant difference between groups (F(1, 29) = 0.21, p = .650). IQT showed a marginal difference between groups, although this did not reach statistical significance at the 5% level (F(1, 29) = 3.09, p = .098). In contrast, DSCCTA showed a statistically significant difference between management and non-management respondents (F(1, 29) = 8.36, p = .007).

Visual inspection of the boxplot (see figure 10) on the role level and reported Digital Supply Chain Cyber Threat Awareness also indicates a distinction between the two groups, despite some overlaps.

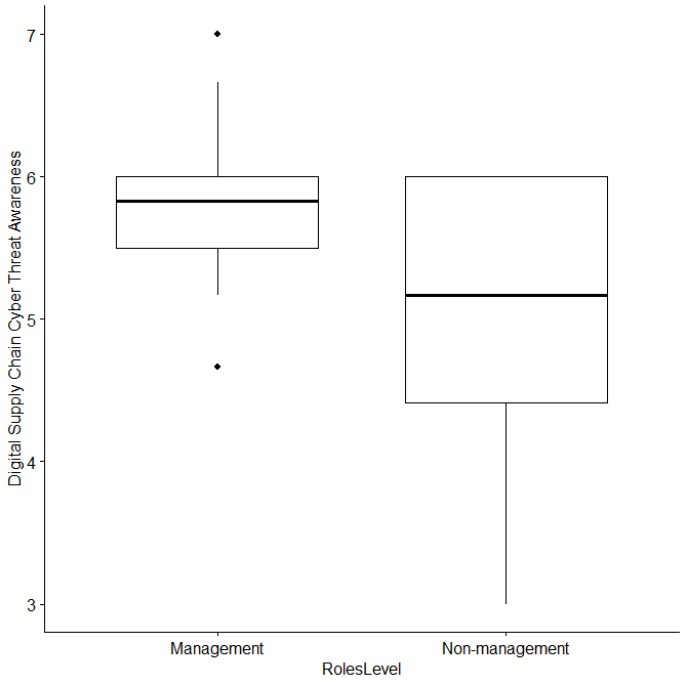

Figure 10: Boxplot Role Level on Digital Supply Chain Cyber Threat Awareness

To examine differences in DSCCTA between management and non-management respondents, a non-parametric Wilcoxon rank-sum test was conducted due to violations of normality assumptions. The results indicate a statistically significant difference in DSCCTA between the two groups ($W = 165$, $p = 0.0368$). This suggests that the distribution of DSCCTA scores differs between management and non-management respondents, with higher levels of cyber threat awareness observed among management-level participants compared to non-management respondents.

Other meaningful comparisons between high and lower levels number of digital services or organisation sizes were not possible due to size imbalances between the separated groups.

5 Conclusion

This study examined how inter-organisational cyber threat information sharing, information quality trust, and cyber threat intelligence capability are associated with digital supply chain cyber threat awareness among information security professionals in European public and private organisations. The research was positioned within the increasing dependency on cloud computing, software ecosystems, and interconnected digital supply chains, where organisations rely heavily on external digital services while simultaneously becoming more exposed to cyber threats propagating across organisational boundaries.

Synthesis of existing literature establishes that digital supply chains consist of intertwined cloud and software supply chains involving multiple actors, infrastructures, and dependencies (ENISA, 2023; Latsiou & Lambrinoudakis, 2026). However, empirical research specifically examining how organisations become aware of cyber threats to reduce the uncertainty of risks to security objectives within these digital supply chains remained limited. This study therefore applied Information Processing Theory (IPT) to examine whether organisations reduce uncertainty regarding digital supply chain cyber threats through cyber threat intelligence capability, external cyber threat information sharing, and trust in the quality of exchanged information. The findings indicate support for all three proposed hypotheses.

First, cyber threat intelligence capability demonstrated a strong positive association with digital supply chain cyber threat awareness. Organisations reporting stronger capabilities in gathering, processing, analysing, and utilising cyber threat intelligence also reported higher levels of awareness regarding threats within their digital supply chains. This finding aligns with prior research arguing that CTI enhances the interpretation of dynamic cyber threats and supports organisational awareness (McMillan, 2013; Chismon & Ruks, 2015; Naseer et al., 2021). Within the context of IPT, organisations with stronger CTI capability may be better able to process threat information and reduce uncertainty regarding digital supply chain risks.

Second, industry-peer inter-organisational cyber threat information sharing demonstrated a moderate positive association with digital supply chain cyber threat awareness. This suggests that organisations engaging more actively in external cyber threat information exchange also tend to report higher levels of awareness regarding threats affecting their digital supply chains. This result is consistent with literature suggesting that external information sharing expands insight beyond internal systems and supports broader situational awareness (Ring, 2014; Tounsi & Rais, 2018; Preuveneers & Joosen,

2023). However, compared to CTIC and IQT, the association was weaker and showed greater variability. This may indicate that simply participating in information exchange does not automatically result in improved awareness, but that additional organisational factors influence the effectiveness of shared information.

Third, information quality trust showed a strong positive association with digital supply chain cyber threat awareness. Organisations perceiving externally shared cyber threat information as accurate, timely, relevant, and trustworthy reported higher awareness levels. This finding strongly supports previous literature emphasising the importance of information quality for effective cyber threat intelligence utilisation (Dalziel, 2015; Ring, 2014). Within IPT, information can only reduce uncertainty if organisations perceive the information as sufficiently useful and reliable to support decision-making.

Together, the findings suggest that awareness regarding cyber threats in digital supply chains depends not solely on access to information, but also on the organisational capability to process threat intelligence and the perceived quality of externally shared information. In this regard, the results support the theoretical framework proposed within this study, where external information gathering, threat intelligence processing capability, and information quality collectively contribute to reducing uncertainty regarding cyber threats within digital supply chains by its proven associations.

Regarding the sub-research questions, the first sub-question (*RQ1*) asked how cyber threat intelligence capability, inter-organisational cyber threat information sharing, and information quality trust are associated with digital supply chain cyber threat awareness. The results provide support for all three hypotheses. H_1 was supported, indicating that cyber threat intelligence capability is positively associated with digital supply chain cyber threat awareness. H_2 was also supported, showing that inter-organisational cyber threat information sharing is positively associated with awareness, although the association was weaker compared to the other variables. Finally, H_3 was supported, demonstrating that information quality trust is positively associated with digital supply chain cyber threat awareness. Overall, CTIC and IQT demonstrated the strongest associations with awareness, while ICTIS showed a weaker but statistically significant positive association.

