Evaluating information security threat in the supply chain Human factor

Akintoye, Christiana

Award date:
2023

Awarding institution:
Coventry University

EVALUATING INFORMATION SECURITY THREAT IN THE SUPPLY CHAIN: HUMAN FACTOR

By

CHRISTIANA OLAJUMOKE AKINTOYE

PhD

JUNE 2023

EVALUATING INFORMATION SECURITY THREAT IN THE SUPPLY CHAIN: HUMAN FACTOR

A Thesis submitted in partial fulfilment of the University's requirements for the degree of Doctor of Philosophy

JUNE 2023

Certificate of Ethical Approval

Applicant:

Christiana Akintoye

Project Title:

Evaluating information security issues in the supply chain: Human factor

This is to certify that the above named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Medium Risk

Date of approval:

16 September 2020

Project Reference Number:

P106106

Abstract

The protection of sensitive data is crucial for the success of corporate operations. As the threats to information security in the supply chain become more prevalent, companies face the potential for significant damage. Recognizing the increased importance of information as a critical asset, organizations must prioritize data safeguarding even more. Extensive research has shown that maintaining information security throughout the supply chain is vital for both companies and individuals. The main goal of this thesis is to uncover and thoroughly examine information security threats that impact the supply chain, offering effective strategies for organizations to mitigate these risks. Notably, there is limited existing research on addressing the human aspect of information security within supply chains, particularly concerning insider threats.

This research is grounded in three theories, including General Deterrent Theory, Social Bond Theory, Theory of Planned Behaviour, and Management Control Mechanisms. It contributes significantly to the body of knowledge by examining and evaluating the influence of these theories on threat mitigation in the supply chain in Nigeria. The research proposes a model to reduce information security threats in the supply chain, serving as a decision-making tool and reference guide for manufacturing companies. The study employed a mixed-method approach, utilizing both qualitative and quantitative methods to answer the research question and achieve its objectives. Data collection involved 498 usable online questionnaires from 150 companies, using a non-probability convenience sampling technique. The collected data underwent analysis using Structural Equation Modeling (SEM) with Partial Least Squares (PLS). Additionally, semi-structured interviews were conducted with nine subject experts with relevant experience from nine companies, and content analysis was utilized to complement the validation of the constructs.

The results indicate that top management support, attitude, and self-efficacy have a positive relationship in mitigating information security threats in the supply chain. Further analysis reveals that commitment has a positive relationship with attitude and self-efficacy in mitigating information threats. Rewards have a positive relationship with attitude, subjective norms, and a direct relationship with information security. Sanctions are significantly related to attitude and subjective norms, except for self-efficacy. Surprisingly, monitoring/evaluation has a positive relationship with attitude, subjective norms, and self-efficacy in mitigating information security threats in the supply chain. The study's final results demonstrate the appropriateness and robustness of the developed model. They also suggest that any attempt to investigate employees' behavior in information security threats in the supply chain will be incomplete unless all three theories (GDT, SBT, and TPB) and control mechanisms are considered. Lastly, the study proposes several guidelines to assist organizations in building and maintaining a successful secure information security in supply chain.

Acknowledgement

First and foremost, I want to appreciate my creator the Almighty God for His divine help and my saviour Christ Jesus and the Holy Spirit.

To my supervisors, Dr. Kamal Muhammad, Dr. Rebwar Gharib and Dr. Mahdi Bashiri for their guidance, patience and support throughout my PhD studies. I say a big thank you.

To my husband (Ilesanmi Akintoye), thank you for your, love care, understanding and financial support. A big thank you to my 3Ts (Tomi, Temi, Triumph), for your love, understanding, patience and moral support.

I am most grateful to my extended family, colleagues and friends.

To the entire management of Coventry University, please accept my heartfelt appreciation for the opportunity to carry out my research at your reputable University.

Declaration

In this thesis, Christiana Olajumoke Akintoye describe the research she conducted. The paper below contains the content material of her research which has been accepted but not yet published.

Akintoye O.C., Kamal. M., Gharib R., and Bashiri M., “Evaluating information security threats in the supply chain: Human Factor.” British Academic Management (BAM) Conference 2022, Manchester, United Kingdom.

List of Appendices

List of Abbreviation

CA	Coping Appraisal
DSL	Dynamic Security Learning
IOS	Inter-organisational Systems
IS	Information System
ISC	Information Security Culture
IS	Information Systems
IST	Information Security Threats
ISTSC	Information Security Threat in Supply Chain
ISP	Information Security Policy
ISSP	Information Systems Security Policy
IUP	Internet Use Policy
LAN	Local Area Network
MIS	Management Information System
PBC	Perceived Behavioural Control
PLOC	Perceived Locus of Causality
PRISMA	Preferred Report Items for Systematic Review Meta-Analysis Protocol
PMB	Protection-Motivation Behaviour
RAT	Routine Activity Theory
SBT	Social Bond Theory
TPB	Theory of Planned Behaviour
GDT	General Deterrence Theory
SC	Supply Chain
SCM	Supply chain management
SPAR-4-SLR	Scientific Procedures and Rationale F in supply chainor Systematic Literature Review
TA	Threats Appraisal

Table of Contents

LIST OF FIGURES

LIST OF TABLES

Chapter 1: Introduction

1.1 Introduction

The importance of information security has increased in the modern business landscape due to the rising frequency and complexity of cyber-attacks. Safeguarding critical information and infrastructure has become a vital aspect of conducting business. The security of organisations is significantly affected by the supply chain, which involves the entire process of obtaining and distributing products and services. This poses a significant security risk as there are numerous internal and external parties with access to private data and infrastructure. It is widely known that relying solely on technology is insufficient for creating a secure environment for information assets. Additionally, it is crucial to consider the human aspect of information security within supply chains.

Literature reports indicate that insiders, such as authorised non-technical employees, are the primary cause of threats to information security. Insider threats have historically been the most common source of incidents. Inadequate user management allows insiders to misuse systems by exploiting their access privileges. There is limited research on incorporating the human aspect of information security in supply chains to mitigate insider threats. Therefore, further research is needed to address information security threats in supply chains. Existing models related to information security threat mitigation in public, private, and healthcare sectors may not be applicable or valid for supply chains. Factors influencing threat mitigation in information security in the supply chains (INTSC) may differ between developed and developing countries. Moreover, differences exist among influential factors in public, private, and healthcare organizations. Despite commonalities among these models, there is currently no specific model investigating INTSC.

This chapter discusses all the aforementioned issues. Section 1.2 provides background information on the research problem, while Sections 1.3 and 1.4 outline the research questions to be addressed. The research methodology is described in Section 1.5, followed by the research context in Section 1.6. The contribution of the research is discussed in Section 1.6, and the aims, objectives, and thesis outline are presented. Finally, Section 1.7 summarizes the conclusions.

1.2 Background to the research problem

Given the persistent occurrence of data attacks, system disruptions, and malicious software, ensuring information security remains a vital undertaking for contemporary organisations. Various aspects such as industrial design, infrastructure control, expert knowledge, and organisational information assets necessitate a stringent level of confidentiality. Additionally, in numerous organizations, information holds the status of a competitive resource, and the repercussions of its leakage can be severe, encompassing reputational damage, intellectual property loss, reduced productivity, diminished

competitive advantage, increased costs, and, in the worst-case scenario, insolvency (Safa et al., 2016; Ahamad et al., 2014)

Supply chain management (SCM) holds immense significance in today's corporate landscape. Efficiently managing supply chains is vital for all stakeholders aiming to gain a sustainable competitive edge (Maskey et al., 2017). The performance of a thriving supply chain can be influenced by information security (Durowoju et al., 2020). Researchers and supply chain managers are particularly interested in identifying the critical factors that contribute to secure data exchange across supply chain interfaces (Kembro et al., 2014). Sindhuja (2021) further emphasizes that the concept of information security has been in existence for a decade, with its fundamental purpose being to ensure the confidentiality and reliability of data during storage and transmission.

Similarly, businesses and organisations heavily rely on diverse platforms for data generation, transfer, and storage. While these platforms offer ample commercial opportunities, they are also plagued with security vulnerabilities and deficiencies. In today's platform economy, information system security needs to be approached not only from an information system (IS) and information technology (IT) perspective but also from an organisational standpoint, which holds broader significance and appeal (Brotbyand, 2013). However, due to technological advancements, the focus of information security practices seems to have shifted from addressing minor security breaches at the system level to managing highly vulnerable organizational conditions (Sindhuja, 2021). The reliance on technological systems that govern critical information has reached a precarious level, with increasing invasiveness (Moletsane and Tsibolane, 2020; Snyman and Kruger et al., 2017; Pham et al., 2017; de Barros et al., 2015). Consequently, information has emerged as a vital asset within the supply chain, necessitating heightened protection of organisational data (Karlsson, 2016).

Information security issues pose threats to an organisation's valuable information assets, and various challenges in the supply chain relate to risks associated with information transmission. In this thesis, these challenges are referred to as threats. The evolution of technology-enabled information exchange has resulted in an expanded number of entry points to sensitive company data. While flexibility, scalability, and efficiency are some benefits of these developments, they also raise the potential for critical data loss, which is the center of efficiency and growth in the corporate world (Sindhuja, 2021). Identifying information security threats within the supply chain, both in general and specific scenarios, proves to be a challenging task according to existing research. This issue is considered a cyber-risk in certain situations due to the presence of general and targeted data threats (Abd Latif et al., 2021), supply chain risks (Ghadge et al., 2012), supply chain vulnerability (Collicchia et al., 2019), supply chain disruption (Durowaiye, 2014), uncertainty in the supply chain (Sanches-Rodrigues et al., 2010), and supply chain security (Sharma et al., 2015). However, studies conducted by Baker et al. (2007), Du et

al. (2012), and Wang et al. (2014) indicate that not all information security issues throughout supply chains have been fully explored, emphasizing the need for further research to address these threats.

The availability of 24/7 internet access brings forth not only numerous opportunities but also a multitude of challenges, including threats to information security (Soomro et al., 2016). Among these challenges, insider threats continue to be a major concern for information systems security managers (Willison and Warkentin, 2013). Numerous instances of cybersecurity breaches caused by employees are readily available, with many of these breaches being unintentional. For example, an employee inadvertently forwarded the Social Security numbers of 2,400 insurance agents to a broker (Crosby, 2013). According to Verizon's annual Data Breach Investigations Report, approximately 58% of cybersecurity incidents in the public sector were caused by employees (Government Security news, 2014). Within this 58%, 34% were due to staff mishandling of data, while 24% were attributed to unauthorized or malicious use of data (Government Security news, 2014).

The human factor is a critical aspect that can contribute to the vulnerabilities of information security within the supply chain. Literature indicates that employees, contractors, and suppliers who have access to the information systems and data of the supply chain have the potential to intentionally or accidentally trigger security breaches, leading to significant repercussions for the organization. Therefore, it is crucial to assess the role of humans in the risks posed to information security by the supply chain and develop effective methods to control and minimize these threats.

Moreover, recent research has demonstrated the effectiveness of technological elements in mitigating these risks. Mathematical modelling has been utilized to establish a connection between strategic goals and risk indicators, reducing the likelihood of adverse outcomes (Ganguly and Guin, 2013). The Analytical Hierarchy Process (AHP) has been employed to break down supply chain threat risk categories (Gaudenzi and Borghesi, 2013). The development of blockchain technology has significantly mitigated the risk of data tampering (Gupta et al., 2020; Zhang et al., 2020; Preveneers et al., 2017). Other technological measures, such as intrusion detection (Barron et al., 2016; Boiko et al., 2019; Gupta et al., 2017) and malware injection prevention (Couce-Vieira and Houmb, 2016), have also contributed to enhancing information security. However, previous studies emphasize that technology alone cannot be solely relied upon. The majority of vulnerabilities in the information security of the supply chain can be attributed to human error. Rao et al. (2014) and Evans et al. (2019) highlight that human error accounts for 51% to 80% of recorded data breaches in information security since humans are responsible for designing and managing technology.

Regardless of whether intentional or unintentional, human behaviour poses a significant threat to the confidentiality of information assets (Safa et al., 2016). When examining information security scenarios related to the supply chain, humans are often considered the weakest link (Alhogail et al., 2015; Hu et al., 2012). However, despite human error being the most prevalent source of security breaches, many

companies still prioritize technological solutions (Safa et al., 2016; Evans et al., 2018). Nevertheless, there is a lack of empirical studies exploring how human factors interact with supply information security vulnerabilities and how these threats can be managed from a human factor perspective.

Regardless of whether intentional or unintentional, human behaviour poses a significant threat to the confidentiality of information assets (Safa et al., 2016). When examining information security scenarios related to the supply chain, humans are often considered the weakest link (Alhogail et al., 2015; Hu et al., 2012). However, despite human error being the most prevalent source of security breaches, many companies still prioritize technological solutions (Safa et al., 2016; Evans et al., 2018). Nevertheless, there is a lack of empirical studies exploring how human factors interact with supply information security threats and how these threats can be managed from a human factor perspective.

Previous empirical studies have explored the relationship between supply chain information security threats and human behaviour in various countries. Safa et al. (2016) conducted a study in Malaysia and found that employee commitment and personal norms influence their attitude, which, in turn, affects their information security behaviour. Ifinedo (2012) conducted research in Canada and indicated that staff attitudes and perceptions of their co-workers impact their intention to comply with information systems security policies (ISSP). Merhi and Ahluwalia (2019), in their study conducted in the United States of America, discovered that employee awareness of the severity of sanctions positively influences compliance with information security policies. Similarly, studies by AlMindeel and Martins (2021) in Saudi Arabia and Dang Pharm et al. (2022) in Australia have also examined these factors. However, Safa et al. (2018) and Safa et al. (2019) focused on applying a theoretical model to mitigate insider threats to information security in organizations, conducting their studies in South Africa and the United Kingdom, respectively. Despite the noteworthy study by William et al. (2019) analysing employee information security compliance behaviour in Nigerian banks and Alese et al.'s (2014) comprehensive examination of cyber threats in Nigeria, the issue of information security threats in the supply chain of Nigerian companies has not yet been addressed.

Nigeria is demonstrating a growing commitment to cyber security, evident in the adoption of risk management programs and increased vigilance in the field (Aladenusi, 2020; CBN, 2018). The country's e-commerce, banking, and telecommunications sectors, with Nigerians being the world's eighth-largest internet users, have a significant presence of digitally engaged and banked mobile customers (Olasanmi, 2019; Wang, Nnaji, & Jung, 2020). Cybersecurity challenges and the Information Security Threats Supply Chain (INTSC) in Nigeria are particularly complex and of global concern due to the increasing ingenuity of fraudsters in devising their schemes (Wang, Nnaji, and Jung, 2020). Several studies have focused on cyber security issues and challenges in Nigeria (Frank and Odunayo, 2013; Oforji, Udensi, and Ibegbu, 2017), but only a few researchers have addressed specific management problems

individually (Okolo, 2016; Osho, 2015). The practical measures adopted by organizations to protect themselves in this context remain largely unknown (Okolo, 2016). Furthermore, the review of published studies on information security highlights the under-researched area of mitigating factors for implementing risk management systems in developing countries (Blanchard, 2010).

Further research is necessary to assess information security threats in the supply chain, considering various potential factors that can jeopardize the availability, confidentiality, and integrity of sensitive data and systems. The human factor, which includes employees, contractors, and suppliers with access to the supply chain's information systems and data, is a crucial aspect to be considered. Several models proposed by experts aim to protect information by focusing on the human aspect. The compliance with Organizational Information Security Policies and Procedures (OISPs) model has been suggested as an effective approach to mitigate information security breaches (Cuganesan et al., 2018; Ifinedo, 2014; Safa et al., 2016). Another approach is the Information Security Knowledge Framework, which enhances employees' knowledge and awareness of information security threats (Safa et al., 2016; Hanus et al., 2016). The conscious care behaviour model, based on information security awareness and experience, has also been presented as an effective approach to reduce human errors in the field of information security (Safa et al., 2015). However, while these models offer insights into information security in the supply chain, not all their factors may have the same influence on the Information Security Threats in the Supply Chain (INTSC). Therefore, it is necessary to explore the applicability of these information security models specifically to INTSC, considering theories such as General Deterence Theory (GDT), Social Behaviour Theory (SBT), Theory of Planned Behaviour (TPB), and control mechanisms.

Given the existing problems concerning information security threats in the supply chain, it is crucial to (a) identify these threats, (b) investigate the impact of human behaviour and approaches, and (c) conduct empirical research on this topic in Nigeria. Therefore, this study aims to address the research question outlined in the following section.

1.3 The overarching research question:

- How do the supply chain employees mitigate information security threats in the supply chain?

1.4 Sub research questions

- What factors influence employees' information security behaviour in an organisation’s supply chain?
- What factors mitigate information security threats in the supply chain?

1.5 Research methodology

The research determined that employing a fully mixed concurrent equal status design approach, combining quantitative and qualitative methods, would be the most effective strategy to address the research questions and achieve the study objective. Before testing the model, it was crucial to ensure that the structures identified in the previous study accurately represented reality. While triangulation is typically accomplished by sequentially integrating quantitative and qualitative methods, in this study, the initial quantitative phase was used solely to validate the constructs rather than for triangulation purposes. Therefore, a convergent paralled mixed methods approach was chosen, utilizing quantitative methods to verify the proposed model and qualitative complement the investigation of the constructs (Creswell, 2012).

The quantitative and qualitative study was conducted among selected employees from the Marketing and Distribution, Logistics and Transport, Production and Operation, and Manufacturing sectors in Nigeria. A self-administered questionnaire was utilized for the quantitative survey, hosted online on Qualtrics, a platform specialized in online surveys. In the initial step of data collection in Nigeria, the survey questionnaire was distributed to individuals working in the sectors. The sample frame included companies from Lagos and Abuja. Partial Least Squares Structural Equation Modelling (PLS-SEM) software was employed for statistical analysis, which is commonly used in the social sciences.

1.6 Research Significance

The significance of a study lies in its ability to address existing and emerging problems and contribute to the existing body of knowledge. This study on information security threats in the supply chain of manufacturing firms in Nigeria is important because it provides knowledge that can help manufacturing firms and business executives in general address current issues related to information security in the supply chain. The study also contributes to academia, industry, and society by generating valuable insights.

One of the key contributions of this study is enhancing the understanding and awareness of manufacturing firm executives regarding information security threats in the supply chain. It equips them with the knowledge to develop and improve their understanding of the severity of different information security threats in supply chains. This knowledge can guide decision-making and enable the implementation of effective measures to protect information from an academic perspective, this study enriches the existing literature on supply chain management by providing secondary data and insights for researchers interested in further exploring supply chain information threats and related concepts.

Furthermore, users of supply chain information will find this study valuable as it sheds light on major information security threats in supply chain firms and their relative severity. The broader society will benefit from this study through increased knowledge and a better understanding of how economic

entities operate. As organisations thrive and succeed, they contribute to the overall well-being of citizens. The findings of this study will equip organisations, particularly manufacturing firms, with essential knowledge to secure critical information, ensuring their competitiveness and long-term sustainability.

1.7 Research Context

In Nigeria, there has been a rise in information security threats and cyber threats since the late 1990s. Various entities, including government organizations, non-governmental organizations, supply chains, public sectors, and non-profit organizations, have joined forces to combat these cyber threats (Allen et al., 2018). Nigeria is currently ranked as the 8th largest internet user globally, particularly in the fields of e-commerce, banking, and supply chain industries (Olasanmi, 2019; Wang, Nnaji and Jung, 2020). The increasing concern regarding cybersecurity challenges in Nigeria stems from the fact that cybercriminals are becoming more sophisticated in their fraudulent activities (Wang, Nnaji and Jung, 2020). These cybercriminals employ various tactics, such as shifting dimensions, size, technological proficiency, and complexity, to effectively target profitable organisations, including businesses, large corporations, and governments, for financial gains (Hinchliffe, 2017).

Nigeria has been identified as a vulnerable nation in terms of information security. While the introduction of the internet brought promising opportunities, it also came with significant disadvantages for the country. The recent surge in cybercrime in Nigeria has been alarming, and its negative impact on the country's socio-economic landscape is deeply concerning (Williams, Maharaj and Ojo, 2019). Several researchers have focused on issues related to information security and cybercrime in Nigeria (Jegede, 2014), with a particular emphasis on combating fraud through technological means. Their studies have examined the effects of adolescent criminality, theft, and cybercrime on Nigeria's financial and supply chain industries, as well as the impact on employee performance and financial losses in the sector (Jegede, 2014). Other research has explored how criminal law can aid in the prevention of cybercrime and how information security compliance can safeguard businesses (Akinyomi, 2012). Additionally, Allen et al. (2018) have discussed the technological aspects of cybercrime, the role of law enforcement in detection and apprehension, and the legal implications of prosecution. Various empirical studies have assessed the effectiveness of organisations' information security practices (Dhillon and Torkzadeh, 2006; Straub and Collins, 1990; Reyes, 2007).

However, there are gaps in comparable research that specifically address information security standards in the Nigerian supply chain, particularly in relation to international information security standards. The methods employed by businesses to safeguard against threats are largely unknown (Baskerville et al., 2018). Against this backdrop, this research aims to expand the boundaries of knowledge by addressing these gaps. The background discussion highlights the significant research problem that remains unaddressed, namely information security threats in the supply chain, which requires more empirical

and in-depth investigation. Therefore, there is a need for the supply chain to prioritize raising awareness and recognizing the importance of human factors that influence the mitigation of information security threats in the supply chain.

1.8 Aim and Objectives

The fundamental premise of this thesis is based on existing reports that highlight humans as the most significant threat to information security in the supply chain. The majority of vulnerabilities in supply chain information security stem from human errors or intentional and negligent human behaviour (Safa et al., 2016). As information has become a crucial asset in the supply chain, safeguarding organisational data has become increasingly critical (Karlson, 2016). Research has indicated that humans are the weakest link in the defence against information security threats, specifically in supply chain settings (Alhogail et al., 2015; Hu et al., 2012). Addressing this research gap is imperative due to the escalating prevalence of information security threats in the supply chain.

This study aims to investigate information security threats within the supply chain by considering relevant behavioural theories that explain employee behaviour to these threats. The major theories employed in this study are the Theory of Planned Behaviour (TPB), Social Bond Theory (SBT), and General Deterrence Theory (GDT). By integrating these three behavioural theories with a management control mechanism, a framework is proposed to mitigate information security threats in the supply chain. Consequently, the aim of this thesis is to:

Study information security threats in the supply chain and develop a model to minimize these risks within the supply chain.

The specific objectives of this research are as follows:

Objective 1: Critically review prevalent threats in information security within the supply chain.

Objective 2: Identify and investigate the influence of human factors on mitigating information security threats in the supply chain.

Objective 3: Develop and propose an integrated human behaviour model for mitigating information security threats in the supply chain.

Objective 4: Provide recommendations for business owners and managers to enhance and secure their information security in the supply chain.

1.9 Thesis Structure

Figure 1.1 shows the seven chapters that make up this thesis. Chapter 1 outlines the research background and discusses why it was necessary to conduct the study, which led to the development of the study's research questions and objectives. In Chapter 2 of this research, relevant literature reviews are done on a wide range of topics, such as information security threats, supply chain management, the human

factor, information and management, and social and behavioural theories. In Chapter 3, the results of the earlier literature review are used to build a conceptual research framework. The conceptual framework is made up of several hypotheses that are intended to be tested to determine how to mitigate information security threats in the supply chain. The research methodology is further explained in Chapter 4. It examines the quantitative and qualitative approaches while collecting the data. In Chapter 5, PLS-SEM was utilised as a statistical method for the quantitative and content analysis was use for qualitative data analysis procedures. This chapter also includes the findings of the analysis. These findings are discussed in detail in Chapter 6. Lastly, Chapter 7 encapsulates the thesis, the contributions, implications, limitations and future of the research.