The second sub-question (*RQ2*) questioned whether public and private organisations differ in cyber threat information sharing and information quality trust. The findings provide only partial evidence for differences between the two organisational groups. H_{4a} was supported, as public organisations reported significantly higher levels of inter-organisational cyber threat information sharing than private organisations. This finding is consistent with literature suggesting that private organisations

may experience greater barriers to information sharing due to concerns relating to confidentiality, competition, liability, and reputation (Peretti, 2014; Skopik et al., 2016). In contrast, H_{4b} was not supported, as no significant differences were observed between public and private organisations regarding information quality trust. Similarly, no meaningful differences were found regarding cyber threat intelligence capability. Overall, the findings suggest that organisational type appears to influence information sharing behaviour more strongly than it influences trust in information quality or internal threat intelligence capability.

The third sub-question (*RQ3*) examined whether public and private organisations differ in their level of digital supply chain cyber threat awareness. H_5 was not supported, as no statistically significant differences in digital supply chain cyber threat awareness were observed between public and private organisations. Although public organisations reported slightly higher average awareness scores, the difference was insufficient to conclude that organisational type meaningfully influences awareness levels within this sample.

From a theoretical perspective, this study provides preliminary empirical support for the application of Information Processing Theory within the context of digital supply chain security, specifically focussing on digital supply chain cyber threat awareness. While IPT has previously stems from organisational decision making and uncertainty, its application in the context of cyber threat intelligence relating to digital supply chains remains limited. However, given the exploratory nature and limited sample size of this study, these observations should be interpreted as preliminary rather than conclusive.

In all to answer the main research question, the findings suggests that cyber threat intelligence capability, inter-organisational cyber threat information sharing, and information quality trust are positively associated with digital supply chain cyber threat awareness among information security professionals in European public and private organisations. While information sharing contributes to awareness, the findings indicate that the capability to process cyber threat intelligence and the perceived quality of exchanged information may play a particularly important role in reducing uncertainty regarding cyber threats within increasingly interconnected digital supply chains.

6 Discussion

The findings of this preliminary study provide several theoretical, practical, and methodological insights regarding cyber threat awareness within digital supply chains. The results generally align with prior literature surrounding cyber threat intelligence, information processing theory, and inter-organisational information sharing, while also highlighting several complexities regarding the practical implementation and effectiveness of cyber threat information exchange between organisations.

The strongest association observed within this study was between cyber threat intelligence capability and digital supply chain cyber threat awareness. This finding supports prior literature arguing that organisations require not only information itself, but also sufficient capability to analyse, contextualise, and operationalise cyber threat intelligence to effectively reduce uncertainty (Chismon & Ruks, 2015; Naseer et al., 2021). Within digitally interconnected supply chains, organisations face increasing complexity due to outsourced infrastructures, cloud services, software dependencies, and limited visibility into external systems. The findings therefore reinforce the relevance of Information Processing Theory within cybersecurity contexts, where stronger information processing capability appears associated with higher levels of awareness regarding threats propagating across digital supply chains. Insights obtained during the expert consultation further support this interpretation. The experts of the consultation session indicated that cyber threat intelligence capability can extend beyond the collection and sharing of threat information alone. Modern cyber threat intelligence tools increasingly include predictive capabilities, leveraging indicators of compromise, behavioural patterns and Artificial intelligence techniques to anticipate attack paths. Possibly, organisations with stronger cyber threat intelligence capabilities may not only process available information more effectively, but may also be better positioned to identify emerging digital supply chain risks proactively. Such capabilities may aid to create awareness independently from inter-organisational information sharing, which could explain why cyber threat intelligence capability was most strongly associated.

The positive association between inter-organisational cyber threat information sharing and digital supply chain cyber threat awareness also supports previous literature suggesting that external collaboration expands organisational situational awareness (Ring, 2014; Tounsi & Rais, 2018). However, the weaker association and increased variability surrounding ICTIS suggest that the effectiveness of information sharing may differ considerably between organisations. This seems consistent with previous studies arguing that information sharing effectiveness depends on contextual factors such as reciprocity, relevance, legal certainty, and trust (Skopik et al., 2016; Zibak et al.,

2022). In practice, organisations may participate in information sharing initiatives while still struggling to operationalise or trust the received information. The expert consultation provides additional context for this finding. Both experts indicated that the value of externally shared cyber threat information is strongly dependent on its timeliness. In practice, threat intelligence distributed through formal sectoral or governmental channels may arrive days after vulnerabilities or attacks become publicly known. Experts from the consultation session referred to incidents such as Log4Shell, where commercial intelligence providers and specialised communities often provided mitigation guidance before official information-sharing channels distributed actionable information. This may help explain why information sharing demonstrated a weaker association with awareness than CTIC and IQT. Access to information alone may be insufficient when organisations require near real-time awareness of rapidly evolving digital supply chain threats.

Additionally, the experts suggested that inter-organisational information sharing may be valuable at strategic and tactical levels rather than operational awareness levels. While organisations can often obtain technical indicators and vulnerability information through commercial providers or internal intelligence capabilities, collaboration with industry peers may be more useful for discussing the implications of threats, supplier risks, governance approaches, and broader digital supply chain risk management strategies. This distinction may partially explain the variability observed within ICTIS scores across respondents.

The findings regarding information quality trust further support this interpretation. Trust in the quality of exchanged information demonstrated a strong association with awareness of threats in digital supply chains, suggesting that organisations are more likely to benefit from external threat intelligence when the information is perceived as timely, accurate, actionable, and relevant. This closely aligns with Dalziel's (2015) conceptualisation of valuable threat intelligence and supports the notion that information quality remains essential for reducing uncertainty and supporting organisational decision-making. The importance of information quality also emerged during the expert consultation. The experts repeatedly emphasised that threat information must not only be accurate, but also timely and actionable. Information that arrives too late may have limited practical value regardless of its technical correctness. This observation aligns with Dalziel's (2015) argument that valuable cyber threat intelligence requires relevance, context, and actionability. The strong association between IQT and DSCCTA therefore suggests that organisations may become more aware of digital supply chain threats when they perceive shared intelligence as useful for informing decisions and mitigation efforts.

The exploratory findings regarding differences between public and private organisations are also noteworthy. Although no statistically significant differences were found overall in the multivariate analysis, public organisations reported higher levels of inter-organisational cyber threat information sharing compared to private organisations. This finding appears in-line with prior literature arguing that private organisations may face stronger concerns regarding confidentiality, competition, legal liability, or reputational damage when sharing cyber threat information (Peretti, 2014; Tounsi & Rais, 2018). Public organisations may operate within environments where collaboration and information exchange are more institutionalised or expected due to governmental coordination structures and regulatory obligations. This interpretation was also reflected during the expert consultation. The experts noted that public-sector organisations, particularly within healthcare, are often encouraged or required to participate in sector-specific knowledge centres and information-sharing communities. In contrast, participation among private organisations appears more variable. Larger organisations, such as banks and insurance providers, often participate in established industry networks, while smaller organisations may rely more heavily on commercial intelligence providers or informal professional relationships. These differences may contribute to the higher levels of reported information sharing observed among public organisations within this study.

Interestingly, despite lower reported sharing levels among private organisations, both sectors reported relatively similar levels of cyber threat awareness, information quality trust, and CTI capability. This may indicate that organisations utilise different mechanisms to achieve awareness. Private organisations may rely more heavily on internal intelligence capability or commercial threat intelligence providers, while public organisations may benefit more directly from collaborative information exchange structures. The consultation findings strongly support this interpretation. The experts indicated that organisations can obtain digital supply chain threat information through multiple channels, including commercial threat intelligence services, specialised cybersecurity vendors, industry communities, and internal intelligence capabilities. Consequently, awareness may not depend exclusively on participation in formal information-sharing arrangements. This may explain why public organisations reported significantly higher sharing levels while reporting similar levels of cyber threat awareness compared to private organisations.

Furthermore, the analysis comparing management and non-management respondents revealed that management respondents reported significantly higher levels of digital supply chain cyber threat awareness. This may imply that management related work, such as strategic visibility, governance, supplier relationships, grant greater insights in threats. Management-level respondents are likely more involved in organisational risk management and decision-making processes, which could increase their awareness regarding supply chain cyber threats.

6.1 Management Implications

The findings of this study carry several practical implications for organisations operating within digital supply chains. First, the strong association between cyber threat intelligence capability and digital supply chain cyber threat awareness suggests that organisations should invest in developing mature cyber threat intelligence processes and analytical capabilities. This includes improving the ability to collect, process, contextualise, and operationalise threat intelligence from both internal and external sources. This has also been confirmed by the experts during the consultation session.

Second, the findings suggest that participation in cyber threat information sharing initiatives alone may not automatically improve awareness. Organisations should therefore focus on improving the quality, contextualisation, and usability of exchanged threat intelligence. Threat intelligence sharing communities, sectoral platforms, and collaborative initiatives may benefit from implementing clearer standards regarding relevance, timeliness, and validation of shared information.

Third, the lower sharing levels observed among private organisations suggest that barriers to inter-organisational cyber threat information sharing remain present. Policymakers, governmental institutions, and sector-specific coordination bodies may therefore consider further mechanisms – other than the NIS2-directive - to reduce legal uncertainty, confidentiality concerns, and reputational risks surrounding cyber threat information sharing. Trusted sharing environments, anonymisation mechanisms, and sector-specific information sharing frameworks may support greater participation among private organisations.

Fourth, the findings indicate that management-level personnel report higher awareness regarding digital supply chain cyber threats. Therefore, organisations may benefit from communicating awareness between management and operational personnel to ensure that awareness regarding external dependencies and supply chain risks becomes more evenly distributed throughout the organisation.

Lastly, organisations may benefit from researching whether inter-organisations cyber threat information sharing may benefit from generating strategical objectives and missions, as was perceived by the experts; whilst maintaining a communication protocol if competitive or other tensions are high.

6.2 Limitations

Several limitations should be acknowledged when interpreting the findings of this study. First, the relatively small sample size limits the statistical power and generalisability of the findings. Although statistically significant associations were identified, the sample restricts the ability to conduct more advanced statistical modelling, moderation analyses, or robust subgroup comparisons. The limited sample size also increases sensitivity to outliers and variability within the data. Furthermore, the researcher could not consider other selected variables due to unbalances due to the low sample size.

Second, the study relied on self-reported survey responses, which introduces the possibility of response bias, subjective interpretation differences, and social desirability effects. Respondents may overestimate organisational capabilities or awareness levels. Although anonymity and attention checks were implemented to reduce bias, common method bias cannot be fully excluded.

Third, the cross-sectional design limits the interpretation of cause-and-effect, if not correlation. While positive associations were identified, the directionality of these association cannot be conclusively established. For example, organisations with higher awareness may also become more willing to participate in information sharing activities, rather than information sharing directly causing increased awareness. Longitudinal research designs would therefore be valuable for examining causal relationships over time.

Lastly, several statistical assumptions were violated throughout the analyses, including violations of normality, bimodal distributions, unequal group sizes, and homogeneity assumptions. Although robust and non-parametric statistical methods were selected accordingly, these characteristics still limit interpretability and robustness of the findings. Additionally, the scope of this study was limited to organisations operating in the Netherlands considering professionals in information security management roles. While this scope was intentionally selected due to the regulatory emphasis on cybersecurity collaboration and information sharing, the findings may not generalise to organisations outside regulated sectors or outside the European context. Non generalisability was also affected by the non-probability sampling methods used.

6.3 Recommendations for Future Research

Future research could further strengthen understanding regarding cyber threat awareness within digital supply chains in several ways. First, larger-scale quantitative studies involving broader samples across multiple sectors and countries would improve statistical robustness and enable more advanced multivariate analyses – including a larger sample size in general. Such studies may also allow researchers to better examine subgroup differences between sectors, organisation sizes, or organisational roles.

Second, future research could examine moderating and mediating relationships between variables. For example, future studies could examine whether information quality trust moderates or mediates the relationship between information sharing and awareness, or whether cyber threat intelligence capability moderates the effectiveness of externally shared threat intelligence.

Third, qualitative research methods such as interviews, focus groups, or case studies may provide deeper insight into organisational decision-making regarding cyber threat information sharing in the context of cyber threats in digital supply chains. Such approaches may uncover more precisely why organisations hesitate to share information, how trust develops between organisations, and how threat intelligence is operationalised in practice.

Fourth, future studies could further differentiate between types of information sharing relationships, such as formal versus informal sharing, public-private versus private-private collaboration, or automated versus human-driven intelligence exchange. Such distinctions may reveal which forms of collaboration contribute most strongly to cyber threat awareness.

Finally, future research could move beyond perceived awareness measures and examine objective cybersecurity outcomes, such as incident response performance, vulnerability management effectiveness, the effect of technologies that improve the trust factor between partners in supply chains and inter-organisationally, such as blockchain (Islam, 2023) or actual reductions in cyber incidents within digital supply chains. Moreover, future studies could replace the awareness construct with a cyber supply chain risk strategy construct and examine the effectiveness of inter-organisational cyber threat information sharing on this level. This may provide stronger insight into whether increased cyber threat awareness translates into measurable improvements in organisational cybersecurity against digital supply chain threats.

7 References

Abdelmagid, A. M., Farshid Javadnejad, Mcshane, M., Diaz, R., & Pinto, C. A. (2025). A New cyber risk identification and assessment approach of the maritime cyber risks. *Enterprise Information Systems*, *19*(10). https://doi.org/10.1080/17517575.2025.2524848

Ahrend, J. M., Jirotka, M., & Jones, K. (2016). On the collaborative practices of cyber threat intelligence analysts to develop and utilize tacit Threat and Defence Knowledge. *IEEE Xplore*, 1–10. https://doi.org/10.1109/CyberSA.2016.7503279

Akinrolabu, O., New, S., & Martin, A. (2018). Cyber Supply Chain Risks in Cloud Computing - Bridging the Risk Assessment Gap. *Open Journal of Cloud Computing (OJCC)*, *5*(1). https://www.ronpub.com/OJCC_2018v5i1n01_Akinrolabu.pdf

Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, *314*(5799), 610–613. https://doi.org/10.1126/science.1130992

Arora, A., Krishnan, R., Telang, R., & Yang, Y. (2010). An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure. *Information Systems Research*, *21*(1), 115–132. https://doi.org/10.1287/isre.1080.0226

Beamon, B. M. (1998). Supply chians design and analysis: Models and methods. *International Journal of Production Economics*, *55*(281-294), 1–14.