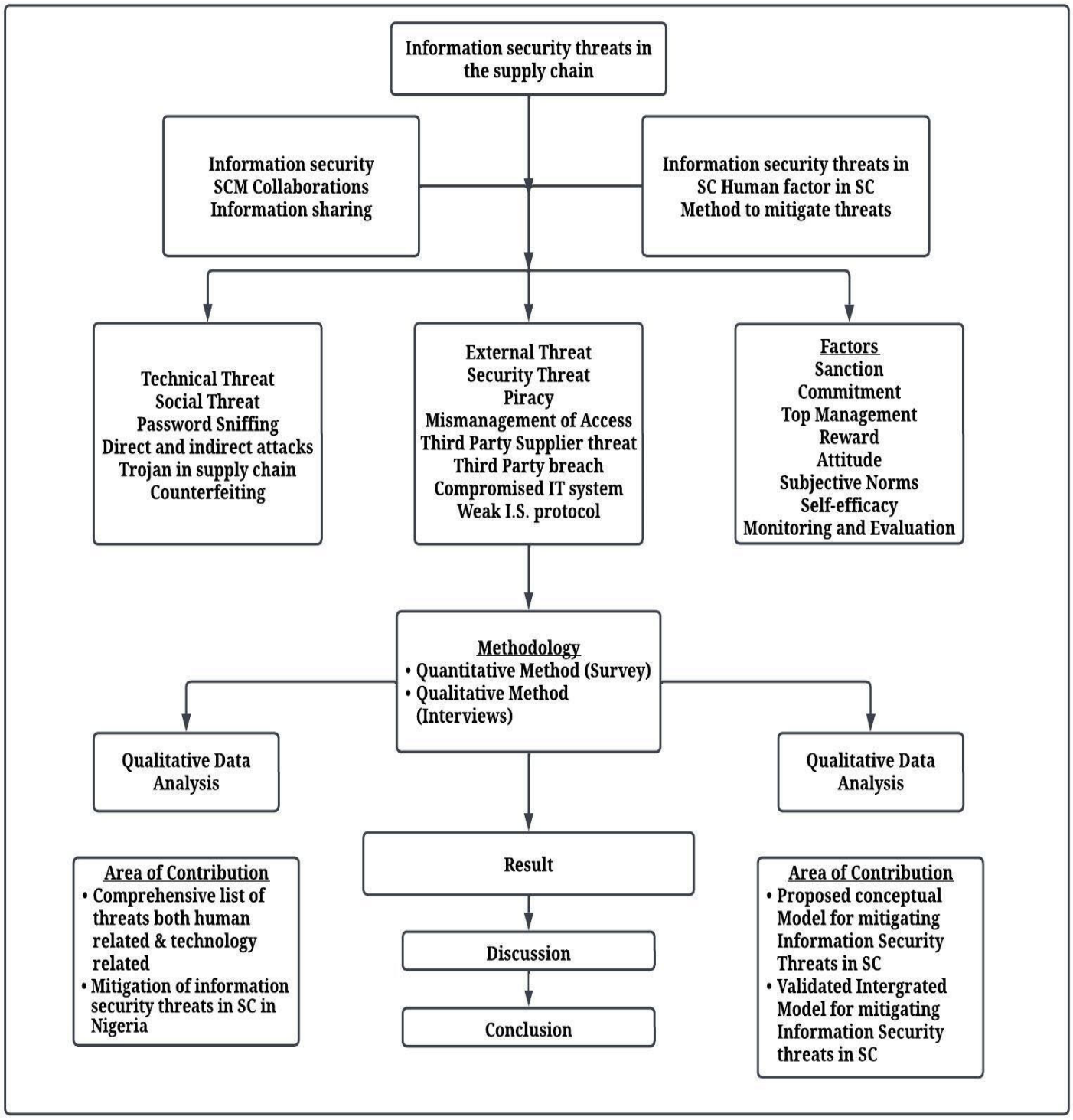


Figure 1.1: The Research Process

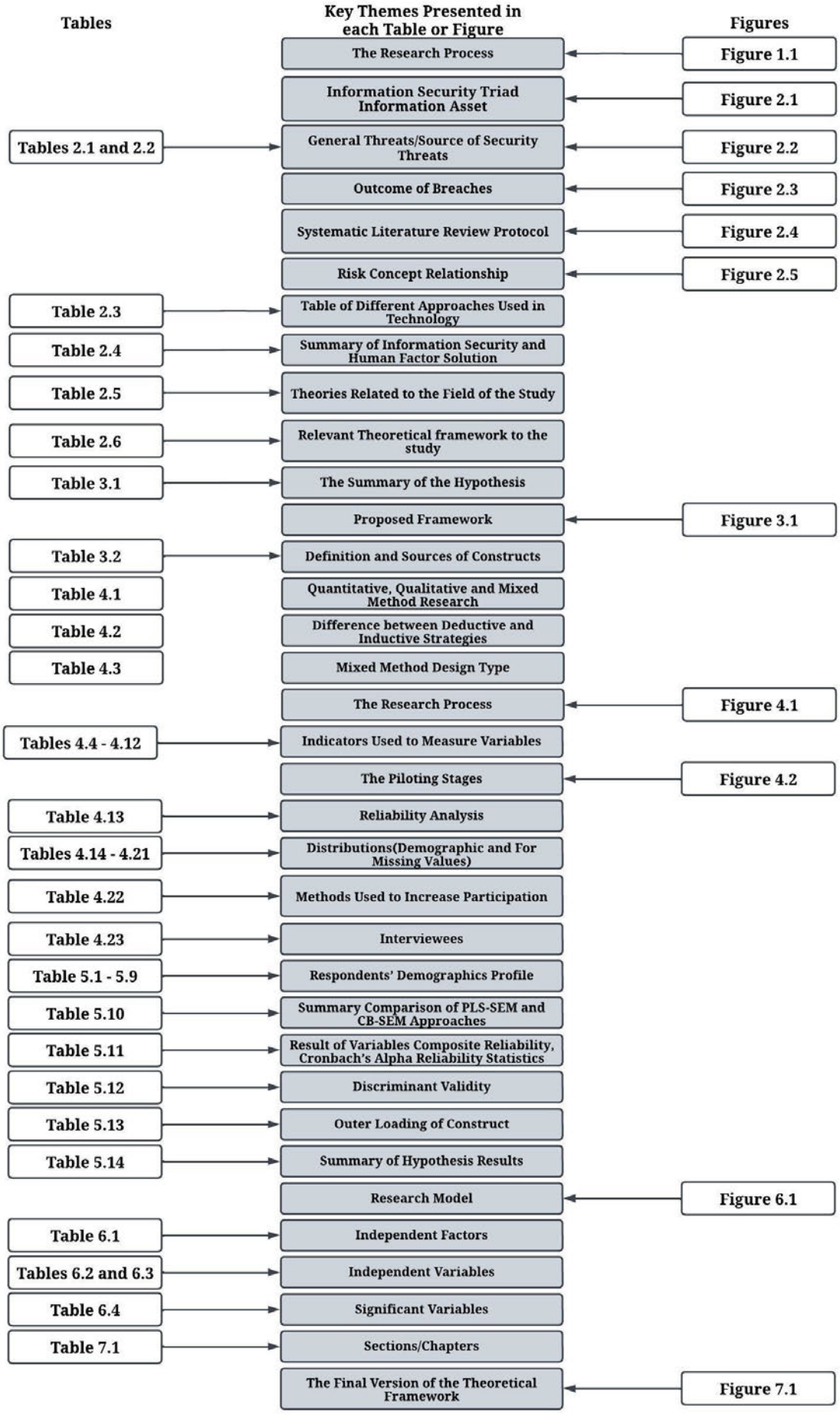


Figure 1.2: Thesis story through tables and figures

Chapter 1: Introduction

Chapter 1 provides an overview of the research focus, which is on information security threats in the supply chain. It emphasizes the importance of considering human factors alongside technology in mitigating these threats. The chapter also states the aim, objectives, and provides an outline of the thesis.

Chapter 2: Literature

Chapter 2 introduces the research field and establishes the scope of the study. It explores information security in the supply chain and categorizes threats into technological and human-related through a systematic literature review. The chapter also discusses current research conducted on information security threats in organizations and highlights relevant theories and proposed frameworks for further investigation.

Chapter 3: Theoretical Framework

Chapter 3 presents a conceptual framework for understanding and mitigating threats in the supply chain. It draws on theories such as the General Deterrence Theory, Social Bond Theory, Theory of Planned Behaviour, and Management Control Mechanisms. The proposed framework serves as a tool for mitigating threats and guiding practitioners and researchers in reducing information security threats in the supply chain**.**

Chapter 4: Research Methodology

Chapter 4 outlines the research methodologies employed in addressing the research issues. It explains the research philosophy, justifies the chosen mixed-method strategy, and discusses the research strategy and design. The chapter also describes the strategies used for empirical data collection, including questionnaire development, pilot study, and semi-structured interviews conducted with employees from the manufacturing business and other sectors.

Chapter 5: Data Analysis

This chapter details the data analysis techniques employed to address the research questions stated in the previous chapter. The chapter consists of two sections. The first section focuses on quantitative data analysis and covers various aspects such as coding technique, data cleaning, and analysis of missing values, demographic data analysis, assessing data normality, identifying outlier observations, examining linearity and co-linearity, and verifying sample size. The second section provides an overview of both the quantitative and qualitative data analysis, including demographic information.

The third section presents the findings obtained through Structural Equation Modelling (SEM). This section is further divided into two major parts: evaluating the reliability of the scales used and

conducting PLS-SEM. The measurement model's validity was assessed using PLS-SEM variance. A test was performed on the hypothesized conceptual model, whereby observable data were produced as a result of the existing causal relationships. Lastly, the chapter includes the analysis of the interview results.

Chapter 6: Discussion

Chapter 6 discusses the findings from the empirical data analysis and the results of the structural equation modelling. It relates these findings to the testing of hypotheses and compares them with previous studies in the field.

Chapter 7: Conclusion, Contribution, Further Research and Limitation

Following a summary of the findings presented in the previous chapter, a discussion ensues, highlighting the key contributions made by this study. The limitations of the study are then addressed in the subsequent section, followed by a discussion on potential avenues for future research. This discussion serves as the concluding part of the chapter.

Chapter 2: Literature Review

2.1 Introduction

This study reveals lack of knowledge regarding the human factors influencing the mitigation of threats within supply chains. While existing studies in the fields of information security threats in supply chains, as well as other sectors and countries, may shed light about interest, they cannot be readily applied or generalised to the Nigerian context without validation. One possible explanation for this is the significant variation among sectors, largely due to the unique characteristics of the supply chain.

The literature review goes beyond previous research summaries by identifying threats in the supply chain and examining both technical and human factors in mitigation approaches. It provides a comprehensive analysis of selected relevant published literature, along with the corresponding references, focusing on the topic under investigation (Hart, 2018). Chapter 2 encompasses a review of previous studies, methodologies used, and discussions critiquing the existing literature.

The chapter begins by exploring the concepts of information security in section 2.2, followed by a systematic review of the literature in section 2.3. Section 2.3.2 identifies general threats, while sections 2.4 and 2.4.2 explain security risks and the control of threats, respectively. Before delving into the discussion on the supply chain concept, section 2.6 provides a review of supply chain and supply chain collaboration, with section 2.6.1 offering an explanation. Furthermore, section 2.6.2 and section 2.6.3 describe supply chain and information sharing, as well as the challenges associated with information sharing in the supply chain. Section 2.6.4 elaborates on information security in the supply chain. Section 2.7 begins by analysing information security threats in the supply chain literature and identifying the threats present. The consequences of these threats are explained in section 2.7.1. Subsequently, section 2.8 elucidates the management of potential threats, followed by section 2.9 which focuses on the human factor in information security and the supply chain.

The researcher evaluates current literature on both technological and human approaches to threat mitigation in sections 2.10 and 2.11, respectively. Section 2.12 highlights relevant theories related to the field of study, and finally, the research gap is discussed.

2.2 Information security

There is a growing collection of body of literature that discuss the topics of data, information security, and system security. Below is a summary of information security with the supply chain, followed by sections covering the definitions of information security, its guiding principles, the concept of information as an asset, potential threats and risks and measures taken to control and mitigate them. This includes standards that can be implemented to achieve the objectives and principles.

2.2.1 Definition

Information security has gone by a few other titles in the past, including IT security, computer security, cyber security and data security. Except for data security, these definitions fail to account for the reality that value the data stored on the computers much exceeds the value of the machines themselves. Information security is the practice of keeping sensitive data and computer systems safe from unauthorised access and use, disclosure, disruption, modification, perusal, inspection, recording or destruction, in order to meet the information security principle (Yinka, 2011).

These authors assert that information security is about restricting who can access the data so that the data maintains confidentiality, integrity and is available always to authorised users (Nel and Drevin; Zhon and Whinston 2013; Pfleeger and Pfleeger 2007). Informational assets are discussed below. Whitman and Mattord (2011) updated definition emphasise the need for data security at all stages of the information lifecycle.

The term “information security” refers to the state of being protected against unauthorised access or use of information, particularly digital data, and how this protection is achieved (Zhon and Whinston 2013). Information security, also known as infosec, involves the set of practices that manage system resources and policies to detect, monitor, and respond to threats to both digital and analog information. According to Rhee, Kim and Ryu (2009), the goal of information security is to implement operational procedures that safeguard sensitive data during its usage, transmission, processing and storage. Ma et al., (2008) present various research-based information security objectives and best practices. In their study, they identify multiple security strategies that aimed at preserving information security (Ma et al., 2008). As businesses heavily rely on information systems for their daily operations, any failure in these systems can result to financial losses (Bulgurcu et al., 2010).

In the realm of information security, the principle of availability ensures that authorised users have uninterrupted access to the system whenever they require it (Tipton and Krause, 2007). These three principles (confidentiality, integrity, and availability) have been demanding for robust information security measures. As technology and its applications have evolved, two additional principles have come into play: authenticity and non-repudiation have evolved (Tipton and Krause, 2007). Validating the authenticity of involved parties, confirming their true identities, becomes crucial in ensuring the

genuineness of transactions conducted over the internet. On the other hand, non-repudiation entails that that neither party involved in a transaction can deny having sent or received it.

In summary, information security encompasses the whole safeguarding of data throughout its storage, processing, or transmission phases to guarantee confidentiality, integrity and availability (CIA) and prevent the unauthorised creation, alteration, interruption and interception of the data.

Table 2.1: Definitions of Information security

S/N	Definition of Information Security	References
1	Application of a risk management approach to preserve information's confidentiality, integrity and availability while ensuring that it is not compromised and is still accessible to authorised users when needed.	ISO/IEC 27000:2021
2	Information security is a condition of information and information processing well-being that guarantees the required level of confidentiality, integrity and accessibility of information in order to protect the security of the organisation and its stakeholders.	Nel and Drevin, (2019)
3	Protecting data from unauthorised access, use, disclosure, interruption, alteration, or destruction is the process of information security. The objective is to guarantee the availability, confidentiality and integrity of information and the systems that support it.	Zhon and Whinston (2013)
4	Information security is the process of preventing unauthorised access to, use of, disclosure of, interruption of, alteration of, or destruction of information and information systems in order to maintain the confidentiality, integrity and availability of information.	Al-Dhahri, Al-Sarti and Abdul (2017)
5	Information security is the use of policy, education, training, awareness, and technology to secure the confidentiality, integrity and availability of information assets, whether they are being stored, processed or transmitted.	Whitman and Mattord (2012)
6	Defines information security as ensuring data integrity, confidentiality, availability and operating procedures by safeguarding the information, the system, and the hardware that stores and transmits the information. Protecting information assets against numerous threats to guarantee business continuity, lessen risks to the firm, and boost profits and opportunities is how the worldwide standard for information security management, ISO17799/ISO27002, defines information security.	Alkhudhayr et al. (2019)

2.2.2 Principle of information security

The CIA is an acronym for the three pillars of information security, as stated in the definitions. Figure 2-1 demonstrates information security concepts. Listed below are descriptions of each guiding principle:

In order to maintain privacy, it is necessary to prevent authorised users from accessing data. Safeguarding the confidentiality of sensitive information is crucial (Yinka, 2011). There is multiple potential risk that could jeopardise personal data. Examples include hackers, unauthorised user actions downloading files without protection, local area networks (LANs) and Trojan horses. These are just a few of the typical threats to data privacy.

Data integrity refers to the accuracy and comprehensiveness of information. It also relies on the trustworthiness and dependability of the data. The integrity of data is a measure of truthfulness and reliability (Yinka, 2011). Implementing access restrictions is vital for ensuring data security, making it crucial to positively and clearly identify all individuals who gain access. Potential threats to data or program integrity, like their impact on confidentiality, include hackers, impersonators, user activities,

downloading without protection, local area networks (LANs), and unauthorised programs like Trojan horses and viruses. If authorised users are not adequately monitored, they can unintentionally or deliberately cause harm to system data and software (Whitman and Mattord, 2012)

Meanwhile, availability ensures that authorised users can access the system whenever they need it (Tipton and Krause 2007). These three principles have been fundamental to information security since the early days of computing, and the demand for information security continues to grow. As technology and its usage have evolved, two additional authenticity and non-repudiation have been introduced (Tipton and Krause 2007). It is important to validate the authenticity of the parties involved, that they are who they claim to be, to ensure transactions via the Internet are genuine. On the other hand, non-repudiation implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.

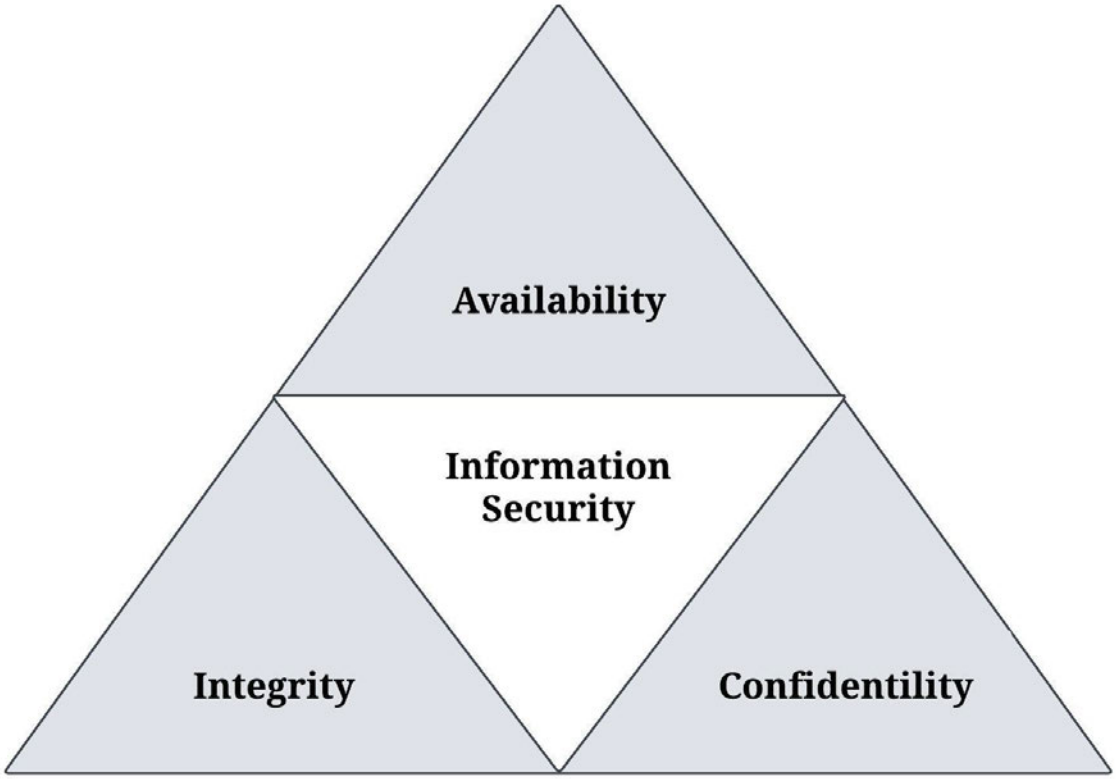


Figure 2.1: Information Security Triad

According to the definition in Section 2.2.1, and Table 2.1, information needs to be protected. Information assets are sometimes referred to as information resources and include hardware, software and people that organisations use to perform computing tasks (Pfleeger and Pfleeger, 2007). Evans (2003), in Information Security Guideline for New South Wales (NSW) Government, has defined an asset as below:

"*An asset is something that the agency values and, therefore, must be protected. Assets include all the information and supporting items that an agency requires to conduct its business. Examples of assets include*:

Assets, as described earlier, may be called information which can exist in many forms. As suggested by ISO 17799, information is an asset which can be "printed or written on paper, stored electronically and transmitted by post or by using electronic means. Whatever form that information takes, or means by which it is shared, it should always be appropriately protected from any possible information security threats.

2.2.3 Information security threats

Due to severe repercussions associated with a failed information system, it becomes necessary to examine various types of information-related issues. It should be noted that no two threats are precisely identical and their impact on a company and its supply chain differ as well. Consequently, it is essential for individuals to understand the extent of harm that each type of threats can cause to an organisation or its supply chain. According to Sarkar (2010), an information security threat is defined as any event or behaviour that has the potential to harm or disrupt the functioning of an information technology system. From the perspective of an information system, a threat encompasses anything that may result in unauthorised access, destruction, disclosure, alteration of data, or denial of service.

The discussion of information security threats can be examined from different perspectives, including source of threats (insider and outsider threat), the type of threats (intentional or unintentional), the type of impact (fabrication, modification, interception or interruption), and the severity of impact (operational impact, monetary impact, regulatory or reputation). Insider threats specifically involve employees with access to relevant information transferring it to unauthorised parties. The anonymity of insiders often serves as an incentive for engaging in illicit activities in this context (Cheng et al., 2013). Despite the distinct perspectives there exists a certain level of interconnectedness among them. This viewpoint is supported by Urcioli et al., (2013) who proposed a chain of threats: threats source – vulnerability factor – threats action – attack implications.

2.2.3.1 Threats Source

According to Parker (1981), there are three main categories of threats to information security: human-caused accidents, natural disasters, and intentional attacks. The first two occur randomly, while the third involves deliberate planning. Figure 2-2 provides a possible depiction of the origins of security vulnerabilities. The most significant threats to safety and security are humans and natural disasters. In the case of natural disasters like hurricanes, floods, fires, and earthquakes, computers and other components of the information technology infrastructure are particularly vulnerable to destruction. Yinka (2011) suggests that preventing natural disasters is nearly impossible but being prepared with a

business continuity plan and a disaster recovery strategy is the most effective way to manage the aftermath of such events.

Individuals can pose a risk to an organization in two distinct ways: through intentional actions that cause harm, or through unintentional actions that result in disruptions to the business. Both external entities and individuals within an organization can potentially be malicious actors, commonly referred to as attackers. Hackers and crackers, who lack authorized access to a system, are examples of external threats. These individuals may knowingly exceed their authorized boundaries within the system as well (Urciuol et al., 2013). However, the most significant threat arises from dishonest insiders, such as current or former employees, who possess malicious intent and possess knowledge of the organization's codes and security protocols (Fagnot and Paquette, 2012). Yeboah-Ofori and Islam (2019) describe that authorised users who misuse their access or privileges represent an internal threat.

According to Oforji et al., (2017), the most significant non-malicious threat to a company's network arises from employees who lack training. Users, data entry personnel, system operators, and even programmers may make errors that jeopardize system security. Incorrect data input or programming mistakes can greatly increase the risk of system failure (Whitman and Mattord, 2012). These errors can occur at any stage of the system's life cycle, thereby heightening its susceptibility to intrusions.

2.2.3.2 Factor (vulnerabilities)

Vulnerability analysis is an additional approach employed to understand information security threats. ISO/IEC 27005:2008 defines a vulnerability as any weakness in an asset or group of assets that could be exploited by one or more threats. The actions and consequences that may arise are determined by the vulnerabilities present. ISO/IEC 27005:2008 categorizes vulnerabilities based on the type of asset they impact.

Based on this definition, organizations that hold information should recognize that their human resources are also susceptible to risks, even if those employees have no malicious intent. Social engineering is a relatively recent method utilized to expose information to danger. Instead of employing technical cracking techniques or breaking into systems, social engineers employ psychological tactics to deceive targets into performing certain actions or disclosing sensitive information (Workman, Bommer and Straub, 2008). By utilizing this method, subsequent actions and attacks appear less challenging to accomplish and more difficult to trace.