Blau, P. M. (1964). Exchange and Power in Social Life. *American Sociological Review*, *30*(5), 789. https://doi.org/10.2307/2091154

Bojanc, R., & Jerman-Blažič, B. (2013). A Quantitative Model for Information-Security Risk Management. *Engineering Management Journal*, *25*(2), 25–37. https://doi.org/10.1080/10429247.2013.11431972

Boyens, J. M. (2024). Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. *NIST Technical Series Publication*, *NIST Special Publication (SP) NIST SP 800*(-161r1-upd1). https://doi.org/10.6028/nist.sp.800-161r1-upd1

Boyens, J., Paulsen, C., Bartol, N., Winkler, K., & Gimbi, J. (2021). Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. *Information Technology Laboratory*, *NISTIR 8276*. https://doi.org/10.6028/nist.ir.8276

Chismon, D., & Ruks, M. (2015). Threat Intelligence: Collecting, Analysing, Evaluating. In *National Security Archive*. MWR Infosecurity. https://nsarchive.gwu.edu/document/17212-united-kingdom-government-threat-intelligence

Closs, D., Mcconnell Chair, J., & Mcgarrell, E. (2004). *Enhancing Security Throughout the Supply Chain*. https://www.businessofgovernment.org/sites/default/files/Enhancing%20Security.pdf

Dalziel, H. (2015). *How to Define and Build an Effective Cyber Threat Intelligence Capability*. Syngress.

Delvecchio, P., Galantucci, S., Iannacone, A., & Pirlo, G. (2025). CARIOCA: prioritizing the use of IoC by threats assessment shared on the MISP platform. *International Journal of Information Security*, *24*(2). https://doi.org/10.1007/s10207-025-01006-2

Durowoju, O. A., Chan, H. K., & Wang, X. (2011). The Impact of Security and Scalability of Cloud Service on Supply Chain Performance. *Journal of Electronic Commerce Research*, *12*(4), 243–256.

ENISA. (2021). ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS. In *ENISA*. European Union Agency for Cybersecurity. https://doi.org/10.2824/168593

ENISA. (2023a). *GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY JUNE 2023 GOOD PRACTICES FOR SUPPLY CHAIN CYBERSECURITY ABOUT ENISA AUTHORS*. https://doi.org/10.2824/805268

ENISA. (2023b). *Incident reporting*. CIRAS. https://ciras.enisa.europa.eu/ciras-consolidated-reporting

Ezhei, M., & Tork Ladani, B. (2017). Information sharing vs. privacy: A game theoretic analysis. *Expert Systems with Applications*, *88*(December 2017), 327–337. https://doi.org/10.1016/j.eswa.2017.06.042

Galbraith, J. R. (1974). Organization Design: An Information Processing View. *Interfaces*, *4*(3), 28–36. https://doi.org/10.1287/inte.4.3.28

Galbraith, J. R. (2014). Organizational Design Challenges Resulting From Big Data. *Journal of Organization Design*, *3*(1), 2. https://doi.org/10.7146/jod.8856

Hampton, C., Sutton, S. G., Arnold, V., & Khazanchi, D. (2020). CYBER SUPPLY CHAIN RISK MANAGEMENT: TOWARD AN UNDERSTANDING OF THE ANTECEDENTS TO DEMAND FOR ASSURANCE. *Journal of Information Systems*, *35*(2). https://doi.org/10.2308/isys-19-050

Hong, Y., Xu, M., & Furnell, S. (2023). Situational support and information security behavioural intention: a comparative study using conservation of resources theory. *Behaviour & Information Technology*, *43*(3), 1–17. https://doi.org/10.1080/0144929x.2023.2177825

Islam, M. D. (2023). A survey on the use of blockchains to achieve supply chain security. *Information Systems*, *117*(102232), 102232. https://doi.org/10.1016/j.is.2023.102232

Jede, A., & Teuteberg, F. (2015). Integrating cloud computing in supply chain processes. *Journal of Enterprise Information Management*, *28*(6), 872–904. https://doi.org/10.1108/jeim-08-2014-0085

Kampourakis, V., Kavallieratios, G., Gkioulos, V., & Katsikas, S. (2025). Cracks in the chain: A technical analysis of real-life supply chain security incidents. *Computers & Security*, *159*(104673), 104673. https://doi.org/10.1016/j.cose.2025.104673

Kushida, K. E., Murray, J., & Zysman, J. (2015). Cloud Computing: From Scarcity to Abundance. *Journal of Industry, Competition and Trade*, *15*(1), 5–19. https://doi.org/10.1007/s10842-014-0188-y

Latsiou, A., & Lambrinoudakis, C. (2026). Cyber Supply Chain Risk Management: From Threats to Treatment. *International Journal of Information Security*, *25*(1). https://doi.org/10.1007/s10207-025-01207-9

McMillan, R. (2013). *Definition: threat intelligence*.

Microsoft. (2025, May 5). *What is a datacenter? - Microsoft Datacenters*. Microsoft Datacenters. https://datacenters.microsoft.com/whatisadatacenter/

Naseer, H., Maynard, S. B., & Desouza, K. C. (2020). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*(April 2021), 113476. https://doi.org/10.1016/j.dss.2020.113476

Nishat Faisal, M., Banwet, D. K., & Shankar, R. (2007). Information risks management in supply chains: an assessment and mitigation framework. *Journal of Enterprise Information Management*, *20*(6), 677–699. https://doi.org/10.1108/17410390710830727

Peretti, K. (2014). Cyber Threat Intelligence: To Share or Not to Share - What Are the Real Concerns? In *Bloomberg Law*. Bloomberg BNA Privacy and Security Law Report. https://news.bloomberglaw.com/us-law-week/cyber-threat-intelligence-to-share-or-not-to-sharewhat-are-the-real-concerns

Ponemon, L. (2015, November 4). *The Second Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way : Ponemon Institute*. Ponemon Institute; Ponemon Institute. https://www.ponemon.org/news-updates/blog/security/the-second-annual-study-on-exchanging-cyber-threat-intelligence-there-has-to-be-a-better-way.html

Preuveneers, D., & Joosen, W. (2023). Privacy-preserving correlation of cross-organizational cyber threat intelligence with private graph intersections. *Computers & Security*, *135*(December 2023), 103505. https://doi.org/10.1016/j.cose.2023.103505

Qamar, S., Anwar, Z., Rahman, M. A., Al-Shaer, E., & Chu, B.-T. (2017). Data-driven analytics for cyber-threat intelligence and information sharing. *Computers & Security*, *67*(June 2017), 35–58. https://doi.org/10.1016/j.cose.2017.02.005

Ray, J. (2015, June 25). *Understanding the Threat Landscape: Indicators of Compromise (IOCs)*. https://circleid.com/posts/20150625_understanding_the_threat_landscape_indicators_of_compromise_iocs

Reichert, B. M., & Obelheiro, R. R. (2024). Software supply chain security: a systematic literature review. *International Journal of Computers and Applications*, *46*(10), 853–867. https://doi.org/10.1080/1206212x.2024.2390978

Ring, T. (2014). Threat intelligence: why people don't share. *Computer Fraud & Security*, *2014*(3), 5–9. https://doi.org/10.1016/s1361-3723(14)70469-5

Shakibazad, M., & Jabbar Rashidi, A. (2019). A New Method for Assets Sensitivity Calculation and Technical Risks Assessment in the Information Systems. *IET Information Security*, *14*(1). https://doi.org/10.1049/iet-ifs.2018.5390

Shu, C., Chen, W., Fan, G., Yu, H., Huang, Z., & Liang, Y. (2025). Tool or Toy: Are SCA tools ready for challenging scenarios? *Computers & Security*, *158*(104624), 104624. https://doi.org/10.1016/j.cose.2025.104624

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*(July 2016), 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Tang, O., & Musa, S. N. (2011). Identifying risk issues and research advancements in supply chain risk management. *International Journal of Production Economics*, *133*(1), 25–34. https://doi.org/10.1016/j.ijpe.2010.06.013

The MITRE Corporation. (2015). *General Information | MITRE ATT&CK®*. Attack.mitre.org. https://attack.mitre.org/resources/

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*(January 2018), 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Tushman, M. L., & Nadler, D. A. (1978). Information Processing as an Integrating Concept in Organizational Design. *Academy of Management Review*, *3*(3), 613–624. https://doi.org/10.5465/amr.1978.4305791

Wang, E. T. G., Tai, J. C. F., & Grover, V. (2013). Examining the Relational Benefits of Improved Interfirm Information Processing Capability in Buyer-Supplier Dyads. *MIS Quarterly*, *37*(1), 149–173. https://doi.org/10.25300/misq/2013/37.1.07

Wheeler, E. (2011). *Security risk management : building an information security risk management program from the ground up*. Syngress.

Yenugula, M., Sahoo, S. K., & Goswami, S. S. (2023). Cloud computing in supply chain management: Exploring the relationship. *Management Science Letters*, *13*(3), 193–210. https://doi.org/10.5267/j.msl.2023.4.003

Zack, M. H. (2007). The role of decision support systems in an indeterminate world. *Decision Support Systems*, *43*(4), 1664–1674. https://doi.org/10.1016/j.dss.2006.09.003

Zhan, L., Ming, J., Fu, J., Peng, G., Sha, L., & Lan, L. (2025). The hidden complexities of Android TPL detection: An empirical analysis of techniques, challenges, and effectiveness. *Computers & Security*, *159*(104672), 104672. https://doi.org/10.1016/j.cose.2025.104672

Zhang, H., Nakamura, T., & Sakurai, K. (2019, August 1). *Security and Trust Issues on Digital Supply Chain*. IEEE Xplore. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00069

Zheng, D., & Lewis, J. (2015). *Cyber Threat Information Sharing Recommendations for Congress and the Administration A Report of the CSIS Strategic Technologies Program*. CSIS

Strategic Technologies Program. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150310_cyberthreatinfosharing.pdf

Zibak, A., Sauerwein, C., & Simpson, A. (2021). A success model for cyber threat intelligence management platforms. *Computers & Security*, *111*(December 2021), 102466. https://doi.org/10.1016/j.cose.2021.102466

Appendices

Appendix A: Survey Measures of Constructs

Construct	Measures of Constructs (MoCs)
ICTIS | Inter-organisational Cyber Threat Information Sharing	• Our organisation participates in (sector-based) cybersecurity information sharing communities. • Our organisation exchanges cyber threat intelligence with industry peers. • Our organisations uses shared technical cyber threat intelligence received from industry peers. • Our organisation exchanges information about system vulnerabilities with industry peers. • Our organisation discusses Tactics, Techniques and Procedures (TTPs) with industry peers. • Our organisation exchanges information about (past) cyber incidents with industry peers.
CTIC | Cyber Threat Intelligence Capability	• Our organisation has the analytical capacity required to analyse cyber threat intelligence. • Our organisation produces cyber threat intelligence that is relevant. • Cyber Threat Intelligence is contextualised within our organisation. • Cyber Threat Intelligence is integrated into our SOC processes. • Our organisation is able to move from “unknown unknowns” to actionable threat landscape insight(s). • Cyber Threat Intelligence insights inform our risk assessment(s).
DSCCTA | Digital Supply Chain Cyber Threat Awareness	• We are aware of common cyber incident types that can affect our suppliers within our digital supply chain(s). • We are knowledgeable on how (D)DoS attacks within our digital supply chain(s) can threaten our information system(s). • We are aware of what kinds of software-/cloud-based system weaknesses within our digital supply chain(s) can threaten our information system(s) • We are knowledgeable on how malware attacks within our digital supply chain(s) can threaten our information system(s). • We are aware of Tactics, Techniques and Procedures (TTPs) used to commonly exploit systems within our digital supply chain(s). • We are aware of the cyber threats within our digital supply chain(s).
IQT | Information Quality Trust	• The externally exchanged cyber threat intelligence information is relevant. • The externally exchanged cyber threat intelligence information is actionable. • The externally exchanged cyber threat intelligence information is accurate. • The externally exchanged cyber threat intelligence information is of quality. • The externally exchanged cyber threat intelligence information can be trusted.

Appendix B: Survey Setup

Welcome Page
Welcome, and thank you for considering participating in this survey. Digital supply chains can be understood as interconnected cloud and software supply chains, consisting of ecosystems of cloud-based services and layered software development activities. As part of a Master's thesis, this study aims to examine how cyber threat information sharing among organisations with similar threat landscapes influences awareness of cyber threats affecting the organisations (consumer) using digital supply chains, and how trust in information influences this relationship. In simpler terms, it looks at how sharing cyber threat information between similar organisations improves awareness of potential risks in used digital supply chains, and how trust in that information affects this. You have been invited to participate because of your professional involvement in cybersecurity and/or information security. The survey will take approximately 8–10 minutes to complete. Your responses will remain completely anonymous and the data will be used solely for academic research purposes. No identifiable organisational or personal data will be collected, such as IP addresses. LimeSurvey is a European-based organisation that uses servers located in Germany and is subject to EU GDPR regulations. The survey will be available and open until the 30th of May. By continuing, you confirm that you are at least 18 years old and consent to participate in this research.
Screening Questions
1) Are you currently in a Cybersecurity- or Information Security Management related role within the organisation? Yes / No 2) Select the role closest to you role: CISO | Head of Information Security / Information Security Manager / Cybersecurity Manager / Information Security Officer / IT Risk Manager 3) Select the amount of experience you have in your role: <2 years / 2-5 years / >5 years 4) Which of these describe your organisations' primary activity? Insurance / Banking / Portfolio management or financial services / Hospital / Care providing / Government services or public administration / Other (Enter your comment here.)