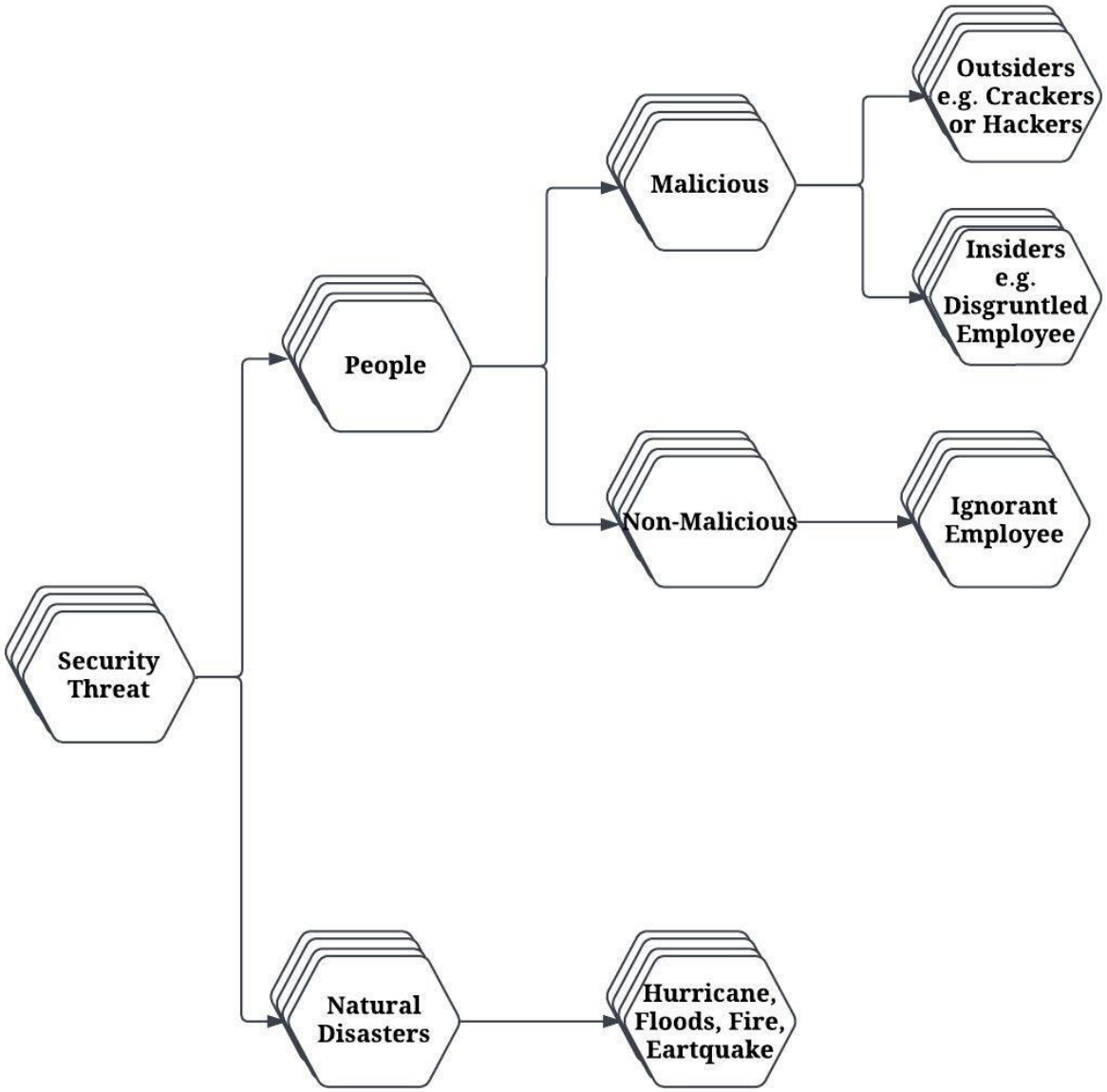


Figure 2.2: Sources of Security Threats

2.2.3.3 Threats (Action) – Implications (Attack)

The consequences of malicious, non-malicious, and physical threats manifest as actions that result in the disclosure, modification, loss, and destruction of data and information, as well as interruptions to their availability. These outcomes are depicted in Figure 2.3 as interception, modification, fabrication, and interruption (Pfleeger and Pfleeger, 2007; Stallings, 2007). Each of these is defined as follows:

- **Interruption:** This occurs when a data asset is lost, corrupted, or made inaccessible, aiming to disrupt its availability.
- **Interception**: Information is intercepted when an unauthorized third-party gains illegal access to it, resulting in a breach of privacy. The unauthorized party could be a human, a computer program, or another computer.
- **Modification**: When an unauthorized party gains access to an asset and makes changes to it, it is referred to as "modification." This represents a significant breach of trust or an attack on the integrity of information.
- **Fabrication:** Unauthorized parties introduce counterfeit items into the system, leading to a breach of authenticity.

Figure 2.3: Outcome of breaches

(Source: Stallings, 2007)

2.3 Systematic Literature Review

A thorough review of existing literature is a crucial component of any rigorous study. It is important to build upon established knowledge and gain insight into the current state of research in order to advance the boundaries of knowledge (Xiao and Watson, 2019). Conducting a review allows researchers to assess the breadth and depth of existing research, identify areas for further exploration, and test specific ideas, hypotheses, or develop new theories through the analysis and synthesis of relevant literature (Pare et al., 2015; Xiao and Watson, 2019). Additionally, reviewing existing work helps uncover any flaws, inconsistencies, or contradictions within the body of literature and ensures the reliability and accuracy of the study.

Systematic literature reviews (SLRs) employ a protocol as an action plan to ensure thorough planning, consistent execution, and transparent reporting. This methodologically sound approach allows for meticulous planning, minimizes bias, enhances transparency, and upholds ethical standards (Paul et al., 2021). Protocols for SLRs, such as the Preferred Reporting Items for Systematic Review and Meta-Analysis Protocols (PRISMA-P) developed by Moher et al. (2009), provide a comprehensive

framework for structured and rigorous reporting of reviews. However, these protocols lack specific guidance for researchers to justify their review decisions.

In response to this limitation, Paul et al. (2021) have introduced an alternative protocol called the Scientific Procedures and Rationales for Systematic Literature Reviews (SPAR-4-SLR). This protocol is specifically designed for SLRs and offers a more detailed structure with three stages and six sub-stages (Figure 2.4). It provides researchers with a systematic approach and rationales to support their review process, thereby enhancing the rigor and transparency of SLRs.

To comprehensively understand threat identification in the supply chain and the theories used in information security research within the supply chain context, a systematic literature review was conducted following the protocol outlined by Paul et al. (2021). The study followed the steps detailed in Figure 2.4 of the protocol, ensuring a structured approach for conducting the systematic literature review.

2.3.1 Protocol of the Systematic Literature Review

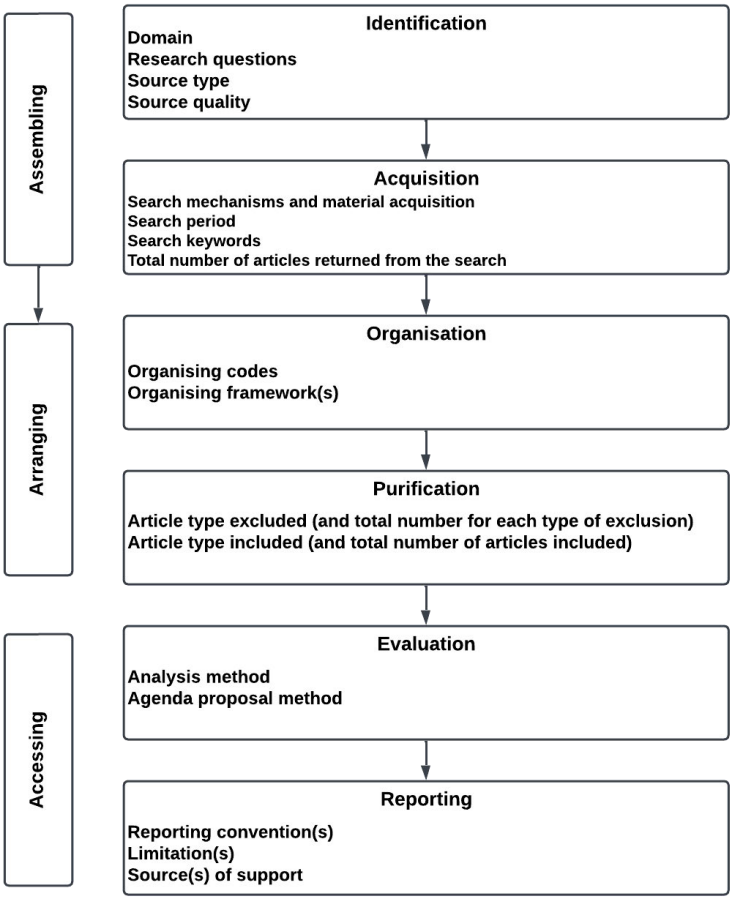


Figure 2.4: Systematic literature review protocol

(Adapted from Paul et al, 2021)

❖ **Identification**

This process involves delineating the scope and selecting a specific domain, such as information systems, information security, supply chain, supply chain security and identifying relevant outlets, such as the International Journal of Information Systems, Computers, and Security. The chosen topic,

"Evaluating information security threats in the supply chain: Human factor," will be the primary focus of the study.

- Research questions

How do the supply chain employees mitigate information security threats in the supply chain?

[RQ1] What factors influence employees' information security behaviour in an organisation of supply chain?

[RQ2] What factors mitigate information security threats in the supply chain?

- **Source type (**Define inclusion and exclusion**)**

  In this study, inclusion and exclusion criteria were established to determine the sources that would be considered. Academic sources, particularly academic journals, were given preference due to their contributions to scholarly progress and rigorous peer review processes. Other academic sources, such as book chapters, theses, and dissertations, were considered to a lesser extent. This decision was based on the belief that these sources are less likely to make significant scholarly contributions and often serve to showcase research capabilities rather than novel findings. Non-academic sources, including market reports, news articles, and white or working papers, were excluded as they do not formally constitute part of the scholarly literature.

- Source quality

  Academic journals offer different quality lists that can assist in identifying suitable journals for article review. Web of Science (WOS) and Scopus are widely recognized quality lists that encompass multiple disciplines. Scopus was preferred in this study due to its wider coverage of subject areas and categories compared to WOS. This broader scope enables researchers to more effectively locate journals that are relevant to their specific study area.

- Acquisition

  Search Mechanism and materials acquisition

  Coventry University subscribes to a range of databases and platforms, including Academic Search Complete, Business Source Complete, Google Scholar, ProQuest, Emerald Insight, Elsevier (Science Direct), IEEE, Taylor & Francis, Scopus, SAGE journals, Springer Link, and Wiley online library. These resources provide access to a wide variety of academic literature and research materials for the university community.

- Search period

  Studies published in the last 12 years between January 2010 and June 2022.

- Search keywords

  The search string was conducted by using a wide variety of various combinations of the categories of keywords given: (supply chain, supply network, threat, risk), (information, data), (information security threats and collaboration, cyber security), and (information security threats and supply chain cyber security) (information technology, human factor). For instance, consider the following search string: (“information, safety" OR "information security danger" OR "information flow" OR "information collaboration", information sharing) AND (information technology, information system).

- The total number of articles returned from the search.

1,859

❖ **Organisation**

Organising code and framework

This refers to the code book the researchers rely upon to code and record each article returned from the search. The code book used was excel document indicate the year, title, article type, method, conceptual and countries because the research will be carried out in a developing country.

❖ **Purification**

The author assessed of the general quality of the discovered research in relation to our inclusion and exclusion criteria and looked at only papers with significant data about information security detailing their theories and supply chain.

Article type excluded based on duplicate (N=250), based on tittle and abstract (N=154) inclusion (N=35)

Article type of included based on record screen **(N=**350), based on structure literature search (N=96), based

on assesses for eligibility (N=157), based on the research method(N=90)

❖ **Evaluation**

In cases where duplicate reports from the same research are identified, the most recent and complete report is selected for evaluation of the research methodology. This approach is adopted to ensure the rigor of the study, including factors such as trustworthiness, reliability, and validity, which are crucial considerations in both qualitative and quantitative empirical studies.

❖ **Reporting**

The systematic literature review yielded numerous general business threats and specific supply chain threats. However, it was observed that previous studies tended to focus on a limited number of possibilities. While multiple criteria were mentioned, several examples were found to be repetitive, overlapping, or expressed using different terminology to convey the same concept. As a result, duplicated risks were removed, and overlapping threats were synthesized, resulting in the identification of 12 general threats and 12 supply chain threats for this study. These threats, along with the relevant theories, are summarized in Table 2.2, Table 2.3, Table 2.6 in the subsequent section.

2.3.2 Identification of General Threats

- **The Stuxnet:** virus was detected when it caused data corruption on Siemens PLC (Programmable Logic Controller) devices. It has the ability to infect USB devices and exploit Siemens SCADA control software installed on Windows systems infected with malware (Urciuoli et al., 2013).

- **The Duqu:** This malicious computer program is designed to steal information from compromised systems. Experts have determined that it shares the same code base as Stuxnet, suggesting a close relationship between the two. The creators of the virus are believed to be the same individuals. Unlike Stuxnet, Duqu does not specifically target Siemens PLC equipment but instead gathers information that can be used to attack various industrial or computer devices. Duqu is known for launching destructive attacks, erasing data, and stealing information (Urciuoli et al., 2013)

- **Flame:** This recently discovered computer worm has infected numerous systems. Experts consider Flame to be potentially more sophisticated than Stuxnet and suspect it was intentionally aimed at Iran, leading to allegations of involvement by the United States and Israel (Urciuoli et al., 2013).
- **Inbound and Outbound Supply Threats**: Organizations establish connections with third-party companies, manufacturers, and distributors through their inbound and outbound supply chains to achieve their objectives. In the context of the Cyber Supply Chain (CSC) system, incoming suppliers, including external providers of electric power transfers, have remote access. A potential risk arises when threat actors breach the incoming provider's system, allowing them to manipulate companies involved in selling electronic items and payment services by falsifying data. Another vulnerability lies in the delivery process, where third-party vendors provide customers with electricity purchased from the utility provider. During this delivery, threat actors may exploit vulnerabilities through injection attacks or the introduction of malware, leading to a misconfigured supply chain system (Yeboah-Ofori and Islam, 2019).
- **Trojan horse**: Trojan horse attacks enable terrorists and criminals to take control of a system and disable security measures or interfere with critical logistical services such as air traffic control systems (Urciuoli et al., 2013). PUAs (Potentially Unwanted Applications) include malicious browser plugins, Trojan horse droppers and loaders, and similar programs (Singh et al., 2010). Trojans are malicious programs that appear harmless or attractive but are designed to steal or destroy computer data, according to Safa et al. (2017).
- Spyware: commonly known as "spyware," is frequently perceived as a risky form of online advertising software. Spyware vendors market their products as useful tools that users can utilize as long as they adhere to the terms of their end-user license agreements. Spyware is a

type of computer software that operates covertly, monitoring and logging a user's online activities without their knowledge or consent. According to Singh et al. (2010), spyware can be categorized into three main types: adware, system monitors, and Trojans, as outlined by Lamba et al. (2017). Spyware poses multiple risks to system security, including the theft of user and business data, alteration of security device settings, installation of additional software, and granting third-party access. Moreover, it has the capability to remotely execute arbitrary code, providing hackers with complete control over the affected device. Furthermore, the installation of potentially unwanted applications like spyware or adware can increase the likelihood of malware infections (Singh et al., 2010). Most advertising software for the internet is called "spyware", and this kind of software is seen as something that might not be safe. The vendor of Spyware sells their products as natural resources that, as long as end-user licence agreements are followed, are good for everyone who uses them and offer a variety of benefits to anyone who uses them. Spyware is a type of software that watches and keeps track of what a computer user does without them knowing. Most of the time, it is placed on the computer without the user's knowledge and behind their back (Singh et al., 2010).

- **Spyware business email compromise:** Businesses' email systems can be compromised, which is not as severe as ransomware but provides attackers with more options. This deceptive form of attack utilizes social engineering to target the finance department of a business, often using fake information from other employees, to initiate bank transfers (Singh et al., 2010). Attackers typically conduct research on the company's structure and personnel before attempting to exploit vulnerabilities. They may impersonate high-level executives to persuade employees to make non-cash payments to the attackers' bank accounts. Business email compromise messages are often difficult to detect since they lack harmful or suspicious links and employ innovative methods to access information assets (Safa et al., 2017).
- **Intentional or direct threats**: Deliberate or direct threats include sabotage, theft, information extortion, and political or economic espionage (Crossler et al., 2013). These threats pose risks to information assets.
- **Unintentional or indirect threats:** Accidental or indirect threats encompass actions like weak password selection, accessing non-work-related websites, or inadvertently clicking on phishing links in emails (Crossler et al., 2013).
- **Computer hackers:** Hackers can be nation-state actors, terrorists, cyber criminals, disgruntled employees, amateurs, script kiddies, malicious hackers, or legitimate vulnerability scanners. Identifying hackers and their activities can be challenging as they operate covertly and exploit networks to harm individuals or organizations through techniques like phishing and hacking (Crossler et al., 2013**).**

- **Malicious insiders:** Malicious insiders refer to individuals within an organization who have authorized access to systems and data but use that access for personal or financial gain to sabotage the system or steal information (Evan, 2019).
- **External intruders:** External intruders are unauthorized users of a system or network, and social engineering techniques may be employed to gain access (Evan, 2019).

- **Physical threat:** The physical dimension includes various information and communications technology (ICT) devices such as switches, servers, and routers. While the focus is often on cybersecurity concerns, the physical dimension also encompasses biological and environmental threats. Natural disasters like floods or tornadoes can disrupt servers and impede the digital supply chain network. Additionally, intentional destruction or theft of physical infrastructure components and terrorist acts are considered physical risks in the context of cyber threats (Sutduean eta l., 2019; Urciuoli and Hintsa, 2017; Tran et al., 2016; Cayetano et al., 2018).

Table 2.2: General Threats

S/N	Threat	Description	Source
1	Stuxnet	The virus spreads through the infection of USB devices and directly attacks the Siemens SCADA (Supervisory Control and Data Acquisition).	Urciuoli et al. (2013)
2	Duqu	The purpose of the Duqu computer worm is to steal information from compromised machines.	Urciuoli et al. (2013)
3	Flame	There is a new worm called flame that has infected a large number of PCs.	Urciuoli et al. (2013)
4	Inbound and Outbound supply threats	The threat actor might compromise the incoming supplier's network, alter data, and switch electronic product and payment service providers. Third-party vendors, rather than the utility itself, purchase customers' power loads and resell them at a profit. The external supply environment refers to the business that sells electricity to homes, businesses and other organisations.	Yeboah-Ofori and Islam (2019)
5	Trojan horse	In a Trojan horse assault, terrorists and criminals may seize control of a network and use it to shut down security systems.	Urciuoli et al. (2013) Singh et al. (2010)
6	Spyware	Spyware suppliers portray their wares as reliable, helpful tools when used under the terms of their end-user licence agreements.	Singh et al. (2010)
7	Spyware business email compromise	In its most basic form, a campaign to compromise business email entails sending emails to financial department employees (often using fake data from other employees), who can fund through bank transfer.	Singh et al. (2010)
8	Intentional or direct threats	Are referring to deviant behaviour such as sabotage, theft, information extortion and industrial or political espionage.	Crossler et al. (2013) Safa et al. (2017)
9	Unintentional or indirect threat	Accidental or indirect hazards include choosing a password, visiting non-work-related addresses, or negligently clicking on fraudulent links on email websites.	Crossler et al. (2013) Safa et al. (2017)
10	Computer hackers	These could be referred to as those who attack the organisation's information system infrastructures for various reasons and are considered state-sponsored hackers, terrorists, non-state hackers, or organised groups of dissatisfied workers.	Crossler et al. (2013)
11	Malicious insiders	Who may legitimately access the organisation's systems and data but use that access to destroy data or sabotage the system.	Evan (2019)
12	External Intruders	An unauthorised system or network user referred to as an external intruder.	Evan (2019)

.

2.4 Security Risk

A security risk refers to the potential for an information security threat to exploit a vulnerability and cause harm. When a threat exploits a vulnerability, it can lead to various risks such as loss of availability, integrity, and confidentiality. Being "at risk" means being susceptible to potential dangers. According to Pfleeger and Pfleeger (2007), security risk involves the possibility of loss and the likelihood of compromising an information asset. The literature highlights the close relationship between risk, threats, and vulnerability, as depicted in Figure 2.5.

The level of security needed for computer assets, including information, should correspond to their value, as emphasized by Pfleeger and Pfleeger (2007). They should be protected in proportion to their significance. Therefore, understanding and assessing the risk is crucial for safeguarding their value.

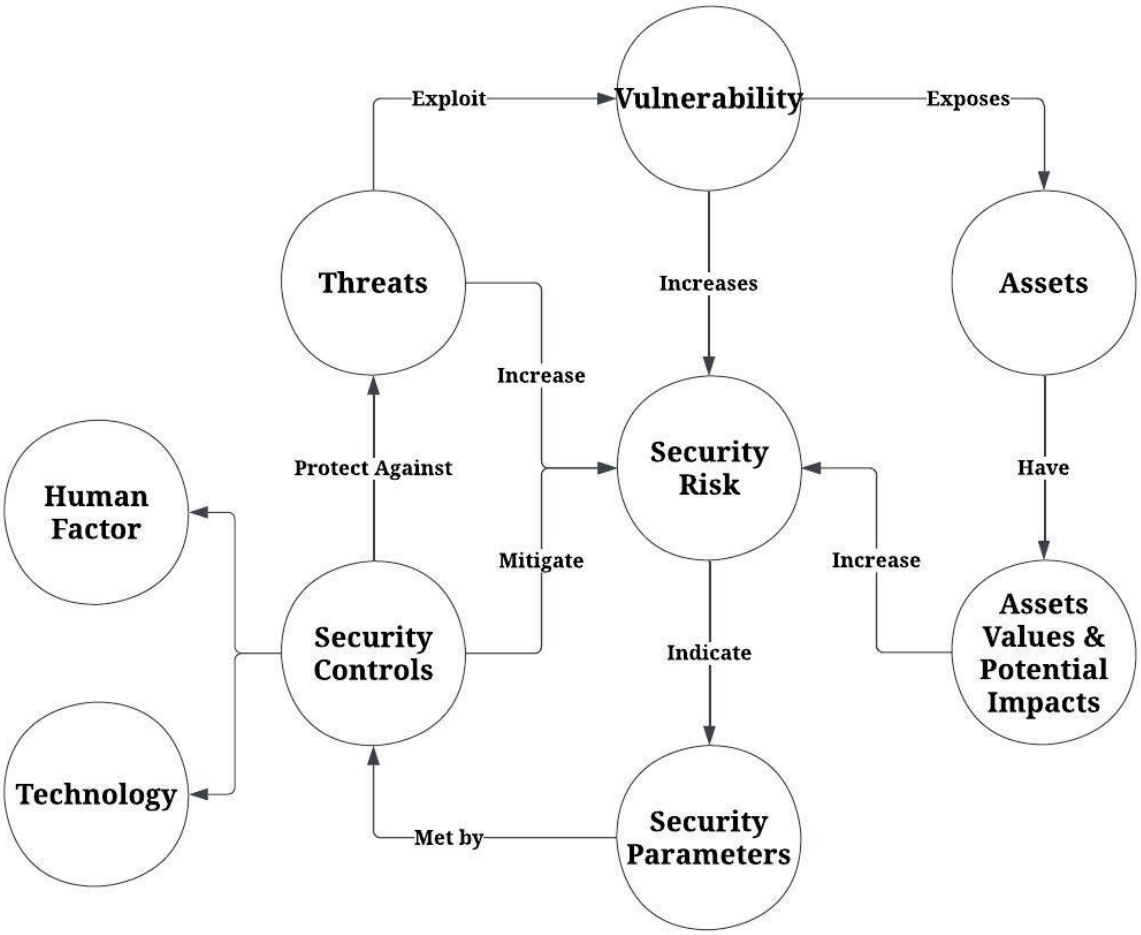


Figure 2.5: Threat Concept Relationship

2.4.1 Risk management

Risk management is a proactive process aimed at achieving favorable outcomes by incorporating flexible approaches to address any risk-related events (Borghesi and Gaudenzi, 2013). According to Borghesi and Gaudenzi (2013), it involves employing measures to protect IT assets from unauthorized access, misuse, manipulation, loss, modification, and unintentional disclosure of data and information contained within these assets. Risk management entails identifying vulnerabilities and threats to an organization's information resources that are essential for achieving business objectives. Based on the value of the information resource to the organization, it involves determining appropriate countermeasures, if necessary, to mitigate risk to an acceptable level. Risk management methods

encompass policy options with varying impacts on risk, such as reducing, eliminating, or redistributing risk. The ultimate goal is to assist businesses in effectively managing mission risks associated with information technology. Proper coordination of risk management maximizes the likelihood of achieving organizational objectives (Borghesi and Gaudenzi 2013).

In this study, the definition by Gjerdrum and Peter (2011) is adopted, which describes risk management as a process aimed at achieving organizational objectives. It is supported by a set of principles and facilitated by a structure/framework that enhances awareness to identify and address threats and emerging risks throughout the organization. This is achieved by improving controls, operational efficiency, and effectiveness (Gjerdrum and Peter, 2011). The overarching objective remains assisting businesses in effectively managing mission risks associated with information technology. Risk analysis commonly serves as an integral component of risk management.

2.5 Summary of information security

The purpose of information security is to prevent unauthorised access to, modification of, disruption of and interception of data. The primary cause of information security incidents is intentional or unintentional disruptions of business operations. There are several safeguards available to maintain operations and limit damage. ISO/IEC 27000, ISO/IEC 27001, and ISO/IEC 27002 are three of the standards provided by ISM for managing information security. Policy, training and education are all laid out in detail to help users develop a more secure habit. The problem is that the standard has been written and executed in a manner that makes compliance mandatory for users, without taking into account individual variances in how people think and act. It is possible that factors like job function, the organisation's objective and employees' own values all have a role in how people see and approach security because the main source and the cause of threats is human.