5) Select the organisations' type:

Public / Private

6) Select the organisations' size (number of employees):

<50 / 50-249 / 250-1000 / >1000

7) Select the approximate number of digital services (e.g., cloud, SaaS, IaaS, Paas) your organisation utilises:

0-5 / 6-10 / 11-20 / 20-50 / 50-100 / >100

8) Which types of digital services does your organisation currently use? (multiple-choice)

Enterprise system services (e.g., ERP, accounting, procurement); Customer system services (e.g., CRM, marketing, customer support); Supply chain system services (e.g., SCM, logistics, inventory); Collaboration tool services (e.g. office tools, messaging, document management); Data & analytics system services (e.g., BI, AI/ML, dashboards); IT Infrastructure services (e.g., cybersecurity, IAM, GRC); Integration system services (e.g., middleware, BPM, workflows); Industry-specific system services (e.g. healthcare, education, manufacturing); Digital platform services (e.g., marketplaces, IoT, blockchain);

Digital Supply Chain Cyber Threat Awareness (DSCCTA)

(Likert-scale (1-7): Strongly disagree, Disagree, Somewhat disagree, Neutral, Somewhat agree, Agree, Strongly agree).

9) Please answer the following statements on the insight and awareness of digital supply chain threats on behalf of your organisation.

(Appendix A)	**1**	**2**	**3**	**4**	**5**	**6**	**7**
DSCCTA1							
DSCCTA2							
DSCCTA3							
DSCCTA4							
DSCCTA5							
DSCCTA6							

10) What is the most common technical incident cause your organisation has experienced in its digital supply chain(s)?

DDoS attack / Malware & Viruses / Ransomware / Software bug / Faulty software changes or updates / Vulnerability exploit / Identity theft / Other

11) What is the most common nature of the incident your organisation has experienced in its digital supply chain(s)?

Human error(s) / Malicious action(s) / System failure(s) / Natural phenomena(s)

12) Did your organisation suffer from a significant security incident in its digital supply chain(s) within the last 12 months?

Yes / No

Cyber Threat Intelligence Capability (CTIC)

13) Please answer the following statements on the Cyber Threat Intelligence capability on behalf of your organisation.

(Appendix A)	1	2	3	4	5	6	7
CTIC1							
CTIC2							
CTIC3							
CTIC4							
CTIC5							
CTIC6							

Cyber Threat Intelligence Sharing (CTIS)

14) Please answer the following statements on the external sharing of Cyber threat intelligence on behalf of your organisation.

(Appendix A)	1	2	3	4	5	6	7
CTIS1							
CTIS2							
CTIS3							
CTIS4							
CTIS5							
CTIS6							

Trust in Information Quality (IQT)

15) Please answer the following statements on the trust in quality of externally shared information on behalf of your organisation.

(Appendix A)	1	2	3	4	5	6	7
IQT1							
IQT2							
IQT3							
IQT4							
IQT5							

Closing Page

Thank you for your time and valuable input. Your responses contribute to academic research aimed at improving cyber threat awareness and collaboration between organisations in increasingly complex digital supply chains. Should you be interested in the outcomes of this study, you are welcome to contact the researcher to request a summary of the findings: noahspierings@securance.com. Your contribution is greatly appreciated.

Appendix C: Data Management Plan

1. 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
Online survey questionnaire		x		

* 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

My data does not contain any personal data ☒

3. Permissions and rights related to the use of data

No additional permissions and rights are related to the use of the data, once the participant continues the survey and thereby states they accept the stated use of the collected data.

3.1. Self-collected data

Online Survey Questionnaire: Section within the survey explicitly mentioning that participating in this survey automatically means giving permission to utilize produced data for the master thesis research.

3.2 Data collected by someone else

Not applicable.

4. Storing the data during the research process

Other location, please specify: ☒

The data is stored within the cloud storage in Germany of the service LimeSurvey. LimeSurvey is (almost) ISO27001-certified which entails they are working on a functioning Information Security Management System. Furthermore, at the end a back-up is made to store on the device of the researcher to ensure redundancy in case the services become unavailable. At the end of the thesis, all data will be removed from the LimeSurvey storage, leaving only the data at the researchers' disposal.

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 readme file linked to the data that describes the main points of the data ☒

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. ☒

5.3 Metadata

Metadata is a description of you research data. Based on metadata someone unfamiliar with your data will understand what it consists of. Metadata should include, among others, the file name, location, file size, and information about the producer of the data. Will you require metadata?

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

You are responsible for the data even after the research process has ended. Make sure you will handle the data according to the agreements you have made. The university recommends a general retention period of five (5) years, with an exception for medical research data, where the retention period is 15 years. Personal data can only be stored as long as it is necessary. If you have agreed to destroy the data after a set time period, you are responsible for destroying the data, even if you no longer are a student at the university. Likewise, when using the university's online storage services, destroying the data is your responsibility.

What happens to your research data, when the research is completed?

I will personally store all data for 5 years ☒; In case other researchers would like to utilise the collected data.