The next section provides an overview of the supply chain concept and information security threats in the supply chain.

2.6 Supply chain

Every company, regardless of its nature of business, relies on supply chains because no single organization can provide all the necessary resources, skills, and expertise (Handfield and Nichols, 1999). Businesses often choose to focus on their strengths and outsource their weaknesses to specialists, leading to diversification that addresses weaknesses and leverages strengths (Fawcett et al., 2007a). This diversification creates a market where supply and demand are balanced.

The term "supply chain" refers to the interconnected network of businesses, individuals, and organizations involved in transferring a product or service from the provider to the end user. This

network includes tasks, information, and materials required to transform natural resources, raw materials, and components into various products (Kenny, 2018). Ultimately, the finished product is made available for purchase by the end consumer. The value chain, on the other hand, refers to the network of organizations involved in generating value through processes and activities, both upstream and downstream, to deliver goods and services to the final customer (Kenny, 2018).

Managing supply chains is challenging due to the presence of multiple actors with distinct and sometimes conflicting objectives (Kumar and Luthra, 2018). Each link in the chain may try to achieve its own objectives, which can sometimes conflict with the overall objectives of the entire chain. Poor behavior or decisions at any point in the chain can impact the efficiency of the entire network, as each link's choices affect others (Li and Xu, 2021). To succeed in today's interconnected business environment, companies often form partnerships to pool resources and expertise (Li and Xu, 2021), making supply chain collaboration essential. Despite this, Behavioral Supply Chain Management (BSCM) is considered a niche within the broader SCM field, even though human behavior plays a role in nearly all supply chain situations (Schorsch et al., 2017)

2.6.1 Supply Chain Collaboration

According to Ralston et al. (2017), the original purpose of supply chain (SC) collaboration was to foster a relationship-based synergy by leveraging the experience and creativity of different firms for the benefit of all parties involved. Collaboration among supply chain enterprises, including procurement, production, and logistics, is crucial for enhancing supply chain efficiency. Ralston et al. (2017) argue that companies working together share information, plan, and cooperate to achieve their common goals. By collaborating, supply chain members can anticipate consumer needs, develop effective strategies to meet those needs, and coordinate their efforts for optimal efficiency (Hudnurkar et al., 2014).

The literature suggests that increased collaboration can lead to significant cost savings, with supply chain costs potentially reduced by up to 12 percent. However, the benefits of collaboration extend beyond cost savings (Cui et al., 2022; Zhao and Wang,2011; Raweewan and Ferrell, 2018; Li, 2021; Maskey et al., 2013). Ashayeri and Kampstra (2015) argue that cooperation is a crucial factor in enhancing supply chain performance, offering advantages in terms of finances and competitive positioning. Several researchers have attempted to identify different levels of integration and the circumstances that facilitate cooperation to guide collaborative efforts (Maskey et al.,2013).

However, with technological advancements, there are now opportunities to integrate the continuous flow of information. Information technology (IT) plays a vital role in enabling collaboration among businesses in the supply chain (Barron et al., 2016; Tseng et al., 2011). Gunasegaram and Kobu (2007) argue that in today's business environment, it is challenging to establish an efficient, competitive, and collaborative supply chain without leveraging information technology. Barratt (2004) suggests that

collaboration initiates information exchange-based connections not only at operational levels but also at tactical and strategic levels, paving the way for long-term partnerships between businesses.

2.6.2 Supply Chain and information sharing

Efficient communication systems based on information exchange, mutual benefits, incentives, and risk sharing are recognized as a crucial foundation for collaboration among supply chain enterprises (Ralston et al., 2017; Barratt, 2004; Weingarten et al., 2010). The importance of information sharing as a strategic asset in supply chain management (SCM) was acknowledged in the 1980s (Handfield and Nichols, 2016). Sharing information acts as the "glue" that sustains collaboration among supply chain partners over time (Fawcett et al., 2007). Cui et al. (2022) emphasize that information sharing can contribute to organizational performance, learning, creativity, adaptability, and awareness of company goals. Managing information involves the distribution of data among stakeholders.

The flow of information plays a vital role in determining productivity and overall supply chain output (Thomas et al., 2013). Open communication and collaboration have long been recognized as beneficial for supply chains, as they reduce uncertainty, improve integration and coordination of processes (Tang and Musa, 2014; Mentzer et al., 2000). Partial information sharing mitigates the bullwhip effect, reduces costs, and enhances trust among supply chain partners (Baihaqi and Sohal, 2013; Zhang and Wang, 2011; Ye et al., 2022; Yigitbasioglu, 2010; Sahin and Robinson, 2002). Supply chain approaches like Quick Response (QR), Efficient Consumer Response (ECR), Vendor Managed Inventory (VMI), and Continuous Replenishment Programmes (CRP) are built on the foundation of data sharing among supply chain members (Sahin and Robinson, 2002). Sharing relevant data, including inventory, sales information, order data, projections, production and delivery dates, key performance indicators, and capacity, is essential for accurate planning, forecasting, and stocking (Mentzer et al., 2000).

Establishing and maintaining loyal relationships with commercial partners is crucial for obtaining reliable information that supports decision-making (Colicchia et al., 2019; Gunasekaran et al., 2007). Controlled sharing of corporate data leads to a more connected and coordinated supply chain, providing a competitive advantage (Sai, Sharma and Routroy, 2016; Barratt, 2004). Information serves as the basis for managerial decisions and is a pillar supporting a robust supply chain (Sai, Sharma and Routroy, 2016). Delays, scarcity, breaches, disruptions, or distorted information can result in severe issues such as reputation loss, reduced competitive advantage, productivity decline, intellectual property loss, and financial costs (Colicchia et al., 2019; Gunasekaran etal., 2007; Sindhuja,2022).

Information is vital for supply chain coordination, integration, flexibility, cost savings, and coordination of supply chain flows (Chopra and Meindl, 2003). Companies like Dell, Wal-Mart, Proctor & Gamble, Cisco, Dillard's, JC Penney, and Lucent Technologies have implemented information-sharing practices to connect various parts of their supply chain networks and enhance productivity (Chopra and Meindl, 2003; Sai, Sharma and Routroy, 2015). However, the rapid advancements in information technology

and information communication technology, along with reduced barriers to entry and trading, have exposed supply chain partners to various threats (Sai, Sharma and Routroy, 2016).

2.6.3 Challenges of information sharing in the supply chain

The willingness to share commercially sensitive information with trade partners is crucial for ensuring customer satisfaction and reducing overall supply chain expenses (Ye et al., 2022; Yigitbasioglu, 2010) . However, the exchange of information can potentially affect supply chain efficiency, and there is a need for further research to understand the risks associated with information sharing across supply chains (Wang et al., 2022; Williams et al.2019). Therefore, both academics and supply chain managers are interested in identifying critical factors for effective information exchange among different nodes in the supply chain (Kembro and Näslund, 2014)

Despite the potential benefits, organizations often hesitate to disclose complete or accurate data due to concerns about data transmission reliability, security issues, and adverse competitive consequences (Kembro and Näslund, 2014; Baihaqi and Sohal, 2013). Information sharing exposes supply chains to various risks known as information threats, which have become significant business risks, including malicious attacks from viruses, worms, and hackers (Ramesh,2014).

Poor data quality or a lack of shared information can lead to operational issues and costly consequences for all parties involved in the supply chain (McFadden and Arnold, 2010). The data sharing process itself is fraught with ICT-related dangers that can have far-reaching effects on business operations (Sodhi and Tang 2012). The confidence of trade partners in the security of a company's supply chain management systems is a critical factor in their willingness and ability to share sensitive information (McFadden and Arnold, 2010). Risks in the digital supply chain arise from authorized disclosure and leakage of information, including commercial, personal, and proprietary data, with difficulties in tracking access and usage (Ramesh,2014)

Several authors in the literature have called for more scrutiny and emphasis on information security in supply chain information sharing (Colicchia et al., 2019; Safa et al., 2017). While the benefits of supply chain information sharing are often praised, there is a need to acknowledge and address the associated pitfalls. Greater attention must be given to information security, as collaborative efforts in supply chains involve the sharing of sensitive information (Bhargava et al., 2013).

2.6.4 Information Security in supply chain

Information security plays a crucial role in the supply chain, as it is vital for ensuring the safety of a company's operations. The reputation and value of an organization depend on its ability to protect its data and resources (Alhogail and Mirza, 2014). Information security encompasses maintaining the confidentiality, availability, and integrity of technology, processes, and people (Von and Niekerk, 2013). In the context of the supply chain, information security refers to the protection of critical data

and systems shared among various parties involved in the supply chain process. This includes ensuring the confidentiality, integrity, and accessibility of sensitive data, as well as preventing cyberattacks and intellectual property theft. Ashenden (2008) emphasize the significance of cybersecurity in the supply chain and identify associated challenges and opportunities. They highlight the need for a comprehensive cybersecurity strategy that includes risk assessment, threat intelligence, incident response, and continuous monitoring. The article also addresses various cybersecurity risks that supply chains must confront, such as insider threats, external attacks, and disruptions in the supply chain. It provides recommendations for mitigating these risks, such as implementing access controls, encrypting data, and establishing supply chain resilience.

The supply chain environment differs significantly from within a single organization, primarily due to the collaboration and information exchange required to enhance productivity and integration. However, increasing the flow of information within the supply chain also increases the risk of information leakage, as noted by (Safa et al. 2017).

2.7 Information Security Threats in Supply Chain (ISTSC)

The purpose of this section is to provide insights into the topic of Information Security Threats in the Supply Chain (ISTSC) and examine relevant theories from the fields of criminology and behavioural sciences. It is crucial to recognize that security risks within the supply chain are not random events, but deliberate actions carried out by criminals, whether they are insiders or external actors (Williams et al., 2019). Effectively managing information security threats throughout the supply chain is an essential aspect of supply chain management. ISO 27001, as highlighted by Pahnila et al. (2007), emphasizes the need to identify potential threats to systems and assets, which can be accomplished through a comprehensive threat database. Various databases exist that compile information on data security breaches reported by different organizations through questionnaires. For instance, the Information Security Breach Survey (ISBS) 2020, conducted by PricewaterhouseCoopers in collaboration with Info security Europe under the guidance of the Department for Business Innovation and Skills (BIS), revealed that numerous organizations had encountered security breaches. These breaches included incidents such as computer theft or fraud, internal employee-related issues, unauthorized access attempts (including hacking), and targeted attacks on goods within the supply chain (Urcuioli et al., 2013; Peterson, 2014).

Several factors contribute to information security problems within organizations, including insufficient employee training on information security, low employee awareness of information security, and ineffective team management. These factors pose significant risks to an organization's information security, as the systems responsible for storing, processing, and transporting information may be vulnerable. Therefore, it is crucial for individuals responsible for protecting information within the supply chain to first identify potential threats and then assess the vulnerabilities present in those

systems. The initial step in this strategy involves identifying the most significant threats to organizational information security and prioritizing them accordingly. To gain a better understanding of the threats faced by the supply chain, this thesis aims to determine the severity of threats within the supply chain. In the next section, the identified threats in the supply chain will be explained (Safa et al., 2017).

Sai, Sharma and Routroy (2016) categorized threats into three types: internal, external, and platform-based, based on their origin. They emphasize that internal security threats to an organization can arise from intentional or accidental violations of company policies by employees and other members of the organization. External threats, on the other hand, come from individuals who have no affiliation or employment with the company. Brown (2015) add that security risks can manifest as worms, viruses, or attacks from malicious software. Other possibilities include software capable of sniffing or cracking passwords, spoofing attacks (such as IP spoofing or web spoofing), denial-of-service attacks (such as email bomb attacks), or direct attacks (hacking) (Mamonov and Benbunan-Fich, 2018; Sai, Sharma and Routroy, 2016). Peterson, (2014) notes that the third type of incident is platform-based and originates from service providers. Examples of platform-based incidents include policy violations, physical damage or theft of resources, system failures, or data corruptions caused by improper resource management or excessive use of computational resources. Additionally, theft of company security regulations or personally committing security theft are considered information security threats (Safa et al., 2017).

Various factors contribute to these problems, such as inadequate employee information security training, lack of awareness among employees about information security, and poorly managed teams. These elements pose significant risks to an organization's information security. The systems responsible for storing, processing, and transporting information may be vulnerable to these issues, so it is essential for those responsible for information protection in the supply chain to identify potential threats and vulnerabilities. The first step in this strategy is to identify the most significant threats to organizational information security and prioritize them. This thesis aims to better understand the threats faced by the supply chain by assessing the severity of these threats. The following section will identify and explain the threats in the supply chain (Safa et al., 2017).

2.7.1 Identification of threats in the supply chain

- **Technical threats:** Technical hazards primarily affect the software supply chain at the hardware, operating system, and application layers of the system. A comprehensive list of technical dangers has been compiled. An example of a hardware danger is unauthorized individuals damaging outsourced software components by attacking a storage facility through the storage device or logical partitions. If the operating system of a software vendor is compromised, unauthorized individuals could inject harmful code into the open-source tool through the network, resulting in security flaws.

Another example is hackers infiltrating a software repository to obtain confidential information about an outsourced software component, such as a hard-coded key (Hassija et al., 2020; Xiong and Lagerstorm, 2019; Al Sabbagh and Kowalski, 2015).

- **Social threats:** Social threats can arise from intentional or unintentional human errors or behaviours. For instance, a provider might deny sending a software product, or non-technical issues in software delivery, such as quality control problems, could cause delays. Internal personnel may inadvertently or intentionally disclose confidential information about outsourced software components due to factors like bribery. Non-technical methods like spoofing can also allow unauthorized parties to access secret information. At various levels in the supply chain, social threats exist, with the majority occurring at the operational level (McEvoy and Kowalski, 2019; Rajanen and Rajanen et al., 2019; Al Sabbagh and Kowalski, 2015). Additionally, societal threats can arise when employees or unauthorized individuals destroy or insert malicious code into software source code or installation packages. Furthermore, accidental release of sensitive information during interactions with colleagues or outsiders can occur (Kunnathur, 2015).
- **Password sniffing/cracking software:** Password sniffing/cracking software: Password sniffing/cracking software, such as Brute (PC), Passfinder (Mac), and Crack V4.1 (Unix-based), represents a common and straightforward attack technique. An employee may use such software to attempt different passwords until they find a working one. Commercial password cracking services are also available. Hackers utilize these software or services to steal passwords, gain unauthorized access to systems, or obtain data for later use (Pad and Singh, 2019; Sai, Sharma and Routroy, 2016)

- **Direct and indirect attacks:** Direct and indirect attacks: Direct and indirect attack threats involve planned assaults. Examples of direct attacks include DDoS attacks, hacking, cybercrime, and password sniffing for financial gain. Industrial espionage, intellectual property compromises, computer system hacking, information rewriting, and theft fall into this category as well. Hackers target online service providers as they can quickly modify, degrade, or destroy these services. Direct attacks may go unnoticed unless the targeted organization identifies them. In more subtle attacks, hackers use deception to trick victims into providing sensitive information or login credentials. Fake goods, software, and hardware, as well as spoofing attacks, are also employed (Deane et al., 2009; Khursheed et al., 2016; Sharma and Routroy, 2016; Boone, 2017).
- **Malicious tampering:** Globalization in the IT sector has opened the door to incidents of poisoned items targeting the supply chain. Attackers can easily access critical data through less-protected third-party providers and suppliers. They may use breached vendors' access as a gateway to their ultimate target (Singh et al., 2019).

- **The insider threat**: Furthermore, firms must be aware of the potential of accidentally releasing sensitive information while conversing with colleagues or outsiders (Kunnathur, 2015). Employees actively abusing or sabotaging a company's data are also reported in the literature concerning these acts of thoughtlessness. For example, a calculated personal vendetta against an employer or opportunistic abuse of confidential information (Sai, Sharma and Routroy, 2016). An insider threat exists because the staff cyber threat is internal, whether deliberate or unintentional. Reporting on maliciously motivated, purposefully carried out cyber-attacks, Urciuoli (2010) believes these should not be permitted to overshadow cyber supply hazards caused by negligent employees (Urciuoli et al., 2013; Urciuoli et al., 2017). The human component can offer the largest and most unforeseeable threat to a company's information security in both the negligent and deliberate modes. Employees could serve as insiders, assisting criminals in their operations, or they could commit a crime independently, given their proximity to facilities or goods (Urciuoli, 2010).
- **Trojan with a supply chain**: Currently, the protection offered to integrated circuits and the integrity of the supply chain are at risk. When malicious hardware modifications are made to ASICs, COTS components, microprocessors, microcontrollers, network processors, digital signal processors and Internet of Things devices, they are known as hardware Trojans (HTs). HTs have become a serious security issue for ICs in abundant previously secure situations, including the military, healthcare, aviation, communications, power management and general critical infrastructures. Most Trojans may be digitally activated, and their activation can be sequential or combinational, depending on their trigger mechanism. Connecting sequential Trojans to the original circuit's core clocks or finite state machines (FSM) is a common practice (Jiaji He et al., 2015).

- **External threats:** Substantially originate in the external environment in which the organisation operates. Network security communication and human threats like hacker software and legal risks are all possibilities. Physical hazards and socioeconomic dangers particular to the nation include the country's existing social and economic situations. Individuals are increasingly using social engineering websites to gather information and impersonate others to trick them into giving over sensitive data or login credentials. The theft of sensitive data, trade secrets or intellectual property also raises serious problems. In the end, some of these physical or legal dangers may put an entire business at risk. On the other hand, other risks may only affect a portion of an organisation or be overcome rapidly for a limited time. Cybercrime exposes organisations to legal dangers (Rao et al., 2017).
- **Employee Negligence**: Information security is a top priority in today’s intensely competitive business environment; the firm thus enthrones information security protocols to protect the

information primarily, foreclose information theft, maintain corporate records; as well as monitor information security compliance and detect information system misuse (D'Arcy and Greene, 2014; D'Arcy et al., 2009). However, employees' negligence still poses a substantial information security threat to firms, perhaps more threatening than external agents. Employees are the weakest link in a firm's supply chain information security system (Bulgurcu *et al*., 2010; Warkentin and Willison, 2009). Studies show that information security breaches often arise from "unintentional behaviours and actions of employees who were negligent, careless or ignored security policies (Kaspersky Lab 2017). Organisational information security experts have consistently pointed to the behavioural tendencies of corporate members as a source of information security threats, insisting that often, security incidents occur from within organisations rather than from external actors (Zauwiyal et al., 2018; Crossler et al., 2013).

Security damaging behaviour, on the other hand, undermines the firm's information security and exposes them to unauthorised parties. Security negative behaviours are of immense concern to firms because they are overly harmful to corporate health. This kind of behaviour often arises from carelessness, ignorance or error. Ponemon (2017) found that most information security threats firms encounter results from negligent employees; and stated that information security breaches involving innocent employees' behaviours and actions are given less publicity, even though they are equally damaging as other sources of threats. The prevalence of negligent employees also implies that the most information security threats firms may encounter emanate from people who use programmed applications and not from the programmers and applications themselves.

Studies focused on human errors show that fatigue or distraction contributes to unintentional mistakes, while loss of vigilance causes intentional mistakes. Norman contends that humans will make errors even in the best-designed systems; hence, plans should be designed to minimise the effect of human error (Lahcen et al., 2020). Human errors are known to have caused damage in various industries. Human mistakes in aviation include lack of communication, complacency, knowledge, distraction, teamwork, weariness, lack of resources, pressure, assertiveness, stress and awareness. These factors can be at play even in the information security in supply chain context and can contribute to either information security assurance or information security damaging behaviours of employees.

- **Mismanagement of access to information:** Every information item belonging to a firm has value to another firm. A firm's sensitive information that gets into the hands of unauthorised actors may be used in ways that may disadvantage the firm. As Jouini et al. (2014) put it, modern technologies have increasingly exposed companies' information assets to many vulnerabilities and threats and their resultant damages Jouini et al. (2014) add that damages to

a firm's supply chain information security can range from small losses to entire information system destruction; affecting information availability, confidentiality and integrity (Cavusoglu et al., 2004), and orchestrating dire consequences on corporate liability, loss of credibility and monetary damage. These threats may emanate from employees' activities or malicious outsiders who may gain access to classified information through mismanaged access controls.

Supply chain information security can hardly be guaranteed without authentication and authorisation, just as access controls are among the first policies usually investigated in the event of any information security breach in a company's supply chain. Access control is required in today's hybrid business environment, where employees increasingly connect to the Internet to access company information. This is because solid access control is required for any information that could be valuable to any actor who does not have the authority to access it (Boiko et al., 2017). The report has been and will continue to be a valued resource and asset. Firms rely heavily on accurate and timely information to guide decision-making that enables competitiveness. Control of access to supply chain information is thus critical to organisations; and requires enforcing persistent policies in a dynamic world without traditional borders (Boiko et al., 2017). Management policies and practices are part of human factors within a firm's information security framework that predispose firms to information security threats.

- **Third-party breach:** Information breaches representing unauthorised movement or disclosure of sensitive information to unauthorised parties that do not have access to the information have become commonplace in today's business environment; individuals and organisations have been victims (Wang et al., 2019). Moreover, these breaches occur through third parties. Third parties include technology service providers, payroll services, accounting firms, invoicing and collection agencies, consulting firms, and design and manufacturing companies collaborating with a firm to deliver value to its customers. In today's corporate environment, it's nearly impossible to find a company that doesn't rely on third parties to support its operations; and most third-party commercial agreements necessitate information sharing and access to the enterprise network, systems and computer resources (Wang et al., 2019). Third-party information sharing is where the majority of third-party breaches occur. Indeed, the frequency of security breaches and incidents caused by third parties is rising.

- **Compromised IT systems:** Businesses increasingly resort to using information technology systems in routine operations (Schlienger and Teufel, 2003). In this regard, computers, computer networks, and often, the internet of things come to the rescue. However, along with the many benefits of using IT come some drawbacks. IT systems are vulnerable and susceptible

to several risks which could threaten the security of a firm's information assets. IT systems that earlier constitute essentials to a firm's competitiveness and sustainability become its albatross when compromised. A compromised IT system is one whose availability, confidentiality and integrity have been negatively affected by an untrusted source (Lim et al., 2009). IT systems compromise may occur through manual interaction by an untrusted source or via automation. Access to a firm's IT systems or network by impersonating a legitimate user or by forceful attack constitutes a compromise and exploits loopholes in an IT systems configuration (Stevens, 2018).

IT security, the protection of computer systems and networks from information disclosure, theft or damage to hardware, software or electronic data, as well as disruption or misdirection of services provided by a firm, has been a top priority for business operators (Stevens, 2018). Even the discourse on information security has shifted from exclusively IT experts' domain to an issue of deliberation among management scholars (Lim et al., 2009). Information security breaches often result from deliberate and opportunistic paths of compromise through the Internet, a firm's online presence and the firm's attractiveness for information security compromise (Lim et al., 2009). These constitute severe threats to a firm's supply chain information security.

- **Weak information security protocols:** Information security protocol describes the measures, plans and actions a firm institute to keep its information assets safe from attacks, breaches and other security incidents (Kaljahi, et al., 2015). Firms employ various protocols that work well together to keep their valued and sensitive information protected. Femi-Oyewole (2015) observed that employees often commit errors that expose the firm's information assets to threats; also, external agents with malicious intents make deliberate efforts to gain access to the firm's information systems, networks and sensitive information. Therefore, the firm must regularly update its information security protocols to keep them error-proof and impregnable to external attacks. Kennedy (2016) notes that while it is costly and involved to protect the firm's information assets, it is even costlier to leave them unprotected in today's business contexts where information is about the firm's most important asset. As advances in ICT allow firms to conduct business activities in cyberspace, a firm's valuable and sensitive information is exposed to threats. Hence, it is essential for firms to take appropriate measures to ensure the safety of their information assets and reputation (Femi-Oyewole, 2015). Typical information security protocols firms can put in place to protect their valued information include firewalls, encryption and education.

Mahieu et al. (2018) explain information protection is becoming an increasing concern and priority for private and corporate citizens in our contemporary world of rapid advancements in

digital technologies. Wu et al. (2015) add that to protect valued information assets from attacks, companies must establish protocols. The establishment of such protocols is made even more pertinent by the fact that employees are often the weakest links in the information security in supply chain (Akhyari et al., 2018) due to their security behaviour in dealing with information assets (Hu et al., 2012). Information security protocols thus influence employee's information security behaviour focused on minimising information security breaches (Vroom and Von Solms, 2004). To further understand threats in the SC, Sections 2.5.3 and 2.6 identify and explain information security threats in the supply chain solution both from technical and human factor perspective. Table 2.2 summaries the threats in the supply chain.

Table 2.3: Threats in the supply chain

S/N	Threats	Description	Category	Source
1	Technical threat	It affects the software supply chain.	Technology-related	Sabbagh and Kowalski (2015) Xiong and Lagerstorm (2019) Hassija et al. (2020)
2	Social threats	Can exist due to deliberate or unintentional human errors or behaviour.	Human-related	Sabbagh and Kowalski (2015) McEvoy and Kowalski (2019) Rajanen and Rajanen et al. (2019)
3	Password sniffing/cracking software	An employee may use this approach to try a variety of passwords until they find one that works.	Human-related	Sharma and Routroy (2016), Pandey and Singh (2019)
4	Direct attack and Indirect	This strategy involves destroying, modifying or extracting data from computer files, which is less obvious to organisations because they are unaware that they are victims of a direct attack. In indirect attacks, the attackers set up 'bait' to gain access to the target system. In a direct attack, the computer system is hacked, and the information is rewritten and stolen.	Human-related	Faisal et al. (2007) Sharma and Routroy (2016) Khursheed et al. (2016) Pandey and Singh (2019)
5	Trojan with supply chain	Hardware Trojans (HTs) are malicious hardware modifications to supply chain.	Technology-related	Jiaji He et al. (2015)
6	The insider threat	Insider risks are employees who work for a supply chain company.	Human-related	Evan (2011), Urciuoli et al. (2013) 7Urciuoli et al. (2017) S8afa et al. (2018)
7	External threats	Originate from outside the organisation.	Human-related	Rao et al. (2017)
9	Mismanagement of access to information	A company sensitive information gets into a wrong hand or unauthorised actors may use in way that will affect the reputation of the company.	Human-related	Jouini et al. (2014)

10	Third party supplier threat	These occur when unauthorised persons gain access to a firm company information system through outsider partner or service provider who has access to the information system.	Human-related	Wang et al. (2019)
11	Employee Negligence	Information security incidents are ascribable to careless or uninformed employee actions.	Human-related	Ponemon (2017) Zauwiyal et al. (2018).
12	Third-party breach	When unauthorised persons gain access to a firm's information system and assets through an outside partner or service provider who has access to the firm's information system and assets.	Human-related	Patterson (2017) Chickowski (2018).
13	Compromised IT systems	Is one whose availability, confidentiality and integrity has been negatively affected by an untrusted source	Human-related	Bendovschi (2015).
14	Weak information security protocols	Firms employ various protocols that work well together to keep their valued and sensitive information protected. Employees often commit errors that expose the firm's information assets to threats.	Technology-related	Femi-Oyewole. (2015) Akhyari et al. (2018)

2.7.2 Consequence of Information Security threats in the supply chain

Several elements must be considered while assessing the security of information exchange. Privacy, protecting private information and maintaining information quality are a few of these concerns. According to Wiengarten et al. (2010), the success of collaborative practices is directly proportional to the quality of the information that participants communicate. This includes the information's timeliness, accuracy, and relevance and add value. Rees et al. (2011) recognise two special damages that may follow directly from the incident when an organisation is attacked: harm to the company's reputation and fines levied by regulatory bodies. According to Olatunde (2014), attacks on information technology systems may result in three different consequences: a loss of integrity, a loss of availability and a loss of confidentiality. In addition, Safa et al. (2017) state that information security threats have serious consequence for companies, such as loss of revenue, reputation, customers, business advantages, and, in worst-case scenario, bankruptcy. The following section explain the consequences in detail.

2.7.3 Loss of reputation

An information security threats entails a sensitive or personal data about customers, its confidentiality is lost resulting in dire reputational risks for the companies. Torre et al. (2018) stated that reputational harm is the greatest effect of an information security threats for an organisation, as it influences brand name and reduces economic value. The most catastrophic threats to a company's reputation and brand name happen when business information and customer's data are stolen. Subsequently, customers appear to lose trust in both the organisation and its attempt to secure their data, thereby compromising the value of the organisation relational capital.

2.7.4 Competitive advantage

An information security threats may lead to the theft of organisational knowledge and intellectual property which are sources of competitive advantage. The organisation uses competitive intelligence to structure its strategic planning (Sinha, 2012), therefore, threats to information security greatly diminish the company's ability their competitive intelligence. Torre et al. (2018) revealed that corporate spying is a deliberate strategy to sabotage competitors, even a whole industry.

2.7.5 Productivity and intellectual property loss

Clare (2016) stated that in addition to sensitive and personal data breaches, other valuable data, like intellectual property, are exposed to the risk of cyber-espionage, unintentional exposure and insider threats. Firms aim at getting information related to intellectual property and trade secrets that can bring financial rewards, economic growth and market leadership. Theft of valuable trade information and intellectual property compromises an organisation's competitiveness and innovativeness and may cause dire repercussion for its long-term goal and competitive advantage (Torre et al., 2018).

2.7.6 Financial Cost

Information security threats are increasingly recurrent and affected companies are believed to incur a high financial cost, including the cost of giving a solution and dealing with potential legal repercussions, loss of consumer confidence, reputation, revenues and ultimately market share. Researchers discovered that the financial cost connected with information security threats negatively impacts shareholders' wealth (Kholekile L. et al., 2018). An information security threat can lead to several costs for an organisation. Though there are dissimilarities among industries and countries, around half of this cost is incurred due to indirect costs, which include loss of goodwill and customer agitation. The indirect financial cost indicates some of the financial losses incurred from information security breaches (Torre et al., 2018).

2.8 Control of Threats

Security controls are procedures used to decrease threats and attacks or other harmful events happening. Tipton and Krause (2007) classify controls used to protect data as either physical, technological or administrative. Access to a building, computer, equipment and the processing resource itself may be restricted using physical security methods like identification cards, locks and alarms. Technical security, also known as logical controls, is a layer of defence built into computers, operating systems, system monitors, firewall communication tools and other peripherals. Protection in a managerial setting may be achieved by administrative security. This comprises administrative controls, operational controls, accountability mechanisms and managerial restraints. You may further categorise these three types of controls as preventative.

The goal of preventative controls is to reduce the likelihood of undesirable occurrences, whereas the goal of detective controls is to discover such events after they have already taken place. Audit trails, intrusion detection systems and checksums are all examples of detective controls (Tipton and Krause, 2007). The usage of computers is often controlled by preventative safeguards. As a result, preventative measures need user interaction to get buy-in and be implemented in the workplace. Because of the importance of users being able to trust their computer systems, effective security awareness programmes may assist in enhancing users' tolerance for preventative measures (Tipton and Krause, 2007).

2.9 Information Security and the Human Factor

As previously discussed, information security has been traditionally defined as the "preservation of confidentiality, integrity and availability. The main goal of any IT infrastructure is to achieve this triad through information security implementations and management. Information security is usually associated with three important components: (a) Physical, (b) Technical and (c) Administrative. The administrative component involves policies, procedures and guidelines and mainly deals with how

technology is to be used securely by those who operate it. Literature reports that technology alone cannot protect information assets.

The range of physical and technological security measures has expanded greatly during the last 15 years. Additionally, there is ongoing innovation in the form of security-enhancing solutions. Information security dangers are more dangerous than ever because of our growing reliance on digital data. Given the abundance of security solutions, one may assume that obtaining an appropriate degree of security is straightforward and that security breaches are uncommon, if not non-existent. The reverse is true, unfortunately. The issue is that technology is built to function autonomously but is nonetheless controlled and used by humans (Schultz, 2005). The "human factor" is a term used in the field of information security.

Security is not something that could be done without human factors in an organisation, 'human' is always proven to be an important space to explore in relation to information security threats. Hence, human factors are, without a doubt, a critical point in information security. The technological solution for security seems to be sophisticated and stringent, humans are the first level of protection to secure information assets (Ngoqo and Flowerday, 2015; Lebek et al., 2014; Sindhuja, 2014; Chen et al., 2009). Information security dangers are more deadly than ever due to the rising reliance on electronic information (Chen et al., 2009). Ngoqo and Flowerday (2015) state that with the abundance of security solutions available, one would anticipate that attaining an acceptable level of security would be simple and that security breaches would be little or non-existent.

The issue is that although technology is made to function without people, people nonetheless manage and use it (Schultz, 2005). This refers to the concept of the "human factor" in information security. In section 2.6.1 of this thesis, threats were identified, and they were caused by employees such as technical threats, social threats, direct attacks and indirect attacks, insider threats, employee negligence and mismanagement of access to information, just to mention a few. Most organisations appear ready to face and prevent the threats, they are inadequately prepared for the threats that originate from within and without the organisation. The human factor is the weakest link in the information security chain (Hu et al., 2012; Alhogail et al., 2015).

Human factors play a significant role in computer. Kreamer et al. (2009) describe the potential connections between organisational and human factors and the technical weaknesses in computer and information security (CIS). They further state that people should be aware of the varied roles of human and organisational elements and CIS vulnerabilities, and that CIS vulnerabilities are not the sole outcome of a technology problem or programming mistake. Badie and Lashkari (2012) propose classifying the factors which affect computer security into two primary groups: human factor and organisation factor. They contend that an analysis of prior research demonstrates that the human component is more significant than the other factors. They also suggest splitting up the human

components into two categories: 1) factors that belong to management, namely workload and inadequate staffing, and 2) factors related to end user, namely lack of awareness, (risky) belief (risky), behaviour, and inadequate use of technology and lack of motivation. Currently, human activity is considered the most critical factor in the management of information security (Stewart and Jurjens, 2016).

It is commonly accepted that employees frequently represent a weak link in an organisation's information asset protection strategy. Researchers have urged greater research in this field since information security has not received enough attention in the literature about the human element effect. Information security is more than just a technological concern; it also involves humans. Using traditional technical systems is no longer sufficient, and conventional approaches should focus on technical fixes appropriate for today's dynamic nature of organisations (Norman and Yasin, 2010). Moreover, organisations should focus on staff behaviour, as the organisations' success or failure effectively depends on the things that its workers do or fail to do (Da Veiga and Eloff, 2010; AlHogail, 2015). Although researchers have studied how human behaviour affects information security, there is little information about how this knowledge is really applied, therefore, the subject needs greater attention.

Rao et al. (2014) and Evans et al. (2019) show human error is the root cause of fifty-one percent and eighty percent of reported information security incidents, respectively, since technology is designed and managed by people leaving opportunities for human error (Divakaran et al., 2008). Intentionally or through negligence, human behaviour is a huge risk to information assets (Safa et al., 2016). 'Human' is seen as the weakest link in the information security defence when investigating information security in supply chain settings (Hu et al., 2012; Alhogail et al., 2015). Studies have also shown that organisations routinely overlook human error as the primary cause of security breaches and focus on technical controls (Safa et al., 2016; Evans et al., 2018). Users, intentionally or through negligence, are an essential threat to information security, in which careless information security behaviour is the main issue. Information security is more than just a technological concern; it also involves humans. Using traditional technical systems is no longer sufficient, and conventional approaches should focus on technical fixes appropriate for today's dynamic nature of organisations (Norman and Yasin, 2010). Security controls frequently demand human engagement, which is critical in the information security process (Van et al., 2010). Employee behaviour, while interacting with information, can be influenced by human characteristics such as knowledge skills and personality. From an organisational perspective, Ashenden's study provided an in-depth insight into the human difficulties confronting the Information Security Department, tying all company areas to information security management.

Kearney (2010) contends that individuals may only contribute to the prevention of security breaches if they are made aware of the risks and are taught secure practices as part of their regular workplace

training. However, employee apathy is a typical barrier to the development of a setting where management and staff are working toward the same information security objectives (Thomson and Van Niekerk, 2012).

2.9.1 The Human Factors in Supply Chain Management

The human factor has a tremendous impact on the success and the failure of our efforts to secure and protect business, systems and information. Even though there is less empirical evidence that individuals in supply chains behave in ways that are counter to what theory predicts, many studies in supply chain management (SCM) use a positivist approach, emphasising theoretical solutions and best practices (Femi-Oyewole, F. (2015). Several studies back up the assertion that SCM research has usually missed the impact on human behaviour (Tokar, 2010; Schorsh and Marcus, 2016). Human and behavioural components (soft wiring) (Femi-Oyewole, F. (2015). play at least a critical role in supply chain management as hard facts of SCM, such as processes, technologies and measurement methods. Knowing the importance of people's behaviour in the supply chain environment requires understanding that individuals do not act solely rationally, that they care about others and that they are influenced by their cultural background. Schosch and Marcus (2016) relate to how crucial human behaviour is to supply chains. Any supply chain should focus on clearly managing the behavioural factor (Huo et al., 2015). However, behavioural SCM is still in its infancy (Donohue and Siemsen, 2011; Schorsh et al., 2016).

Researchers have recognised the value of the human factor in many SCM processes over time, which has a direct impact on productivity and organisational success (Strandhagen et al., 2017; Tokar, 2010). As SCM today is facing a fiercely competitive market, the role of the human factor is also becoming critical in the coordination phase, which requires information sharing, effective communication, partnering and performance monitoring.

There are many uncertainties around the human factor due to its variability in terms of physical, cognitive, perceptual and psychosocial components (Nilsson, 2006), making it the most crucial factor (Grosse et al., 2017). Human effort is still viewed as crucial despite technological advances (Jager et al., 2014; Mortal and Pennathur, 2004), and is frequently underestimated and rarely taken into consideration in many parts of SCM and organisational performance. Human challenges are found in the direction of human, social and organisational elements to ensure that the organisation maximises the benefit by integrating several different tools within the organisation, such as organisational structure, procedures and relationship management (Evans et al., 2019; Divakanran et al., 2008).

Welinger et al. (2009) took holistic approach to the organisational and technological difficulties that IT workers encounter in their firms. The following human obstacles to imposing restrictions were described: tight timelines, commercial partnerships with other firms, dispersion of IT roles, and access control to sensitive data, organisational scale and top management support are all examples of security

controls. Device complexity, vulnerabilities in systems and apps, mobile and distributed access, and a lack of effective protection measures are all technical issues (Kraemer et al., 2009; Badie and Lashkari, 2012; Metalidou et al., 2014).

Metalidou et al. (2014) show that information security knowledge is a vital tool for addressing security vulnerabilities. According to the study, the human element is often the weakest link in the security information assets, and this vulnerability is caused by the characteristics and behaviour of an individual. Previous studies demonstrated the lack of interest in learning about the effect of the human element on information security, even though this element is crucial in preserving the protection of the organisation's information (Metalidou et al., 2014). The increasing threats to information technology have made the researchers explore new strategies more dependent on human-centred solutions than technology solutions. The Information Security Retrieval and Awareness (ISRA) model proposed by Kritzinger and Smith (2008) can be utilised by the industry to improve information security awareness among personnel. The model focuses more on non-technical information security issues than technical issues, emphasising that non-technical cases involving humans should be given equal weight in securing information flow. According to the literature, human behaviour in the supply chain has been understudied in the area of factors that mitigates information security threats in the supply chain. As a result, it is crucial in the information security process (Van et al., 2010).

2.10 Related works on information security threats in the supply chain from technology perspective

Numerous research studies have been conducted on the topic of preventing cyberattacks. The literature review reveals that addressing supply chain (SC) threats requires the development of technological solutions to mitigate risks within the SC. In 2019, Abel and Islam proposed an approach that aids in modelling, analyzing, and reporting cyber threats in CSC attacks. Reed et al. (2017) presented a framework and a comprehensive list of supply chain attack patterns within the system. Li et al. (2009) found that there are limited remedies available to effectively stop cyberattacks based on a cross-case examination involving three UK-based organizations. Mirkovic and Reiher (2005) recommended protective measures at the source-end, while Chen and Hwang (2006) suggested core-end defense strategies. Wang et al. (2007) proposed casualty end protection, and Seo et al. (2013) introduced adaptable probabilistic filter planning. Khan and Creazza (2009) explored the application of product design to reduce supply chain risk. Furthermore, an analysis of a product design case study conducted in 2012 (Khan et al., 2012) highlighted that efficient product design management is a key strategy for mitigating supply chain risk.

The use of conceptual models and frameworks has emerged as the second most popular strategy to provide a comprehensive understanding of supply chain risks and their mitigation. Tse et al. (2011) developed a conceptual framework for managing quality risk in the context of a product recall caused

by vulnerabilities in the global supply chain. They emphasized the importance of supply chain visibility and strategic supply management in a multi-layered supply chain. Nooraie and Parast (2015) highlighted the significance of modelling in identifying and mitigating potential supply chain disruptions before they become critical. Jia and Rutherford (2010) examined the cultural implications between China and the West to define supply chain relational risk. Elahi (2012) identified four forms of risk in a conceptual study and emphasized the need for risk management to be shared throughout the organization. Ponomorov and Holcomb (2009) proposed a conceptual framework for analysing supply chain resilience based on the relationship between logistics capabilities and risk sharing. However, Wieland and Wallenburg (2013) found that supply chain integration has a minor impact on improving resilience. Ringsberg and Lumsden (2016) provided guidance on the application of standardized frameworks to cargo management.

Various modeling approaches have been employed to assess supply chain threats and their impact. Ganguly and Guin (2013) emphasized the need for risk quantification and mathematical modeling to establish a link between objectives and risk indicators in order to reduce potential dangers. They utilized the Analytical Hierarchy Process (AHP) to decompose supply chain risk categories and prioritize risks. Gaudenzi and Borghesi (2013) also found that AHP helped in prioritizing risks in their model. The subjectivity of risk assessment was acknowledged, as different individuals or parties may have different perspectives on what constitutes risk (Gaudenzi and Borghesi, 2013). Pujavan and Golgeci (2013) proposed the "House of Risk" framework for ranking and prioritizing hazards in a two-stage process. Wang et al. (2013) employed structural equation modeling to investigate perceived risk in the Chinese automotive spare parts industry. Lockamy and McCormack (2012) used Bayesian network modelling to assess the potential risk exposure of casting suppliers. In the context of supply chain resilience, Wieland and Wallenburg (2013) conducted a structural equation modelling analysis across three countries. Manuj et al. (2009) developed a simulation model building process for supply chain modeling. Information security knowledge sharing was proposed as another method to reduce information security hazards and raise awareness among employees (Attfield et al., 2010; Safa et al., 2016).

Cybersecurity, information security, technology, and telecommunications are the most common application contexts in supply chain research. This is unsurprising given the digital nature of cybersecurity. ICT has become increasingly important in supply chain management, as it provides essential infrastructure for global trade (Lu et al., 2013). However, research on the security of ICT supply chains is still in its early stages, with proposed models and frameworks often lacking validation data (Bartol, 2014; Lu et al., 2013). While security standards and regulations exist for different industries, widely accepted standards and recommendations for supply chain cybersecurity are still lacking (Boyson, 2014). Kennedy et al. (2019) applied criminology theory to improve consumer detection of threats to vehicle cybersecurity in the automotive supply chain. Pandey et al. (2020) focused

on data security and vulnerability detection. Block chain technology was used by Choi (2019) for authentication in luxury goods supply chains, and Debnath et al. (2020) raised data security concerns in mobile phone recycling. Hardware and software supply chains are also critical application contexts.

Table 2.4 Summary of Technology Approach

Field of Research	Application Context	Approaches	Sources
Supply Chain	Automotive Cybersecurity	Criminology theory Data protection and Vulnerability detection	Kennedy et al. (2019) Pandey et al. (2020)
	Energy, electricity, gas, oil and petroleum	Enhancement (SCADA System) Malware injection Blockchain technologies Stochastic Optimisations Model	Feltus et al. (2014) Couce-vieira and Houmb (2016) Mylrea and Gourisetti (2018a) and Mylrea and Gourisetti (2018b) Heath et al. (2020)
	Cyber, Information Technology and Telecommunication	Assurance Reference Model Risk Management Framework Guidelines and Government Awareness, Forensic analysis Bayesian analysis Machine learning Model Optimisation	Lu et al. (2013) Bartol (2014) Boyson (2014), Keegan (2014) Venter (2014), Masvosvere and Venter (2016), Tuptuk and Hailes (2018) Fernandes et al. (2019), Yeboah-Ofori et al. (2019a) Yeboah-Ofori et al. (2019b) Zheng and Albert (2019)
	Healthcare and Pharmaceutical Products	Block chain Technologies	Kshetri (2017), Norfeldt et al. (2019)
	Hardware and Software	Power signatures and infrared -(IR) thermos-graphic signatures Trojan horse identification Vulnerability identification Malware detection New Standard	McFadden and Arnold (2010), Jones and Horowitz (2012), Ramesh (2014), Das et al. (2020). Kuypers et al. (2014), Benthall (2017), Cayetano et al. (2018). 6De Haan (2020) Lysne et al. (2016), Uncu et al. (2019) Collier et al. (2014)
	Finance	Blockchain Technologies	Ma et al. (2019)
	Food and Perishable items	Encryption algorithms Hyperledger Fabric Physical layer and Blockchain	Chen et al. (2019) Iftekhar et al. (2020) Mondal et al. (2019)
	Luxury items	Blockchain Technology	Choi (2019)

	Maritime	Automatic Identification Systems (AISs), Attack Path	Mileski et al. (2018) Polatidis et al. (2017 ; 2018 ; 2020)
	Manufacturing	Vulnerability identification and intrusion detection Blockchain Technologies Designing Trustworthy gates Cyber security framework Designing up-to-date standards	Barron et al. (2016), Gupta et al. (2017) Boiko et al. (2020) Preuveneeers et al. (2017), Gupta. (2020) Fraile et al. (2018) Hutchins et al. (2015) Tuptuk and Hailes (2018)
	Reverse and Waste Others	Game-theoretical Blockchain Technologies Nonlinear Budget Constraints	Nagurney et al. (2017), Li and Xu (2021) Nijilla (2020), Simon and Omar (2020) Kshetri (2017), Ghadge et al. (2019) Helo and Hao et al. (2019) Colajanni et al. (2020)

2.11 Related works on information security threats in the supply chain from a human factor perspective

Information systems in organisations are the result of the collaborative efforts of technology, people, and management. Information security in supply chain depends significantly on all three of these factors, although people are often seen as the weakest link due to their error-prone nature (Evan, 2016). Despite the importance of information security in the supply chain, not much effort has been made regarding human factors. Most emphasis has been placed on enhancing technology as it has been recognised as the solution to having successful information security in the supply chain. However, behavioural SCM is still in its infancy (Donohue and Siemsen, 2011; Schorsh et al., 2016). It has received little attention.

Literature reports that many of the threats to the operation of computer systems in an organisation can be traced back to computer users' actions. However, information security threats cannot be detected, removed, prevented or avoided by relying solely on technology (Herath and Rao, 2009). Human behaviour that may place an organisation at risk includes, accidentally or deliberately, the exposure of passwords to others, victimisation of phishing emails by clicking on embedded website links, or the attachment of non-familiar media to work or home computers (Kathryn et al., 2014). Badie and Lashkari (2012) categorised the factors that affect the security of computers into two significant categories: the human element and the organisation factor. They reckon that the review of previous studies reveals that the human factor is more important than the organisational factor. They also suggested the human element should be divided into two groups: factors related to management, namely inadequate staffing and workload, and aspect related to the employee (end-user), namely lack of awareness, belief, behaviour, inefficient use of technology and lack of motivation (Metalidou et al., 2014).

Kathryn et al. (2014), created an empirically validated instrument called the Human Aspects of Information Security Questionnaire in their study (HAIS-Q). This instrument was used to assess employee knowledge, attitude and behaviour in order to establish a baseline for management to evaluate the success of various information technology (IT) control techniques or to track an organisation's long-term security health. There is still evidence of employee-related data security breaches. It requires employee and technology factor involvement in developing and maintaining a secure environment, and this has been a major challenge because organisations invest more on technology rather than in their employee (Kathryn., 2013). Nowduri (2014) carried out a detailed review of the literature on management information systems (MIS) and outlined a framework for the competency model in MIS among sustainable corporations. Posey et al. (2013) investigated protection-motivated behaviours (PMBs) of organisational insiders to protect organisationally relevant information and computer-based information system from a systematic approach. Posey et al. (2013) noted that organisational leaders

should recognise the important role of corporate insiders rather than relying on technology to protect the organisations' information resources.

Posey et al. (2013) identified and presented how corporate insiders classify 67 different PMB homogenous classes encompassing of eight taxonomy categories which are logically grouped into 14 clusters to reduce threats. Budzak (2016) explored people issues relating to information security, including threats to information security systems (ISs) and risks associated with ISs, and addressing mitigation of the threats through managing roles, responsibilities, relationships and training. The regular and constant deployment of information security campaigns, training, induction and awareness helps to improve people's knowledge and understanding of threats and risks to information security and how to mitigate those threats (Budzak, 2016).