Appendix D: Python Data Sanitisation Script

```
import pandas as pd

# Load the CSV file into a pandas DataFrame
df = pd.read_csv("./results_survey_24-05-2026.csv", sep=',')

print(len(df.keys()))

# Remove unnecessary columns
columns_to_remove = [
    "Response ID",
    "Date submitted",
    "Last page",
    "Start language",
    "Seed",
    "Date started",
    "Date last action"
]

df = df.drop(columns=columns_to_remove)

column_names = [
    "Confirmation",
    "Roles",
    "Experience",
    "Organisation",
    "Comment",
    "Type",
    "Size",
    "NrDS",
    "Enterprise system services (e.g., ERP, accounting, procurement)",
    "Customer system services (e.g., CRM, marketing, customer support)",
    "Supply chain system services (e.g., SCM, logistics, inventory)",
    "Collaboration tool services (e.g. office tools, messaging, document management)",
    "Data & analytics sytem services (e.g., BI, AI/ML, dashboards)",
    "IT Infrastructure services (e.g., cybersecurity, IAM, GRC)",
    "Integration system services (e.g., middleware, BPM, workflows)",
    "Industry-specific system services (e.g. healthcare, education, manufacturing)",
    "Digital platform services (e.g., marketplaces, IoT, blockchain)",
    "DSCCTA1",
    "DSCCTA2",
    "DSCCTA3",
    "DSCCTA4",
    "DSCCTA5",
```

```
    "DSCCTA6",
    "TechInCause",
    "ComNatIn",
    "In12Mnth",
    "CTIC1",
    "CTIC2",
    "CTIC3",
    "CTIC4",
    "CTIC5",
    "CTIC6",
    "ICTIS1",
    "ICTIS2",
    "ICTIS3",
    "ICTIS4",
    "ICTIS5",
    "ICTIS6",
    "IQT1",
    "IQT2",
    "IQT3",
    "IQT4",
    "IQT5",
]

# Install new column names
df.columns = column_names

# turn likert-scale into quantitative scale
likert_map = {
    "Strongly Disagree": 1,
    "Disagree": 2,
    "Somewhat disagree": 3,
    "Neutral": 4,
    "Somewhat agree": 5,
    "Agree": 6,
    "Strongly agree": 7
}

df = df.replace(likert_map)

likert_columns = df.columns[1:]  # assuming first column is ID
df[likert_columns] = df[likert_columns].replace(likert_map)

mapping_NrDS = {
    "0-5": "Low",
    "6-10": "Low",
```

```
    "11-20": "Low",
    "20-50": "High",
    "50-100": "High",
    ">100": "High"
}

df["DigitalServicesLevel"] = df["NrDS"].map(mapping_NrDS)

likert_columns = df.columns[1:]  # first column is ID
df[likert_columns] = df[likert_columns].replace(likert_map)

mapping_Roles = {
    "CISO / Head of Information Security": "Management",
    "Cybersecurity Manager": "Management",
    "Information Security Manager": "Management",
    "IT Risk Manager": "Management",
    "Information Security Officer": "Non-management",
}

df["RolesLevel"] = df["Roles"].map(mapping_Roles)

mapping_employees = {
    "<50": "Low",
    "50-249": "Low",
    "250-1000": "High",
    ">1000": "High",
}

df["OrgSizeLevel"] = df["Size"].map(mapping_employees)

# make all likert-scale numeric
likert_cols = [col for col in df.columns if any(x in col for x in [
    "DSCCTA", "CTIC", "ICTIS", "IQT"
])]

df[likert_cols] = df[likert_cols].apply(pd.to_numeric, errors="coerce")

# make Confirmation and In12Mnth binary
yes_no_cols = ["Confirmation", "In12Mnth",     "Enterprise system services (e.g., ERP,
accounting, procurement)",
    "Customer system services (e.g., CRM, marketing, customer support)",
    "Supply chain system services (e.g., SCM, logistics, inventory)",
    "Collaboration tool services (e.g. office tools, messaging, document management)",
    "Data & analytics sytem services (e.g., BI, AI/ML, dashboards)",
    "IT Infrastructure services (e.g., cybersecurity, IAM, GRC)",
```

```
    "Integration system services (e.g., middleware, BPM, workflows)",
    "Industry-specific system services (e.g. healthcare, education, manufacturing)",
    "Digital platform services (e.g., marketplaces, IoT, blockchain)"]
df[yes_no_cols] = df[yes_no_cols].replace({"Yes": 1, "No": 0})

# print values of NaN and 0 in confirmation
print("\nAmount of incomplete rows: {}; \nAmount of non-confirmations: {}\n".format((len(df) -
len(df.dropna(subset=df.columns.difference(["Comment"])))), len(df[df['Confirmation'] == 0])))

# drop NaN except comment colum
df = df.dropna(subset=df.columns.difference(["Comment"]))
df["Comment"] = df["Comment"].fillna("") # for R analysis

# drop Confirmation = no (0)
df = df[df['Confirmation'] > 0]

# round all likert-scale averages
#cols_to_round = ["AwareAverage", "CapabilityAverage", "SharingAverage", "TrustAverage"]
#df[cols_to_round] = df[cols_to_round].round(2)

# Check df
print(df.head())

# Optional: convert to a NumPy array
np_array = df.to_numpy()

# Check shapes
print("DataFrame shape:", df.shape)
print("NumPy array shape:", np_array.shape)

df.to_csv("C:/Users/NoahSpierings/OneDrive - Securance/Documents/IMMIT/Masters' Thesis/Thesis
Files/Data Analysis/results_survey_readyforr.csv", index=False)
```

Appendix E: R Descriptive Analysis and Statistical Testing Code (polished)

```
# Load required libraries – to install initially: install.packages(c("...", "..."))
library(tidyverse)
library(psych)
library(car)
library(careless)
library(ggpubr)
library(effsize)
library(moments)
library(biotools)

# Import Dataset from Python
df <- read.csv("results_survey_readyforr.csv")

# inspect input
str(df)
summary(df)

# Data preparation for statistical analysis (convert to factor)
df$Type <- as.factor(df$Type)
df$DigitalServicesLevel <- as.factor(df$DigitalServicesLevel)
df$OrgSizeLevel <- as.factor(df$OrgSizeLevel)
df$RolesLevel <- as.factor(df$RolesLevel)

# Straight-lining detection
longstring_items <- df[, c( paste0("DSCCTA", 1:6), paste0("CTIC", 1:6), paste0("ICTIS", 1:6),
paste0("IQT", 1:5) )]
flagged <- which(longstring(longstring_items) > 10)

# Cronbach's Alpha reliability test
alpha(df[, paste0("CTIC", 1:6)])
alpha(df[, paste0("ICTIS", 1:6)])
alpha(df[, paste0("IQT", 1:5)])
alpha(df[, paste0("DSCCTA", 1:6)])

# Create averages
df$CTICAverage <- rowMeans( df[, paste0("CTIC", 1:6)], na.rm = TRUE )
df$ICTISAverage <- rowMeans( df[, paste0("ICTIS", 1:6)], na.rm = TRUE )
df$IQTAverage <- rowMeans( df[, paste0("IQT", 1:5)], na.rm = TRUE )
df$DSCCTAAverage <- rowMeans( df[, paste0("DSCCTA", 1:6)], na.rm = TRUE )

# Descriptive analysis
describe(df$CTICAverage)
describe(df$ICTISAverage)
```

```
describe(df$IQTAverage)
describe(df$DSCCTAAverage)
describe(…)

hist(df$CTICAverage)
hist(df$ICTISAverage)
hist(df$IQTAverage)
hist(df$DSCCTAAverage)
hist(…)

# Spearman correlation analysis (H1-H3)
cor_vars <- df %>% select(CTICAverage, ICTISAverage, IQTAverage, DSCCTAAverage)
res <- psych::corr.test(cor_vars, method = "spearman")
res$r   # correlation matrix
res$p   # p-value matrix
res$ci  # confidence intervals

# Public vs Private testing (H4a, H4b, H5)
boxM( df[, c( "CTICAverage", "ICTISAverage", "IQTAverage", "DSCCTAAverage" )], df$Type )
manova_model <- manova( cbind( CTICAverage, ICTISAverage, IQTAverage, DSCCTAAverage ) ~ Type,
data = df )
summary(manova_model, test = "Pillai") summary.aov(manova_model)

# Follow-up non-parametric tests
wilcox.test(ICTISAverage ~ Type, data = df)
wilcox.test(IQTAverage ~ Type, data = df) wilcox.test(DSCCTAAverage ~ Type, data = df)
ggboxplot(df, x="Type", y = "ICTISAverage", ylab = "Inter-organisational Cyber Threat
Information Sharing", xlab = "Organisation type")
ggboxplot(df, x="Type", y = "IQTAverage", ylab = "Information Quality Trust", xlab =
"Organisation type")

# Management vs Non-management Analysis
boxM( df[, c( "CTICAverage", "ICTISAverage", "IQTAverage", "DSCCTAAverage" )], df$RolesLevel )
manova_role <- manova( cbind( CTICAverage, ICTISAverage, IQTAverage, DSCCTAAverage ) ~
RolesLevel, data = df )
summary(manova_role, test = "Pillai")
summary.aov(manova_role)
wilcox.test( DSCCTAAverage ~ RolesLevel, data = df )
```