According to D'Arcy, Hovav and Galletta (2013) point out that insider exploitation of IS resources poses a serious risk to businesses. Using an expanded form of the deterrence theory, they looked at whether users' knowledge of IS security countermeasures influenced their perception of the certainty and severity of organisational punishments. Using a representative sample of 269 workers from 8 different organisations, they discovered that users knew about the company's security standards thanks to staff training and the prevention of abuse. Furthermore, they found that the perceived severity of penalties was more beneficial than real punishments in curbing IS usage. Siponen and Vance (2012), have focused on deterrence theory in their investigations of IS security policy breaches, whereas they may benefit more from looking at neutralisation theory. They hypothesised that a neutralisation would have a favourable effect on the desire to break IS security regulations. The authors also theorised that people's intentions to break IS's security regulations were dampened by legal punishments, informal sanctions and humiliation. Using a sample of 395 workers from various companies, they discovered that neutralisation accurately predicted workers' desire to breach IS security standards. However, in the context of neutralisation, the impact of informal punishments on intent was not statistically significant. Furthermore, in the face of neutralisation, legal punishments failed to foretell IS security breaches.

Safa et al. (2019) proposed a model based on three theories (General deterrence, Situational crime prevention, planned behaviour), in order to mitigate the risk of insiders from engaging in information security misbehaviour they further empirically tested their framework using 152 paper -based questionnaire and 334 electronic questionnaires with employees of several companies that are active in the domain of e-Commerce, banking and education. They utilised SEM and CFA to analyse 612 collected questionnaires from organisations in the field of e-Commerce, banking and insurance, with employees that are familiar with the importance of information security. The result of the data analysis revealed perceived sanction, severity increases the risk, and reducing the reward towards safe information were significant. The findings also revealed that attitude, perceived behavioural control and subjective norms towards intention to secure information behaviour were significant.

Safa et al., (2018) proposed a model based on insider threats by analysing the role of motivation and opportunity to better understand how these factors (Commitment, attachment, involvement, and personal norms (Social Bond theory (SBT); and reduce the reward, increase the risk, reduce provocation, remove excuses and increase effort (Situation Crime Prevention Theory (SCPT) mitigate insider threats in organisation. They further empirically tested their model with 612 participants from organisation. Their findings revealed that commitment to an organisation's plan and policies have a significant effect on negative attitudes concerning misbehaviour. And also found out that commitment and reducing the reward had a significant effect on negative attitudes about misbehaviour.

Wang et al. (2015) and Cheng et al. (2014) emphasised that general deterrence theory was created as a technique to minimise the extent to which people participate in deviant behaviour, and it also employs punishment as a threat to people who would abuse the information system. It assumes that human behaviour is rational to some extent and that incentives, particularly the negative incentive inherent in formal penalties, can impact it (Cheng et al., 2014). Security countermeasures are a combination of activities and procedures that dissuade computer abuse and can lead to a considerable reduction in computer abuse (Wang et al., 2015). General deterrence describes human behaviour and decisions in terms of minimising their cost and maximising their benefit to the individual (Safa et al., 2019).

However, Cuganesan et al. (2018) have found that both sanction and reward have an equal negative impact as to attitude, self-efficacy or norms on the level of reducing information security compliance. In line with this finding, Cheng et al. (2013) also found that perceived sanction severity, commitment and subjective norms are major motivations for employees to engage in violation intention. Further examination of these studies revealed that the inconsistent results could be for two possible reasons. Firstly, these studies used slightly different indicators to measure the constructs, particularly sanction severity, commitment and level of reducing issues. For example, in a study by Cheng et al. (2013), sanction severity was measured by five indicators (if caught, I will be sanctioned by my organisation, I think receiving sanctions would have a bad influence on my career development, I think being reprimanded would have a bad influence on my career development) whereas in the Safa et al. (2019) study the same construct was measure by four indicators (consequences of the violation, deserve punishment, punishment will be high, receiving sanctions because of my information security misconduct). Thus, based on this observation, one could argue that the definition and aspect around sanction severity need can vary from one information security to another depending on the purpose and type.

Lee, Lee, and Yoo (2004) emphasized the significance of social bond theory in mitigating insider computer misuse within organizations. Similarly, other studies have employed social bond elements to explain compliance with information security policies and procedures. Therefore, these variables related to social bond can be considered as factors that contribute to reducing the risks associated with

information security (Ifinedo, 2014; Safa et al., 2015). Demonstrating commitment involves actively supporting the protection of organizational information assets, making a personal pledge to do so, and putting forth effort towards achieving this goal. Individuals who are committed to a cause attach great importance to their own successes and reputations.

Moreover, several researchers have attempted to examine factors that mitigate information security threats through established information security compliance behaviour in information security (Leering et al., 2020; Cuganesan et al., 2018; Ifinedo., 2012; Ifinedo, 2013; Cheng et al., 2013; Vance et al., 2012). Cuganesan et al., (2018) investigate the informal factors (i.e. Top management and workplace) and formal (specification, monitoring and evaluation) that influence employee attitudes and self-efficacy beliefs about information security. They discovered that senior management, specification, monitoring/ evaluation have a significant influence on attitude and norms. The outcome of their research showed that formal control (sanction), informal control (norms, self-efficacy, and attitude) and management control mechanism (reward and senior management support) are effective tools to influence the information security behaviour of employees. However, their data was collected from a government institution (Law Enforcement Agency).

Theory of planned behaviour (TPB) is extensively employed in many fields since it is one of the most predictive theories of influence. Users' intentions to follow information security policies were shown to be affected by users' attitudes, subjective norms and perceived behavioural control, as shown by Ifinedo (2014). He added that these factors shape an individual's actions using a survey of 124 business managers and IS professionals in Canada. This study showed that factors such as self-efficacy, attitude toward compliance, subjective norms, response efficacy and perceived vulnerability positively influence ISSP behavioural compliance intentions of employees. Balakrishnan (2015) used TPB to evaluate his staff's security policies and compliance habits. Perceived severity, perceived vulnerability, and perceived advantages are all health Based model (HBM) characteristics integral to information security awareness that was shown to be associated with this activity.

Wang, Tsui and Xin (2011) stated that it is widely documented in organisational research that leadership plays a significant impact in developing attitudes and beliefs around work and the associated responsibilities. Humaidi and Balakrishna (2018) are of the view that top management behaviour is often influenced by their superiors, who are also the leader of the organisations. Employees in the organisation tend to do what they have been asked to do and to respect their superiors, which can have positive or negative effects. Top management support has a significant impact on workers' information security behaviour, as has been shown in prior research (Huang and Chuang, 2007; Ifinedo, 2012). Leaders should set a good example when it comes to security and urge staff to follow ISP guidelines (Siponen et al., 2010). It has also been suggested that support from top management is a key factor in information security perceptions, beliefs and attitudes (Hu, Hart and Cooke, 2007), however, the

consequences of this factor are seldom investigated experimentally. Most senior managers are concerned about the confidentiality of organisations' operational data rather than protecting the firms' knowledge and information assets (Ahmad et al., 2014). Astuti and Nasution (2014) noted that 36% of SME leaders adopt IT solutions to minimise the effects of information security threats on computer system.

The effectiveness of rewards in influencing employee performance is crucial for achieving organizational objectives. However, empirical evidence regarding the impact of rewards is inconclusive (Malik, Butt, & Choi, 2015). Byron and Khazanchi (2012) emphasize the importance of awards within organizations and their widespread application. Research suggests that incentives can influence individual behavior if the recipients perceive the rewards as significant and relevant (Malik, Butt, & Choi, 2015).

Monitoring and evaluation involve continuously assessing the performance of programs, policies, and projects, including evaluating costs, deliverables, and timelines (Haque & Khan, 2014). This process ensures that implementation aligns with the established plans. In the realm of information security, monitoring and evaluating employees in terms of reducing security breaches, compliance, and appropriate information management practices convey the significance of security and the expected behavior from employees (Boss et al., 2009; Chen, Ramamurthy, & Wen, 2015).

Furthermore, several more researchers have attempted to examine human behaviour phenomenon in information security. Sindhuja (2014) introduced a supply chain framework to capture the information security measure at an intra-and inter-organisation level, by consolidating the technical, formal (organisational/managerial) and informal (people/social) controls under one roof, in a supply chain. Sindhaja's supply chain framework consists of various dimensions of information security and supply chain operations. Information security consisted of dimensions such as physical and logical information security, information security culture information security policy, information communication, supply chain operation and supply chain performance. Although the framework aimed to increase the level of developing the information security initiative in manufacturing companies and increasing trading partner's relationship, yet it was not theoretically based, and its application has not been implemented on a specific type of information security in the supply chain. This research work has gone a step further by identifying various information security threats in the supply chain and designing a framework using the human approach to combat these threats.

Other relevant theories that have been adopted in these studies include the Health Belief Model (HBM; Bonar and Rosenberg 2011; Dodel and Mesch 2019), the Rational Choice Theory (Li et al. 2010; Vance and Siponen 2012), the Social Bond Theory (Choi and Song 2018), the Social Exchange Theory (D'Arcy and Greene 2014), Control Theory and Reactance Theory (Lowry and Moody 2015),

Compensation Theory (Zhang et al., 2009). Personality (Shropshire et al. 2015; McCormac et al. 2017), and Norm Activation Theory (Yazdanmehr and Wang 2016).

In particular, Vafaei-Zadeh et al. (2020) attempted to improve the level of supply chain information integration on the operational performance through introducing information quality, information technology and information security. Although, these focused on social and technical related factors, yet they were only applied to supply chain information integration. Considering the target sample for this study, one could argue that these might have different effects on level of reducing information security threat when applying them to other types of information security in the supply chain. However, this research aims to investigate the effect of GDT, SBT alongside TPB and control mechanisms (top management, reward and monitoring /evaluation) factors on employees' behaviour in order to decrease information security threats in the supply chain.

Summary

To bridge the gap between theory and practice in understanding the human factors affecting the mitigation of information security risks in the supply chain, a review of existing literature was conducted. This review focused on human factors in related domains to gain insights into crucial success variables that are context-dependent and organization-specific. By examining these related fields, including managerial, organizational, policy compliance, and mitigation factors, a comprehensive understanding of the factors influencing the prevention and reduction of information security threats in the supply chain was developed, regardless of varying perspectives and criticalities.

The literature review identified examples of behavioural theories utilised in research connected to information security. However, due to limited empirical studies on information security threats in the supply chain, it remains challenging to draw definitive insights on how organizations mitigate threats in their supply chain and what variables and knowledge are necessary for addressing common issues. Furthermore, extensive research suggests that the success of supply chain maturity relies on a combination of multiple variables rather than a single component. Table 2.5 below.

Table 2.5: Summary of information security and human factor solution

Authors	Journal	Context of Study	Related Framework	Findings
Princely Ifinedo, 2014	Information & Management	Information systems security policy compliance	Social bond Social influence Locus of control Self-efficacy	Social bond and subjective norms made at work have a significant impact on employees' attitudes toward ISSP compliance. Marketing/Data research firm in Canada. 124 respondents.
Safa et al., 2019	Future Generation Computer System	Deterrence and prevention-based model to mitigate information security insider threats in organisations	Sanction certainty Sanction Severity Increase the effort Increase the risk Reduce the reward Reduce provocations Remove excuses Subjective norms Altitude	Information security misbehaviour among employees is deterred by deterrent considerations in workplaces. In addition, sanction severity has a major impact on people's attitudes and prevents them from information security violations. e-Commerce, Banking & Education. 486 Respondents in the UK. Empirically tested.
Merhi and Ahluwalia, 2019	Computer in Human Behaviour	Focuses on examining factors that affect employee behaviour	Punishment severity Certainty of detection Descriptive norm Moral norms	By broadly disseminating policies that clearly states punishment severity of failing to exhibit needed behaviour, IS users are made aware of what is expected of them, and a significant portion of them comply. Education, Retail, IT & banking. 133 respondents in USA.
Safa et al., 2018	Information security and application	Motivation and opportunity based model to reduce information security insider threats in organisations	Increase the effort Increase the risk Reduce the reward Reduce provocations Remove excuses Attachment Commitment Involvement Personal norms	A negative attitude toward misconduct affects employees' intentions to engage in misconduct favourably, which in turn lowers intentions for insider threat behaviour. Mixed Methodology. e-Commerce, Banking & Insurance. 612 Respondents in South Africa.

Cheng et al., 2013	Computer & Security	Understanding the violation of IS security policy	Perceived certainty Perceived severity Attachment Commitment Involvement Belief Subjective norm Co-worker behaviour	The severity of sanctions rather than the certainty of sanctions play a major role in the deterrence effect of formal control. Employees are less likely to violate the ISSP if they believe there will be severe sanctions if they are found out. Data are gathered at a particular point in time and from a single source. Other controls could be added to the model in subsequent studies to further the exploration. 185 employees in China. Empirical.
AlHogail, 2015	Computers in human behaviour	Establishing ISC in organisation	Strategy Technology Organisation People Environment	Provides a comprehensive base for organisations to develop an effective ISC in order to protect information assets. Data collected from expert.
Leering et al., 2020	Behaviour & Information Technology	More honour'd in the breach; Predicting non-compliant behaviour	Normative belief Compliance intention Self-efficacy Time pressure	Negative habits are a major contributor to non-compliant behaviour. Situational elements like time constraints and a lack of self-efficacy feed this behaviour. 651 respondents in the Netherland. Empirically tested
Princely Ifinedo, 2012	Computers & Security	Understanding information systems security policy compliance	Perceived Vulnerability Perceived severity Response efficacy Response cost Self-efficacy Attitude Subjective norms	It implies that an employee's attitude towards ISSP compliance in their organisation, as well as the point of view of colleagues in their workplaces, play critical roles in encouraging ISSP behavioural intentions. 124 business managers in Canada. Empirically tested.

Furnell et al., 2017	Computers & Security	Enhancing security behaviour by supporting user	Password selected by unguided users and those receiving guidance and alternative forms of feedback	Its advice to help users to refined their password choices. Experimental studies.
Hovav and D'Arcy, 2011	Information & Management	Information systems misuse	Security policies Security awareness programme Preventive security software Computer monitoring	Security-awareness programmes, user awareness of security policies, and preventive security software tends to significantly lowers users' IS misuse intentions while computer monitoring does not. 579 respondents in USA.
Furnell and Rajendran, 2012	Computer & Security	Understanding the influences on information security behaviour	Security monitoring Perceived benefits Personal benefits	
Safa et al., 2016	Computer & Security	Complying with organisational information security policies	Knowledge sharing Collaboration Intervention Experience Attachment Commitment Personal norms	Employees' attitudes are influenced by the commitment and personal norms. The behavioural intention regarding information security compliance is significantly influenced by attitude toward compliance with organisational regulations on information security. IT. 462 respondents in Malaysia.
Vance et al., 2012	Information & Management	Motivating IS Security Compliance	Vulnerability Perceived severity Rewards Response efficacy Self-efficacy Response cost	It is important to address past and automatic employee behaviour in order to increase compliance to information system security. 210 respondents in Finland.
Sindhuja P. N., 2014	Information Management & Computer Science	Information security initiatives on supply chain performance	Physical security Logical security InfoSec culture InfoSec policy Supply chain operation Supply chain performance	Information Security Initiation which includes technical, formal and informal security aspects in an intra- and inter-organisational setting, is favourably correlated with supply chain operations, which in turn has a favourable impact on the performance of the supply chain.

				191 respondents.
Cuganesan et al., 2018	Behaviour & Information Technology	How senior management and workplace norms influence information security attitudes and self-efficacy	Specification Monitoring/Evaluation Rewards Sanctions Senior Management Support Attitudes Norms Self-efficacy	Senior management's role in information security must be approached from an "employee-centric" perspective, and employees' perceptions of the leaders' commitment to information security must be evaluated through their communication and role-modelling behaviours. 388 respondents from Law Enforcement Agency. Australia.
Arachcilage et al., 2013	Computes in Human Behaviour	Avoiding phishing attack	Perceived threat Perceived susceptibility Perceived severity Safeguard effectiveness Safeguard cost Self- efficacy	In order to protect computer users against phishing assaults, the game design framework should take into account factors such as perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity, and perceived susceptibility. Education. 151 respondents in UK.
Hanus et al., 2016	Information system management	Users' security awareness	Coping appraisal Perceived severity Response efficacy Self-efficacy Response cost	Perceived severity, response efficacy, self-efficacy and response cost are significantly influenced by security awareness. Education. 241 respondents in USA.
Barton, 2014	Computer & Security	Information system security Commitment: A study of external influence	Normative mechanism Mimetic mechanisms Coercive mechanism Senior management	The findings suggest that senior management supports are critical to ISS success.
Wei et al., 2019	Information & Management	How explorative, information and exploitative IT capabilities inter-dependently moderate the relationship between supply	Organisational Information processing	Our findings suggest that while information sharing and company performance are moderated by complementary rather than substitutive IT capabilities, collaborative planning and firm performance is moderated

		chain information integration and firm performance		by complementary rather than substitutive IT capabilities. 215 firms in China.
Kankanhalli and Xu, 2009	Decision support system	Users' computer security behaviour	Perceived susceptibility Perceived benefits Perceived barriers Self-efficacy Perceived severity Cues to action General security orientation	The primary effects of perceived barriers, cues to action, overall security orientation and perceived severity, according to the data, are not statistically significant. Users may be discouraged from adopting safe behaviour if security is perceived as an inconvenience. Health, Education, IT-related organisation. 134 respondents.
Herath and Rao, 2009	European journal of information system	Protection motivation and deterrence: a framework for security policy compliance in an organisation	Punishment severity - Compliance behaviour toward IS policies Detection certainty - Compliance behaviour toward IS policies Perceived probability of security breach Perceive severity of security breach Security breach concern level Response efficacy Response cost Security policy compliance intention Security policy compliance attitude Self-efficacy Subject norm Descriptive norm Resource available Organisational Commitment	They found out that if employees perceive that their compliance behaviours have a favourable impact on the organisation or benefit the organisation, they are more likely to have more positive attitudes towards the security policies.

Parsons et al., 2014	Computer & security	Determining employee awareness using the human aspects of information Security Questionnaire	Knowledge of policy and procedure Attitude towards policy and procedures Self-Reported Behaviour	Training and education will be more effective if they define not just what is anticipated (knowledge), but also why this is important (attitude) a rise in non-compliant behaviour. 500 respondents in Australia. Empirically tested.
Badie and Lashkari, 2012	Journal of Basic and Applied Scientific Research	A new Evaluation Criteria for Effective Security Awareness	Lack of awareness User behaviour User belief Lack of motivation Inadequate use of computer security	One of the few things that can effectively manage hazards relating to people is knowledge and culture. Lack of sufficient awareness and training for those who may require it can expose the business to several security issues, when the threats and points of entry are people rather than technology or application vulnerabilities.
AlMindeel and Martins, 2021	Information Technology & People	Increase Understanding of Information security awareness	Perception Aspirations Challenge Enablers	Employees view information security awareness as a kind of defence against the risks connected to information security misbehaviour. Interview, Saudi Arabia.
Dang-Pham et al., 2022	Computer and Security	Identifying information security opinion leaders in organisations: Insights from the theory of social power bases and social network analysis	Infosec leadership Reward Sanctioning Infosec Negligence	Influential InfoSec opinion leaders were regarded by peers as having a working grasp of InfoSec and being able to encourage and penalise InfoSec behaviour. Information security leadership was also found to be increased by additional characteristics such formal seniority, age, tenure and department affiliation. IT-related organisation. 246 Employees in Australia.
Siponen et al., 2014	Information and Management	Employees' adherence to information security policies: An exploratory field study	Severity Vulnerability Response efficacy Self-efficacy Attitude	Employees' self-efficacy to potential information security threats, attitude toward adhering to information security policy, and employee normative beliefs all had a highly significant and positive impact on the

			Normative beliefs Rewards	employee's intention to comply with information security policies and procedures. It also revealed that the intention to comply with information security policies had a highly significant and positive impact on actual compliance with the policies. 669 respondents in Finland.
Anderson and Argarwal, 2010	MIS Quarterly	Practising safe computing	Security threat Perceived citizen Effectiveness Subjective norms Descriptive norm Attitude	The findings suggest that a home computer user's intention to perform security -related behaviour is influenced by a combination of cognitive, social and psychological components. Home computer users USA. 594 respondents.
Johnston and Warkentin, 2010	MIS Quarterly	Fear appeals and information security behaviour	Fear appeals and information security behaviour	The findings of this research contribute to information systems security research, human -computer interaction and organisational communication by revealing a new paradigm in which IT users form perceptions of the technology not on the basis of performance gain but on the basis of utility for threats mitigation. Experimental.
Moody and Siponen, 2013	Information and Management	Using the theory of interpersonal behaviour to explain non-work-related personal use of the Internet at work	Beliefs Norms Evaluation Roles Self-concept Attitude Affect Social factors	The use of internet for personal purposes is due to the feelings associated with doing so, and the habit that these employees have formed. Employee motivation and commitment lowers the use of computer for personal use at work place. Private service company. 238 respondents in Finland.
Zhang et al., 2021	International Journal of Logistics:	How does knowledge seeking and knowledge generation promote green	Knowledge seeking Knowledge application Knowledge generation	

	Research and applications	supply chain management? An empirical study from China	Self-efficacy	264 companies in China.

Table 2.5 above shows factors that occurs frequently and are supported by empirical research evidence that was selected to establish a conceptual model of mitigating factors for INTSC. These factors play an essential role in the information security domain but not in the supply chain; broad in scope and cover many regions and sectors. This research identified nine factors posited to influence the different dimensions of INTSC from related contexts, as some of the factors overlap with each other in the constructs. These factors (Sanction, Commitment, Reward, Self-efficacy, Subjective Norms, Attitudes, Top management and Monitoring/Evaluation) were selected based on their frequent discussion in the literature and organised recurrence of the constructs and their importance to security-related behaviour (Cheng et al., 2014). Also, these factors are an extension of the model of Cugansan (2018) for information security compliance. This thesis follows the view that these factors are linked to theories that will be explained in the next section.

2.12 Theoretical Background

Reflecting on the literature review, scholars have long acknowledged that although progress has been made in creating and deploying more sophisticated protective technology and establishing and enforcing effective security policies and procedures, human factors play a crucial role in ensuring the safety of an organisation's sensitive data. Literature reports that IS researchers who conducted the first studies on information security mostly relied on questionnaires sent out to managers and people working in companies, which were then organised according to ad hoc theoretical or empirical frameworks (Hu et al., 2011). IS researchers have recently begun to use more well-established theories in their studies of information security challenges (for example, Siponen, 2010:D'Arcy, 2009; Dinev, 2007).

Several theories have been employed as pillars in information security policy, security compliance, cyber-information security, supply chain, and supply chain security research. Furthermore, these theories have been used widely in literature to explain and predict employee security-related behaviour. Research in the field of information security has often taken its theoretical grounding from the criminology literature due to the striking similarities between violations of information security policies in organisational settings and criminal behaviour in social settings (Alsare et al.,2018). Despite their widespread use in the field of criminology, rational frameworks are often employed in tandem with other theoretical models. Since humans have limited cognitive capacity (Simon, 2000), the elements influencing their ability to make sound decisions will vary depending on their circumstances. Table 2.6 highlighted related theories related to this study.

Table 2.6: Theories related to the field of the study

Theory	Description	Authors/Origin /Year/Domain	Other authors apply it in their studies	Why GDT, SBT, TPB was chosen
General Deterrence Theory (GDT)	• Human beings are fundamentally rational in their behaviour and choose crime when it pays. • Individuals are less likely to commit criminal acts if the perceived certainty, severity, and celerity of sanction against the acts are greater. • Explain how severe, swift, and precise sanctions deter people from engaging in actions	Gibbs (1975), Criminology	Safa et al., (2019), Alshare et al., (2018) Cheng etal.,2014, Chen et al., (2018), John et al, (2016) Dinev et al., (2009), Guo and Yuan (2012), Hovav and D'Arcy (2012), Safa et al., (2019), and Siponen and Vance (2010)	• The perceived severity of penalties was more beneficial than real punishments in curbing IS usage. • The concept is that the greater the perception of the severity of a sanction, the less likely an individual will indulge in such behaviour, which is why it was chosen. • This insight helps to understand how the legal system and enforcement mechanisms affect behaviour; it also guides the development of strategies aimed at deterring possible offenders. • In comparison to sanction certainty and sanction perception, the author adopted sanction severity because, from previous studies, employees are observed to exhibit positive information security behaviour if they know the punishment for the defaulter is severe.
Protection Motivation Theory (PMT)	• Explain how a person examines a threat and a potential solution in his mind before deciding whether to behave in an adapted or ill-adaptive way.	Rogers (1975), Psychology	Boss et al.,2015, Chou and Chou (2016), Dang-Pham and Pittayachawan (2015), Hanus and Wou (2016), Hina etal.,(2019),	• Protection Motivation Theory (PMT) is a useful framework for predicting how employees—including IT professionals and others—would react to programmes that highlight potential dangers and how they will

			Johnston and Warkentin (2010), Meso et al.,2013, Posey et al, (2015), Torten et al.,2018, Tsai et al., (2016), Van Bavel et al., (2019), Warkentin et al., (2016), and Workman et al., (2008).	respond in terms of their desktop security behaviours. Therefore, businesses should put a lot of work into creating and delivering training to every employee. ● Participants who were exposed to coping messages—either alone or in conjunction with a threat appeal—behaved more securely than participants in the control condition. ● Threat appeals were less effective than PMT components at predicting intent to engage in protective behaviours.
Neutralization theory	● State that individuals breach the law because they find some way to defend their actions despite abiding by society's norms and standards.	Sykes &Matza (1957), Criminology	Al-Mukahal and Alshare (2015)	● Trust, the effect that information security policy implementation would have on the workplace, and the information security policy's clear definition of its scope all had a major role in predicting the frequency of information security policy violations. ● The results also show that cultural factors like collectivism and the avoidance of uncertainty regulate links between trust, the extent to which policies are clearly defined, how much of an impact they have on workplace environments, and the frequency with which policies are violated.
Social Bond Theory / Social Control Theory	● Individuals are sensitive to the consequences of their actions and reasoned judgements based on the	G.S. Becker (1974), Criminology	Safa et al., 2016; Ifinedo,2014,	● Since people are the primary source of behavioural information security control, people's commitment to protecting information security assets

	cost-benefit analysis of the intended acts. ● The decision to engage in criminal behaviour is a function of a criminal act's perceived costs and benefits. ● Define those individuals who evaluate the potential outcomes of each option before identifying their option	Hirschi (1969)		is crucial. Committed people invest more time and effort to succeed in their careers and they are loyal to their organisation. ● Committed employees will not intentionally engage in information security misconduct because of their dedication to their career progression and company growth. The commitment of employees has been selected over other social bonds factors like attachment and involvement.
Theory of Reasoned Action or Theory of Planned Behaviour	● Explain how each person's behaviour is a conscious choice impacted by social pressure and cognitive thought. ● An individual's favourable or unfavourable evaluation of a specific behaviour, specifically related to mitigating information security threats in the supply chain. ● Reflects how individuals perceive the opinions and beliefs of their closest friends and colleagues regarding a specific action. ● Self-efficacy refers to an individual's belief in their ability to successfully accomplish specific tasks or goals. It is a concept that is	Hirschi (1974), Criminology Ajzen (1991) Bandura's (1991)	Safa et al., (2018), Fauzi et al., (2019), (Dinev et al. 2009; Bulgurcu et al. 2010; Hu et al. 2012; Ifinedo 2012; Cox 2012; Ifinedo 2014; Safa et al. 2015; Humaidi and Balakrishnan (2015), Yoon and Kim (2013) Siponen et al. (2014), Ifinedo 2014; Cox (2012) Safa et al. (2015)	● Since people are the primary source of behavioural information security control, people's attitude to protecting information security assets is crucial. ● It is the most predictive and persuasive theory. ● It suggests people's intentions are influenced by attitudes subjective norms and self-efficacy. ● This theory was selected by the author because previous research depicts that securing information of a company supply chain effectively requires some level of employee competence. More so, the attitude of workers towards information security in their organisation supply chain is

	closely related to self-confidence and perceived competence. Self-efficacy beliefs influence an individual's motivation, effort, persistence, and resilience in the face of challenges or setbacks.			influenced by their colleagues, friends, line manager and other social pressures.
Self Determination Theory	• Explains what intrinsic and some kinds of extrinsic motivation are and how they affect situational reactions in various disciplines	Ryan and Deci (2000), Psychology	Menard et al.,2017, Kranz and Haeussinger, (2014)	• Findings offer compelling empirical proof that workers who believe their actions are under their control and internalise ISS management's external rules are more likely to follow ISPs. • Deterrence-based methods like monitoring or punishment can only be a supplement to an efficient security management, given the significance of internal PLOC (perceived locus of causality) and the modest influence of external PLOC.
Social Cognitive Theory	• Explain the simultaneous and dynamic interaction of societal and personal factors in	Bandura (1989), Psychology	Ahmad, (2019); Ifinedo, (2014)	• Social bond and subjective norms made at work have a significant impact on employees' attitudes toward ISSP compliance.
Involvement Theory	• Explain how much energy, time, and engagement in a particular task affects attitude and manifests in various ways. • This theory can be found in a variety of sectors, including customer engagement, product involvement, and student involvement.	Astin (1999), Education.	Safa et al., (2016),	• Employees' attitudes are influenced by the commitment and personal norms. The behavioural intention regarding information security compliance is significantly influenced by attitude toward compliance with organisational regulations on information security.

Theory of Interpersonal Behaviour	● Demonstrate that behaviours are more intricate than they appear since they are made up of facilitating situations, additional social components, attitude forecasters and factors such as habits and intents that can better predict behaviours.	Triandis (1977)	Moody et al., (2018), Moody & Siponen, (2013).	● The use of internet for personal purposes is due to, the feelings associated with doing so, and the habit that these employees have formed. Employee motivation and commitment lowers the use of computer for personal use at workplace.
Cognitive Evaluation Theory	● Explain the ways in which people's intrinsic motivation can be affected by both internal and external factors.	DeciL, Cascio F (1975), Psychology	Siponen et al., (2014)	● Employees' intentions to follow information security policies and procedures were significantly and favourably impacted by their sense of self-efficacy in the face of potential information security threats, attitude towards adhering to information security policy, and normative views. ● Information security policies were more likely to be followed when people intended to do so, a highly favourable and significant influence.
Organizational Behaviour Theory	● Explain the social conditions that allow for the application of a variety of control methods.	Davis & Newstrom (1989), Management Organisation	Lowry and Moody, (2015)	● Putting compliance aside, reactance at work is a particularly problematic phenomenon because it can lead to the kind of harmful antisocial action that is closely linked to the emergence of unpleasant emotions like anger. Therefore, tight control may lead to unintended ISP compliance, but if reaction is also sparked, the result could be a disastrous Pyrrhic victory for any organisation.

Norm Activation Theory	● Identifying which of one's own personal norms served as the impetus for one's behaviour and how that behaviour relates to one's adherence to their own internally held values is important.	Schwartz (1977), Psychology		
Psychological Reactance Theory	● Explain how individuals feel that if any of their activities are interrupted or threatened to be halted, it will stimulate the encouraging state of psychological reaction. Describe how people feel if any of their activities are stopped or threatened to be stopped ● Predicts that any person has a range of behavioural liberties (a sphere of personal freedom) that, should they be taken away or threatened with being taken away, will cause reactance, a negative state of arousal.	Brehm (1966) Psychology Brehm, (1972); Brehm & Brehm, 1981).	Lowry and Moody, (2015)	● Beyond mere compliance, reactance in the workplace is a particularly problematic phenomenon because it can lead to the kind of damaging antisocial action that is closely associated with unpleasant emotions like anger. Therefore, tight control may lead to undesirable ISP conformity, but if reaction is also sparked, the result could be a disastrous Pyrrhic victory for any enterprise.
Social Exchange Theory	● Studying people's actions and how they interact	Blau (1986); Liao, (2008) Management Organisation	D'Arcy and Greene, (2014)	● Findings offer factual proof that workplace security compliance is influenced by security culture. Another conclusion is that an employee's intention to comply with security regulations is influenced by his or her sense of job satisfaction, albeit this link seems to depend on the employee's position, tenure, and industry. Surprisingly, there was a negative correlation between the intention to adhere to security compliance standards and perceived organisational support.

Dynamic Capabilities Theory	● The approach, which evolved from resource-based thinking, places a premium on the adaptability of businesses in the face of ambiguity and rapid change. ● Capability of a business to respond to changes in the competitive landscape and develop innovative value-creation strategies by integrating, constructing, and reconfiguring internal and external resources through organisational processes. ● Analyses how well businesses can anticipate change, adapt to new circumstances, and reorganise their resource bases to maintain a competitive edge in an uncertain market.	Teece et al., (1997) Management Organisation	Asamoah et al., (2021) Singh et al., (2019), Yu et al., (2019)	● The study found a good and significant impact of IOS use on SCM capabilities. The ability to gather information from both inside and outside the organisation is made possible by a company's integrated supply chain management systems that are used for communication and intelligence. IOS findings are underutilised when it is only used for business intelligence and communication. The study's findings show how IOS communication and business intelligence utilisation are connected. ● Exploitative dynamic capacities can be developed with a transactional leadership style and absorbed slack resources, but explorative dynamic capabilities can be developed with a transformational leadership style and unabsorbed slack resources. Additionally, we discovered that exploitative dynamic abilities support explorative dynamic abilities and that explorative dynamic abilities strengthen exploitative dynamic abilities.
Contingency theory	● Indicates that different contexts call for different approaches to managing the processes of organising decision-making and leadership.	Lawrence and Lorch, (1967); Luthans (1976)	Asamoah et al., (2021), Grotstch et al., (2013), Park et al., (2016)	● The ability to gather information from both inside and outside the organisation is made possible by a company's integrated supply chain management systems that are used for communication and intelligence. IOS findings are underutilised when

	● It also looks at the factors both within and outside the company that might affect its atmosphere.			it is only used for business intelligence and communication. The study's findings show how IOS communication and business intelligence utilisation are connected. ● Using the contingency theory, this study attempted to theorise that social factor, such as organisational culture, may influence how supply chain security practises are implemented within an organisation and how much they affect risk vulnerability.
Technology Acceptance Model (TAM)	● Explains why people would adopt m-commerce as a new technology. Additionally, it was created to describe and forecast consumer intent to adopt an information system.		Dinev et al., (2009) Barry M and Jan M. T., (2018)	● Potential smartphone users would only engage in mobile commerce if they found it to be fun, safe, and beneficial. Therefore, if adopting the technology will result in more observable and useful benefits for customers, the intention to use it will increase.
Cognitive Evaluation Theory (CET)	● Explain how both internal and external factors affect an individual's motivation.		Siponen et al., (2014)	● Employees' attitudes towards sticking to information security policy, sense of self-efficacy in the face of potential information security threats, and normative beliefs all had a significant and positive impact on their intents to follow information security rules and procedures.
Rational Choice Theory	● Presupposes that an individual would select a course of action that, in their estimation, will result in a social outcome that maximises	G.S. Becker (1974)	Li et al., (2010) Sato Y, (2013),	● Employees must weigh the costs and benefits of adhering to the IUP. When perceived benefits are outweighed by possible dangers from formal punishments and security threats,

	their desire within a set of subjectively imagined limitations.			employees are more inclined to abide by the internet use policy (IUP). The detection likelihood plays a major role in the deterrence effect of formal sanction risks.
Risk Compensation Theory	• Suggests that when people feel more protected, they may act less cautiously.		Zhang et al.,2009	• The degree to which one intends to follow security policy is significantly influenced by attitude and perceived behavioural control (PBC). Technical protection perception has a direct and indirect impact on behavioural intentions via PBC.
Norm Activation Theory	• Sentiments of moral responsibility are an appropriate tool to assess personal norms since obligations, like norms, precede actions.	Schwartz (1977) Psychology	Yazdanmehr and Wang 2016	• It suggests that personal norms may serve as an alternative explanation for well-established characteristics like fear appeal and deterrence for ISP compliance behaviour. • The strength of ISP-related personal norms on ISP compliance relies on how much of a personal obligation an employee feels.

Literature report that security controls are procedures used to decrease threats and attacks or other harmful events happening. Tipton and Krause (2007) classify controls used to protect data as either physical, technological or administrative control. Protection in a managerial setting may be achieved by administrative security. Safa et al. (2018) and Safa et al. (2019) adopted formal and informal control to reduce the tendency for information security misconduct. Formal control employs legislation and official government agencies to promote compliance, and informal control, which employs morality and social institutions to encourage individuals to conform to the law. Both may be effective in preventing illicit activity (Chen et al., 2014). Since people's beliefs, morals, and social standing may differ, it is difficult to determine which type of control is more effective. Typically, a combination of formal and informal constraints is used to deter criminal activity, with formal restrictions receiving slightly more weight (Chen et al., 2014).

Since supply chain companies are an administrating setting, this research suggested that control mechanisms (top management, reward and monitoring/evaluation) apply to supply chain companies. This control mechanism prevents employees' deviant behaviour and compels employees' actions (Chen et al., 2014). It results from an employee's self-evaluation of their relationships with others, as well as consideration of external pressures. A large body of literature examines the controls mechanism for information security and supply chain at technical controls, but theories related to information security and control mechanism level have been scarcely emphasized. In this study, the researcher establishes a framework from the view of both theories and control mechanisms the conceptual model is shown in Fig 3.1.

Table 2.5 above highlights human behavioural theories that are related to the study. Based on the findings and application of these theories from other extant literature, the author adopted the three most relevant theories in evaluating the influence of human factors in supply chain information security. The theories below were adopted by the author for this research.

General deterrence theory (GDT): The author chose to prioritize the concept of sanction severity over sanction certainty and sanction perception based on previous research findings. These studies have shown that employees are more likely to engage in positive information security behaviour when they are aware of the severe consequences imposed on individuals who fail to comply. By focusing on the severity of punishments, the author aims to examine how employees' awareness of the harsh penalties influences their adherence to information security measures. This decision is grounded in the understanding that the knowledge of severe repercussions serves as a motivating factor for individuals to follow security protocols.

Social Bond Theory: Employees who are committed to their career advancement and the growth of their company are unlikely to deliberately partake in information security misconduct. The author has chosen to focus on employee commitment as a key factor, prioritizing it over other social bonds

elements such as attachment and involvement. This decision is based on the understanding that committed employees, driven by their dedication and loyalty, are less likely to engage in behaviours that jeopardize information security. Their strong commitment serves as a protective factor, reducing the likelihood of intentional misconduct in this area.

Theory of Planned Behaviour: The author chose this theory because prior research has shown that effectively securing the information of a company's supply chain relies on the competence of its employees. Additionally, the attitudes of workers towards information security in the supply chain of their organization are influenced by various social factors, including colleagues, friends, line managers, and other social pressures. These considerations led the author to select this theory as a framework for understanding the interplay between employee competence and social influences on information security attitudes within the organizational supply chain.

2.13 Research gap

Through an extensive review of relevant literature examining factors related to information security threats in the supply chain, it was revealed that there is a lack of comprehensive studies focusing on the effectiveness of these threats beyond just technological aspects. The identification and classification of threats in the supply chain were identified as challenging tasks that require attention.

The sharing of information within supply chains exposes them to various risks commonly referred to as "information threats" (Rajagopal et al., 2017), which have become significant risks for businesses. These threats include harmful attacks from viruses, worms, and hackers (Sharma, 2016). Existing literature has discussed information security threats in a scattered manner, without providing an exhaustive list of all potential threats in the supply chain. Some studies have identified specific threats such as Stuxnet, Dudu, and Flame (Urciuoli et al., 2013), Trojan horses, spyware, and spyware businesses (Singh et al., 2017), intentional or direct threats, and unintentional or indirect threats (Safa et al., 2017). Others have focused on the impact of Trojans on the supply chain (Jiaji He et al., 2015), threats caused by third-party suppliers (Wang et al., 2019), and information security threats resulting from employee negligence (Zauwiyal et al., 2018), among others.

To the best of the author's knowledge, no existing literature has provided a comprehensive and detailed identification and discussion of information security threats in the supply chain. General threats are summarized in Table 2:3, while Table 2:4 describes specific information security threats in the supply chain. This research aims to fill this gap by extensively addressing these threats. Thereby **fulfilling**

Research Objective 1:

To critically review prevalent threats in the information security within the supply chain.

Several studies have predominantly focused on information technology systems as the primary source of information security threats, particularly within the domain of information technology (Brotby and Hinson, 2013; Kenny 2017; Masvosvere and Venter, 2016; Tsai et al., 2021; Fernandez et al., 2019; Yeboah-Ofori et al., 2019a; Yeboah-Ofori et al., 2019b; Zheng and Albert, 2019). However, Singh et al. (2013) argue that technology alone cannot provide a reliable solution to address the complex information security needs and challenges within organizations. Werlinger et al. (2009) also suggest that, in addition to technological measures, employee and organizational factors should be taken into consideration to effectively manage information security difficulties. Despite the significant investment in technological measures and security products, users of a system can become the largest opponents and introduce substantial risks (Alhogail et al., 2015). The behaviour of individuals who access, use, administer, and manage information resources plays a crucial role in determining the success of these technologies (Ashenden, 2009). However, human behaviour in the context of information security and the supply chain has received comparatively less attention in research (Schorsh,2016)

The behaviour of employees, whether intentional or negligent, poses a significant risk to information assets. Safa et al. (2016) argues that relying solely on technology is not sufficient. Previous studies have consistently shown that most information security issues are caused by human errors (Evans et al., 2016; Kwon, Ulmer and Wang, 2012). The human and behavioural aspects, referred to as "soft wiring," play a crucial role in supply chain management, encompassing processes, technologies, and measurement methods. Effective supply chain management should prioritize the clear management of the behavioural factor (Huo et al., 2015). However, the field of behavioral supply chain management is still in its early stages (Donohue and Siemsen, 2011; Schorsh et al., 2016). It can be argued that relying solely on technology cannot resolve these issues; the human factor is necessary for efficient supply chain performance (Abawajy, 2014; Abouzahra, M. and Ghasemaghaei, M., 2020; Kraemer and Carayon, 2007). Therefore, there is a lack of focus on the human factor in the context of the supply chain. This research aims to provide comprehensive insights into the human factors that influence information security threats in the supply chain and propose mitigation measures to reduce these threats.

Previous empirical research on information security in the supply chain and human behaviour has been conducted in various countries. Safa et al. (2016) conducted research in Malaysia and found that employee commitment and personal norms influence their attitude, which, in turn, affects their information security behaviour. In Canada, Ifinedo (2012) concluded that employees' attitudes and perceptions of their co-workers impact their intention to adhere to the Information Systems Security Policy (ISSP). Merhi and Ahluwalia (2019) conducted a study in the United States and discovered that employee awareness of the severity of sanctions positively influences their policy compliance. AlMindeel and Martins (2021) conducted a similar investigation in Saudi Arabia, while Dang Pharm et al. (2022) conducted their research in Australia. Different authors have explored various aspects of information security threats and tested their models in different countries.

Past empirical studies have investigated the risks associated with information security in the supply chain and the influence of human behaviour in multiple countries. Safa et al. (2016) conducted research in Malaysia and determined that employee commitment and personal norms play a role in shaping their attitude, which subsequently affects their information security behaviour. Ifinedo (2012), who conducted a study in Canada, proposed that employees' attitudes and perceptions of their co-workers impact their intention to adhere to the Information Systems Security Policy (ISSP). In a study conducted in the United States, Merhi and Ahluwalia (2019) found that employee awareness of the severity of sanctions positively influences their compliance with policies. Similar investigations have been carried out in Saudi Arabia by AlMindeel and Martins (2021) and in Australia by Dang Pharm et al. (2022). Various authors have explored different aspects of information security threats and tested their models in diverse countries.

Sindhuja (2014) conducted a study in India to examine the impact of information security initiatives on the supply chain. In a similar vein, Safa et al. (2018) and Safa et al. (2019) conducted research on mitigating information security insider threats using a theoretical model, but their studies were empirically tested in South Africa and the United Kingdom, respectively. Cuganesan et al. (2018) investigated compliance with information security in the workplace using a similar construct, but their model was tested in Australia. Leering et al. (2020) conducted a study on non-compliant behaviour in the Netherlands. Alese et al. (2014) analysed issues related to cyber threats in Nigeria. Although William et al. (2019) examined employee behavioural factors and information security compliance in Nigerian banks, there is still a gap in research that explores a standardized approach to mitigating information security threats in the supply chain of Nigerian companies, especially when considering international security standards. The William et al. (2019) studies focused on employee behavioural factors and compliance with information security standards in Nigerian banks. Therefore, this study will be conducted in the context of a developing country, which ranks 8th globally in terms of internet usage and faces significant challenges related to cyber threats. Table 2.5 provides an overview of selected academic studies that concentrate on information security in organisation.

Furthermore, this research encompasses both emerging and established countries. Given these circumstances, the aim of this study was to thoroughly investigate the factors contributing to the mitigation of information security threats in the supply chain in Nigeria, despite the significant challenges faced by businesses and the government. While there have been previous studies that primarily focused on information security management and risk management, such as (Al-Awadi and Weir 2016; Alkhudhayr et al., 2019; Alhassan and Adjei-Quaye 2017) they alone do not provide an adequate foundation for successfully mitigating and preventing threats in information security within the supply chain.

Understanding and addressing the impact of human risk factors can be challenging. Most studies lack a comprehensive approach to evaluate the effectiveness of general risk management elements in different relevant contexts concerning information security threats in the supply chain. Therefore, there is a need for rigorous qualitative and quantitative empirical research to verify and refine these characteristics within their natural environments. This is crucial because information security threats in the supply chain are not a linear process; rather, they are complex, involving qualitative and quantitative variables that influence the effectiveness of mitigation efforts (Tsai et al.,2021). In the context of information security threats in the supply chain, quantitative approaches may prove inadequate since, as stated by Hutchins et al., (2015), quantitative methods are not applicable when human actions are unpredictable. To contribute to the existing literature, this thesis will employ a combination of qualitative and quantitative approaches, leveraging qualitative research to complement quantitative analysis and investigate the influence of human factor variables on information security threats in the supply chain in Nigeria.**Thereby fulfilling Objective 2:**

To identify and investigate human factors influence of human factors on mitigating information security threats in the supply chain.

- **Objective 3**: To develop and propose an integrated human behaviour model for mitigating information security threats in the supply chain.
- **Objective 4:** To provide recommendations for business owners and managers to enhance and secure their information security in the supply chain.

The review of literature uncovered several important theories and elements that could be relevant for mitigating threats, as supported by empirical studies. These factors were carefully selected and their relevance to the study was explained, as presented in Table 2.5, opening avenues for further investigation. To address goal 2 more comprehensively, the literature review emphasized key aspects. Consequently, the research questions outlined in section 1.6 seek to explore in greater depth how each of these aspects contributes to the mitigation of information security threats at the supply chain level. Exploring these characteristics further may provide insights needed to bridge the gap in understanding the human factor identified in this chapter.

Furthermore, the examination of relevant literature revealed a lack of theoretical models that capture the success variables influencing the adoption of ISTSC. Consequently, the research identifies factors, establishes their relationships, and analyses the impact of people's behaviour on threat reduction. These factors are examined through hypotheses, delving into the complex interactions that often result in ongoing changes. In this regard, a model of human behaviour was developed in Chapter 3 (Figure 3.1) based on three theories (GDT, SBT and TPB), components gathered from the literature, such as top management, reward systems, and monitoring/evaluation (refer to sections 2.12 and 2.12.1). The purpose of this model was to illustrate how these factors influence ISTSC, fulfilling the objective of understanding the interplay between various elements and their impact on information security threats in the supply chain.

Research Objective 3:

To develop and propose integrated human behaviour model for mitigating information security threats in the supply chain.

The advancement of past research is beneficial to IS managers working in different organisations and industries, particularly huge manufacturing companies in Nigeria. This is because SC assaults are becoming more vital than ever for organisations all over the globe. As a consequence of this, investigating the variables that have an impact on the adoption of ISTSC in Nigeria can turn out to be an essential part of the study that is required to assist businesses in successfully reducing threats in the supply chain. The empirical investigations that were carried out to meet the study goals are answered

and discussed in detail throughout Chapters 4, 5, 6 and 7 of this thesis. Thereby fulfilling **Research Objective 4:**

> *To provide recommendations for business owners and managers to enhance and secure their information security in the supply chain.*

- **Summary**

This chapter looked at several key features of supply chain management and how sharing information can help improve SC performance. The definitions and evolution of supply chain management and supply chain collaboration were the focus of the first half of the review. Supply chains are challenging to manage since they are made up of a number of groups with varied and sometimes conflicting goals. However, because no single firm can generate all of the necessary resources, skills and experience on its own, it is critical for supply chain enterprises to work with one another, focusing on the whole chain's performance. As the demand for supply chain collaboration grows, so does the necessity for information sharing among chain partners, as information exchange is one of the most crucial foundations of collaboration. The requirement for information sharing in the supply chain has its own set of difficulties. Information exchange with trading partners will aid in the building of collaborative partnerships and the development of more valuable and actionable knowledge, lowering overall supply chain threats.