Appendix F: Expert Consultation Session

Purpose of the consultancy session (04-06-2026 – 45 minutes)

The consultancy session was done with two Chief Information Security Officers (CISOs): one currently operating within a public-sector care-providing organisation and one currently operating within a private Software-as-a-Service (SaaS) organisation, who previously held a comparable role within the banking sector. During the session, the research problem and questions, theoretical framework, conceptual model, constructs, hypotheses, and preliminary findings were presented. Afterwards, the experts discussed the findings, existing discussion points and provided reflections based on their professional experiences. The notes have been shared with the CISOs for validation.

Notes from the consultancy session

The experts indicated that public-sector organisations are often expected or required to participate in sector-specific knowledge-sharing centres. Within healthcare, an example is Z-CERT, where CISOs commonly register and receive cyber threat information. In contrast, private-sector organisations are generally not yet required to participate in comparable information-sharing structures. CISOs from private organisations can voluntarily register with the Dutch National Cyber Security Centre (NCSC), although this is expected to change for many organisations once the “Cyberbeveiligingswet” – Dutch translation of NIS2 directive - comes into force. The experts also noted that several industry-specific information-sharing groups exist. Banks and insurance organisations, for example, maintain CISO groups where cyber threats, vulnerabilities, and security developments are discussed collectively. Smaller private organisations generally have fewer opportunities to participate in such structures, although cyber threat information can often be obtained through alternative sources.

Timeliness of Cyber Threat Information

A topic of discussion was the importance of timeliness. According to the experts, cyber threat information rapidly relies on the timely delivery of it. The NCSC was described as sometimes lagging behind rapidly developing threats, particularly software vulnerabilities. The Log4J vulnerability was discussed as an example where other sources reportedly provided information regarding detection and mitigation before guidance became available through the NCSC. A similar observation was made regarding Z-CERT, where information may also be delivered later than through specialised commercial products or services. The experts thus again emphasised that timely information is often more valuable than simply having access to information-sharing mechanisms.

Cyber Threat Intelligence Capability

The discussion highlighted that cyber threat intelligence capability extends beyond the collection and processing activities reflected in traditional intelligence processes. One expert noted that predictive capabilities are increasingly becoming part of cyber threat intelligence practices. Modern tools that utilise artificial intelligence and indicators of compromise (IoCs) can assist organisations in predicting potential attack paths before incidents occur. The experts indicated that such capabilities contribute to awareness by enabling organisations to anticipate threats rather than only responding to existing threat information.

Information Sharing and Supply Chain Awareness

The experts suggested that inter-organisational information sharing may be most useful at tactical and strategic levels. Information-sharing relationships allow organisations to discuss broader objectives, risks, and considerations regarding digital supply chains and cybersecurity management. Threat intelligence relating to suppliers and digital supply chains can also be acquired through commercial intelligence services. According to the experts, this may allow organisations to achieve awareness more quickly than through some collaborative sharing mechanisms. The experts further observed that the awareness construct used within this study appears to reflect tactical and operational awareness. In practice, they considered information sharing particularly valuable for discussing the strategic implications of cyber supply chain risks, including questions regarding what specific risks mean for individual organisations.

Competition, Trust, and Cooperation

The experts noted that competitive relationships can influence the willingness of organisations to share cyber threat information. Some organisations may perceive an advantage in retaining information rather than sharing it with industry peers. A traditional perspective was described as organisations aiming to be "more secure than their neighbour." However, the experts emphasised that ethical considerations play an important role within cybersecurity communities. According to the experts, organisations should prioritise ethical responsibilities when they discover information that could affect others within a digital supply chain. At the same time, effective information sharing depends on the development of relationships and trust between organisations. The experts suggested that win-win situations contribute to the development of trust and increase the likelihood of information exchange.

Sharing Information About Suppliers

Finally, the experts noted that organisations often find it difficult to share information concerning suppliers and supply-chain relationships. Such information may be commercially sensitive or confidential. Nevertheless, the experts indicated that discussing supplier-related cybersecurity concerns is generally more informally accepted within cybersecurity communities than in many other business contexts. As a result, practitioners may be more willing to exchange information about supply-chain risks than might otherwise be expected.

Appendix G: Usage Log for External Tools and AI-Assisted Work

Technology statement

During the preparation of this work, I used ChatGPT in order to check spelling and grammar, coherence, enhance readability and support the development of Python and R code. The following parts of the assignment were affected / generated by AI tool usage: Introduction / literature review / research methodology / results / conclusion / discussion and appendices. After using this tool / service, Noah Spierings evaluated the validity of the tool's outputs, including the sources that generative AI tools have used, and edited the content as needed. As a consequence, Noah Spierings take(s) full responsibility for the content of their work.

Logbook for the Usage of AI Tools

Instance of AI Usage

Research stage: Proof reading.

Purpose of AI Use and Tool Used: ChatGPT was utilised to provide feedback on spelling, grammar, readability and sentence structure/phrasing. For the prompt, the researcher requested for the AI-tool to clarify the adjustments suggested so that afterwards checking was made possible.

Critical Reflection or Responsible Usage: The researcher carefully read the text and ensured that potential hallucinations were avoided. This helped with minor textual changes in spelling and consistency regarding British English versus American English, and (hopefully) improves readability. The researcher experienced that the AI-tool suggests a lot of texts(tual changes) that are redundant.

Instance of AI Usage

Research stage: Python and R code development

Purpose of AI Use and Tool Used: During the development of Python code to sanitise the data and perform the statistical analyses in R, ChatGPT was consultant on what modules to use and how to write the code for executions.

Critical Reflection or Responsible Usage: Tests were done and documentation was checked to ensure that the code executed as desired. Various personal adjustments were made, but this did speed-up the analysis phase; regarding code creation.