This section includes an overview of the literature that aided in the development of the research's theoretical framework. In order to manage supply chain information exchange, supply chain information security is a must. Sharing information with partners can aid companies in coordinating and cooperating, improving supply relationships, reducing supply chain dangers and increasing customer satisfaction. However, because of the challenges, corporations are hesitant to share information in the SC, emphasising the importance of identifying supply chain vulnerabilities. This chapter's section 2.5 describes how a systematic study of the literature was conducted to identify a broad list of threats that affect supply chain information security and possible solutions to address those issues from the human factor perspective.

Several threats to supply chain have been found in previous studies. However, a comprehensive list was not found in the literature research. Furthermore, there has been little work done to analyse and categorise the dangers that have been detected thus far. To cover all of the identified concerns and define the threats in the supply chain, a comprehensive outline was required. Such analyses allow for a better knowledge of how information risks are enabled in SC, allowing for the development of solutions to strengthen SC information security. The comprehensive literature analysis identified 16 threats that could have an impact on supply chain information security. It also synthesised the many classifications used in the literature and identifies and explains the 16 threats.

Human behaviour in supply chains is understudied, according to the literature review. Decision-makers that make poor decisions lead to deviant behaviour. According to literature analysis, technology alone cannot solve the problem of minimising supply chain threats. Human factors were identified as a factor that will be utilised as an approach to mitigate information security threats in the supply chain domain.

According to the literature review, few studies on supply chain management and information security have been conducted in developing countries like Nigeria, which differ greatly from developed countries in terms of information technology availability, infrastructure development, culture, management styles and policies, and organisational size. Adoption of models that were designed primarily for rich countries may not yield meaningful outcomes in developing countries. There is a definite need to conduct a study in a developing country to see if past research findings are applicable. The next chapter focuses on creating a theoretical framework for reducing information security threats.

Table 2.7: Summary of research gap

Summary of Research Gap	
a.	Lack of comprehensive identification of information security threats in the supply chain
b.	Insufficient research on the influence of human factors and mitigation approach in information security threats in the supply chain
c.	Scarcity of empirical research on mitigation of information security threats in Nigeria's supply chain

The study goals are discussed in Chapter 3, along with several related topics. In addition to this, a discussion of the conceptual framework as well as the theories that drives this study is included, and the hypotheses.

Chapter 3: Research Framework

3.1 Introduction

Chapter 2 provided an overview of the existing academic literature, focusing on the literature review and identifying gaps that require further investigation. The review of literature has shed light on various theories that have been significant in previous studies. These theories are valuable as they enhance our understanding of how to mitigate threats in information security within the supply chain (Sulaiman et al., 2022). By examining the literature in Chapter 2, this research has gathered substantial evidence to identify the most relevant theories related to human behaviour in the context information security in supply chain.

It is crucial to recognize that solely investing in and prioritizing the technical aspects of information security in the supply chain while neglecting the human factor will inevitably result in ineffective performance within the supply chain. Consequently, this thesis will integrate three theories—GDT, SBT, and TPB—along with the incorporation of control mechanisms such as top management support, reward systems, and monitoring/evaluation. Based on this integration, a framework will be developed to guide the subsequent steps in empirical studies.

3.2 Theories and Control Mechanisms Underpinning the Study

The study proposes a framework to address information security threats within the supply chain by focusing on human factors, particularly human behaviour. It acknowledges that insiders (employees) are the source of these threats, which is consistent with expert opinions (Safa et al., 2018; Humaidi and Balakrishnan, 2015). This study aims mitigate information security threats in the supply chain by using a novel approach which emphasizes behavioural solutions for employee and organizational issues (Ifinedo, 2014; Ifinedo, 2012). This approach aligns with previous studies that examined employee behaviour in handling information systems within their respective organizations and investigated human behaviour in the context of information security threats (Sulaiman et al., 2022; Merhi and Ahluwalia, 2019; Chen et al., 2018; Alshare et al., 2018; Sli et al., 2017; Chou and Chou, 2016; Tsai et al., 2016; Warkentin et al., 2016; Boss et al., 2015; Posey et al., 2015).

The purpose of this study was to explore methods of influencing employees' attitudes and mindsets to prevent misconduct in the field of information security within the supply chain. To achieve this, the researchers combined the General Deterrence Theory and the Social Bond Theory. Additionally, the Theory of Planned behaviour (TPB) was utilised to understand how emotional factors impact employee behaviour. The study identified various control mechanisms such as top management support, rewards,

monitoring, and evaluation, which could shape employees' attitudes towards minimizing threats in the supply chain.

The author emphasizes that the integration of these theories and an extensive literature review enhances the reliability of the research model. The General Deterrence Theory, Social Bond Theory, and the Theory of Planned Behaviour are aligned with each other and collectively contribute to influencing individuals' attitudes. By incorporating these theories, the study provides a comprehensive framework for understanding behaviour change and improving employees' information behaviour to mitigate information security risks in the supply chain. While these theories have been widely employed to explain human behaviour in the domain of information security, their application within the supply chain context has been limited. Thus, these three theories serve as the foundational basis for this study. In the subsequent sections, a conceptual framework for factors mitigating information security threats in the supply chain will be discussed.

3.3 Research Model and Hypotheses

Abbott and McKinney (2012) explain that social research is crucial for making generalisations about the social environment based on theory and data, rather than relying solely on personal views or experiences. Social research involves a dynamic interaction between ideas and facts, which forms the basis of every social science. Theories serve as the foundation of social science by providing a framework for understanding the relationships between different factors. These theories make assumptions about the nature of social phenomena and offer general explanations for various social behaviours under specific social conditions (Abbott and McKinney, 2012).

In contrast, hypotheses are proposed explanations for specific phenomena. They are derived from theories and establish relationships between two or more concepts, which can be empirically tested (Abbott and McKinney, 2012). Hypotheses specify how these concepts are expected to interact and work together. For example, in this study, the theory will be used to link concepts such as sanction severity (from the General Deterrence Theory) and attitude (from the Theory of Planned Behaviour) to examine their role in mitigating information security threats within the supply chain. These relationships will be tested in Chapter 5, along with other constructs.

To facilitate the testing of the proposed framework, the study formulated specific objectives and research questions.

- **Objective 1:** To critically review prevalent threats in information security within supply chain.
- **Objective 2**: To investigate and evaluate human factors that influence the mitigation of information security threats in the supply chain.

- **Objective 3**: To develop and propose an integrated human behaviour model for mitigating information security threats in the supply chain.
- **Objective 4:** To provide recommendations for business owners and managers to enhance and secure information security in supply chain.

The proposed conceptual framework addresses the following overarching research questions:

- How do supply chain employees mitigate information security threats in the supply chain?
- What factors influence employees' information security behaviour in an organisation's supply chain?
- What factors mitigate information security threats in the supply chain?

.

3.4 General Deterrence Theory

The General Deterrence Theory (GDT) was initially developed with the aim of reducing the occurrence of deviant behaviour (Strub, 1990). According to deterrence theory, individuals are generally rational in their actions, and they are less likely to engage in criminal acts if they perceive that the likelihood, severity, and swiftness of sanctions against those acts outweigh the benefits of committing the crime (Dinev et al., 2011). Merhi and Ahluwalia (2019) further explain that human behaviour is based on the assumption that individuals are to some extent rational and can be influenced by the incentives inherent in formal sanctions. This core concept of deterrence theory has been supported by empirical evidence across various disciplines and levels of analysis (Trang and Brendel, 2019).

Hua and Bapna (2013) acknowledge that deterrent approaches and sanctions have an impact on individuals' behaviour, particularly in avoiding specific actions within a company. The effectiveness of such sanctions is contingent on the certainty and severity of the penalties. For instance, if a potential criminal believes that their illegal actions will be detected (certainty of sanctions) and that the authorities will impose harsh punishments such as fines, imprisonment, termination, public denunciation, or other forms of punishment (severity of sanctions), they are likely to refrain from engaging in deviant behaviour (Li et al., 2010).

General Deterrence Theory (GDT) has proven to be a valuable framework for understanding human behaviour about computer crime and intentional abuse (Crosser et al., 2013). GDT explains human behaviour and decision-making by considering the minimization of costs and the maximization of individual benefits (Safa et al., 2019). Organizations may face various negative outcomes such as damaged reputation, compromised competitive advantage, reduced productivity, and financial losses when employees engage in behaviours that pose a threat to the availability, confidentiality, and integrity

of their information assets (Safa et al.,2019). When studying computer crime, the General Deterrence Theory (GDT) has been instrumental in investigating how the perceived certainty of being detected and the severity of punishments act as disincentives or deterrents against engaging in prohibited behaviour (D'Arcy and Herath, 2011).

A review of the existing literature shows that GDT has been widely applied at various levels. Evidence is emerging, however, to suggest that it is equally important to look at GDT at INTSC. This study suggests that sanctions are essential mechanisms in General Deterrence Theory to maintain a balance between organizational goals, activities, and objectives (Cuganesan et al., 2015). GDT has been successfully applied as an efficient approach to ensuring compliance with organizational information security policies (OISP) (Son, 2011). While GDT has been widely applied at various levels, recent evidence suggests its relevance in understanding information security threats within the supply chain. This research utilises GDT to demonstrate how the severity of sanctions influences employees' attitudes, thereby preventing deviant behaviour and mitigating threats in the realm of information security within the supply chain.

The following subsections will delve into the constructs of the General Deterrence Theory (GDT) and Theory of Planned Behaviour (TPB) and explore their relationship in the context of information security threats within the supply chain.

3.4.1 Sanction Severity and Attitude

It is widely acknowledged that deterrence factors exert a negative influence on individuals' propensity to participate in criminal activities. The General Deterrence Theory (GDT) has frequently been utilised to understand human behaviour in various domains. The certainty and severity of punishment play a pivotal role in shaping individuals' mindset and determining their decision to either commit a crime or refrain from engaging in delinquent behaviour (Safa et al., 2019). Moreover, organizational punishments, such as the severity of punishment, have a direct and positive impact on employees' attitudes towards complying with Information Systems Security (ISS) policies (Bulgurcu et al., 2010; D'Arcy et al., 2009). According to Merhi and Ahluwalia (2019), punishment is highly effective in bringing about behavioural changes, and Johnson et al. (2016) suggest that punishments, when appropriately employed, can lead to quicker and more enduring behavioural transformations. Bulgurcu et al. (2010) found that penalties influenced employees' perceptions of the benefits of compliance. However, Moody et al. (2018) discovered no significant impact of penalties on ISS compliance. The use of sanctions can assist in shaping employees' perceptions of positive and negative outcomes (Bulgurcu et al., 2010; D'Arcy et al., 2009). Consistent with previous research in the field, this study proposes that the severity of sanctions acts as a deterrent to discourage employees from engaging in unlawful behaviour. Punishment and penalties serve as forms of sanctions, helping to establish

acceptable attitudes and rules that should be followed. Based on this discussion, the following hypothesis was formulated.

Hypothesis 1a*:* *There is a positive relationship between sanction severity and attitudes in reducing information security threats in the SC.*

3.4.2 Sanction severity and subjective norms

According to Vonai (2013), sanctions are widely regarded as one of the most effective but also criticized approaches to addressing information security risks and issues within organizations. They rely on the concepts of threat, discipline, and fear to enforce compliance with the organization's information security frameworks and processes. Sanction severity has been shown to reduce instances of cyber loafing and misuse of organizational equipment (Henle and Blanchard, 2008). In studies related to Information Security Policy (ISP), sanctions have been examined in various contexts, including both malicious and non-malicious scenarios (Trang and Brendel, 2019). Sanctions are commonly included as a variable in deterrence-based ISP studies (D'Arcy and Herath, 2011) and are also used as control variables in theoretically grounded studies (Siponen and Vance, 2014).

Siponen and Vance (2010) investigated the effects of two factors, sanction certainty and severity, on employees' compliance with Organizational Information Security Policies (OISP). According to Jordan and Myers (2011), punishment should be sufficiently severe to outweigh the benefits derived from engaging in illegal acts. Punishment, when used as a legitimate deterrent, helps differentiate between desirable and undesirable behaviours (Merhi and Ahluwalia, 2019). Strict penalties for specific behaviours communicate to individuals which behaviours are acceptable and unacceptable (Merhi and Ahluwalia, 2019).

Well-defined and widely accepted policies assist in integrating such pronouncements into normatively acceptable behaviour within the group. While some studies suggest the moderation of sanction usage due to potential negative implications for relationships and organizational well-being, it is recognized to have positive outcomes in terms of enhancing subjective norms in information security. Punishments, when used as legitimate deterrents, clearly communicate that certain behaviours are unacceptable to members (Merhi and Ahluwalia, 2019)

Although studies acknowledge the potential negative impact of sanctions, they often recommend their use in situations where information threat severity is high or significant. Sanctions are seen as directly influencing individual behaviour as they pose a significant threat to their functioning and well-being within the organization (Trang and Brendel, 2019; Ologbo et al., 2012). They promote conformity and ensure that actions align with the information security expectations of the supply chain. Scholarly literature largely agrees on the forms and approaches of using sanctions and subjective norms within organizations. These range from the progressive development and monitoring of information security

in the supply chain to providing feedback on deviance or information distortion, as well as the appropriate application of sanctions to avoid bias and the abuse of authority within the organization. Sanctions can be imposed by friends, peer groups, or supervisors, resulting in the loss of respect, and esteem among coworkers, and adverse effects on career opportunities (Trang and Brendel, 2019). It could be argued that sanctions are most effective when supervisors and managers possess the necessary power and authority over subordinates' well-being or job security. They leverage fear and discipline to ensure compliance with established norms and defined parameters within the organization are established. Based on these considerations, the following hypothesis was proposed.

Hypothesis 1b: *There is a positive relationship between sanction severity and subjective in information security threats in the SC.*

3.4.3 Sanction severity and self-efficacy

While sanctions are commonly recognized for their strict impact and ability to moderate behavior, they also have positive effects on individuals' behavior and actions (Trang and Brendel, 2019). Firstly, sanctions are observed to align work values and actions within the organization. Secondly, they emphasize strict compliance with existing work or functional parameters. Thirdly, they ensure quality outcomes through control measures and discipline, driving individual efforts and role performance (Ologbo et al., 2012). Therefore, it can be argued that sanctions foster work features that highlight self-efficacy within functions such as information security.

According to Safa et al.,(2019) sanctions contribute to the development and maintenance of work systems and outcomes that align with the organization's core interests and goals. While sanctions are often viewed as employing threats and fear of repercussions for non-compliance or deviance, they are also crucial in highlighting the importance of studies that link sanctions to attitudes and subjective norms (Hannah and Robertson, 2015; Tsohou et al., 2015; Johnson et al., 2016). This study directly explores the connection between sanctions and self-efficacy in information security threats within the supply chain, suggesting a need for further research. Considering the implications of sanctions on outcomes such as control and strict adherence to established parameters, it is important to examine their implications for self-efficacy. Therefore, this study proposes the following hypothesis:

Hypothesis 1c: *There is a positive relationship between sanction severity and self-efficacy in information security threats in the SC.*

Hypothesis 1d: *There is a positive relationship between sanction severity and information security threats.*

3.5 Social Bond Theory

Social bond theory was initially developed to understand adolescent delinquency. Behaviours such as cigarette smoking, drunk driving, drug abuse, and misbehaviour among juveniles are influenced by their attachment to conventional significant others, commitment to traditional goals, involvement in normal activities, and belief in common value systems (Posey and Lowry, 2015; Vance, Siponen and Pahnila, 2012; Peguero et al., 2011; Mesch, 2009; Booth et al., 2008; Chapple et al., 2005). This theory has gained significant attention from experts in various fields (Safa et al., 2018).

According to Hirschi (1969), a weak or broken social bond in society leads to deviant behaviour due to a lack of social control. Social bond theory suggests that individuals or groups with strong social ties are less likely to engage in deviant behaviour. It focuses on the importance of socialization practices in promoting law-abiding behaviour (Kalu et al., 2020). Lee et al. (2009) found a significant impact of social bond factors on insider computer misuse.

Individuals' attachment to the conventional values of others, commitment to conventional goals, involvement in conventional activities, and belief in standard value systems have been identified as influential factors affecting delinquent behaviour (Lee et al., 2009). Previous studies have also suggested that social bond factors play a significant role in mitigating insider computer abuse within organizations. Social bond factors have been used to explain compliance with organizational information security policies and procedures, as they help reduce the risk of information security threats by promoting adherence to policies and procedures (Ifinedo, 2014; Safa et al., 2016; Cheng et al., 2013; Goo et al., 2014; Jaafar and Ajis, 2013).

3.5.1 Commitment and Attitude

Commitment has attracted significant attention in the fields of management and behavioural sciences due to its predictable outcomes. It is believed that commitment entails a sense of responsibility towards the organization one works for, including a willingness to exert effort for the company (AlHogail, 2015). According to Safa et al., (2018) commitment can be described as a set of internal thoughts and feelings. Ifinedo (2014) defines commitment as a strong belief in and acceptance of duty, which is essential for understanding employee work and behaviour.

Numerous studies have demonstrated that an organization's success greatly relies on the dedication of its employees (Safa et al., 2016; Ifinedo, 2014;). Highly committed employees align themselves with the organization's goals and values, possess a strong desire to belong to the organization, and exhibit higher levels of organizational citizenship behaviour. Employees play a central role in information security as they directly interact with sensitive information. Their commitment and responsibility to protect information assets are crucial in this domain (AlHogail, 2015). Commitment is associated with

the desire to attain a prestigious job, where personal achievement and reputation are vital for committed individuals (Cheng et al., 2013). Committed employees invest more time and energy into achieving career success (Cheng et al., 2013; Safa et al., 2018). Additionally, committed individuals are less likely to take risks that could jeopardize their career aspirations by violating rules (Lee et al., 2004; Caputo and Pfleeger, 2012).

Studies have found that expectations, commitment, and beliefs significantly influence employees' intentions to violate information security policy (ISSP) (Cheng et al., 2013). Attitudes towards compliance with information security policies (ISOP) are impacted by employees' commitment to their organizations. Committed employees are less inclined to engage in information security misbehaviour due to the association between commitment and individual attitudes towards ISOP compliance (Safa et al., 2016; Ifinedo, 2014). Ifinedo (2014) demonstrated the influence of social bond factors (Commitment) on employees' attitudes and subsequent intentions to comply with organizational information security policies and procedures. In a similar vein, Safa et al. (2016) outlined how various factors, including information security knowledge sharing, collaboration, intervention, and employees' experience in information security, along with social bond factors, have a positive impact on employees' attitudes and intentions towards complying with information security policies. Additionally, Siponen et al. (2014) conducted a study that revealed the connection between employees' attitudes, intentions, and subsequent behaviour in the realm of information security.

However, there is a lack of research on commitment in the context of supply chain information security threats. Therefore, it is crucial to investigate the phenomenon of commitment in this specific domain. Based on this rationale, this study hypothesizes that commitment influences attitudes towards information security in the supply chain, leading to a reduction in information security threats. Thus, the following hypothesis is proposed.

Hypothesis 3a*: There is a positive relationship between commitment and attitudes toward information security threats in the SC.*

3.5.2 Commitment and Subjective Norm

Commitment is a crucial factor for achieving success and desired outcomes in various functions, including information security. It involves dedication, attachment to goals and services, and a comprehensive understanding of the intricacies and processes of information security. Skotnes (2015) noted that commitment to information security provides operational assurance and reduces the occurrence of high-risk events. Similarly, Cheng et al. (2013) emphasized the importance of involvement in ensuring focus and adherence to information security policies and practices. Safa et al. (2016) argued that actions and behaviours reflecting emotional attachment and involvement in information security operations and functions promote compliance at different levels and units within an organization, not just at the top management level.

While there is a scarcity of empirical research specifically focusing on commitment and information security, existing studies often highlight commitment in terms of increased emotional attachment and dedication (Skotnes, 2015). Cheng et al. (2013) discussed the positive implications of commitment for enhancing the resilience and effectiveness of information security systems. Commitment fosters members' receptiveness to the organization's values and policies, facilitating collaboration and operation within well-defined boundaries and operational frameworks in the realm of information security. Individuals' actions are influenced by the expectations they perceive in their environment (Knapp et al., 2006). In the context of information security threats in the supply chain, employees are more likely to mitigate threats if they observe compliance and adherence from their superiors, peers, and subordinates. The compliance of significant others in the workplace, such as immediate superiors, co-workers, and the organization as a whole, plays a crucial role in reducing the likelihood of engaging in antisocial activities, as suggested by the social bond theory (Hirschi, 1969).

Bulgurcu et al. (2010) and Herath and Rao (2009) found that subjective norms significantly influence compliance with information security policies in organizations. Furthermore, Ifinedo (2014) highlighted the positive impact of commitment on subjective norms. Lee and Larsen, (2009) discovered a positive correlation between environmental commitment and subjective norms related to well-being. Prominent individuals including parents, friends, teachers, and educational institutions hold significance in an individual's life. Similarly, in the workplace, immediate supervisors, colleagues, the job itself, and the organization can be considered as important figures. According to the social bond theory, establishing strong connections with these individuals decreases the probability of engaging in antisocial behaviour. Based on the existing research, commitment and subjective norms have significant implications in the field of information security in supply chain. Hence, the following hypothesis is proposed:

Hypothesis 2b: *There is a positive relationship between commitment and subjective norms in information security threats in the SC.*

3.5.3 Commitment and Self-efficacy

According to Safa et al. (2016), commitment involves emotional engagement and a sense of responsibility towards the organization. Committed employees are often self-motivated and focused on achieving their goals. Skotnes (2015) suggests that this dedication can lead to sacrificing personal time and investing personal resources in professional development. Although there is a lack of direct research on the relationship between commitment and self-efficacy in information security, studies have indicated a connection between commitment and positive outcomes such as organizational citizenship behaviour, improved performance, and effectiveness (Cheng et al., 2013; Skotnes, 2015; Safa et al., 2016). These findings suggest that commitment encompasses behaviours that contribute to confidence in goal attainment and, consequently, self-efficacy.

Another study by Chesnut and Burley (2015) explains the concept of self-efficacy has become widely studied as a significant factor that is thought to impact the Commitment and exhaustion levels of both pre-service and in-service teachers, as well as student achievement, and their openness to embracing and executing educational reforms. Furthermore, commitment is recognized as a crucial characteristic in employees' attitudes and behaviours towards achieving desired goals. In addition to consistently delivering high-quality work, Moody et al., (2018) note that committed employees demonstrate greater consistency in their behaviours and have confidence in the outcomes of their actions. Users play a fundamental role in the field of information security as key components (AlHogail 2015). Their commitment to protecting valuable information assets is essential for maintaining the overall security of information (AlHogail 2015). Self-efficacy also influences the degree of commitment, as it is demonstrated through the amount of effort individuals put in and how persistent they remain (Rue et al., 2007).

Expanding upon self-efficacy within the realm of information security, Rue et al., (2007) argue that individuals' perceptions of their own competence in safeguarding their information and information systems can shed light on their present security practices and their determination to continue their ongoing effort (Hsu and Chiu 2004). Rue et al., (2007) point out that apart from experience, the perception of having control over information security threats is also anticipated to impact the development of self-efficacy in the field of information security. These observations provide further support for the potential role of commitment as a predictor of self-efficacy in information security. Based on the literature, this study proposes commitment as a possible precursor to the outcome of self-efficacy. Therefore, the following hypothesis is proposed.

Hypothesis 2c*: There is a positive relationship between commitments and self-efficacy in information security threats in the SC.*

Hypothesis 2d: *There is a positive relationship between commitment and information security threats in the SC.*

3.6 Theory of Planned Behaviour (TPB)

The theory of planned behaviour (TPB), proposed by Ajzen (1999), suggests that individual behaviour is influenced by attitude, subjective norms, and perceived behavioural control. TPB has emerged as a highly predictive theory used in diverse studies to forecast individual behaviour. It builds upon the theory of reasoned action (Ajzen, 1991) and focuses on the individual's intention to engage in a specific behaviour. Ajzen (1985) proposed three independent determinants of intentions: attitude, which reflects motivational factors influencing behaviour; subjective norms, which capture the social pressure individuals perceive from important others; and perceived behavioural control, which pertains to individuals' beliefs about their ability to perform the behaviour. TPB has been extensively employed to

investigate individual behaviour and intentions in various contexts (Cavusoglu et al.,2018; Caputo, 2020; Ifinedo, 2014; Ajzen, 1999).

Previous research has established that intention to comply with Information Systems Security Policies (ISSP) is strongly influenced by attitude, subjective norms, and perceived behavioural control (Bulgurcu et al., 2010; Ifinedo, 2012). Subjective norms reflect the social influence exerted on individuals to perform a behaviour and encompass perceptions of what important individuals think. Self-efficacy, drawing from Bandura's (1991) social cognitive theory, represents individuals' belief in their abilities to cope with or carry out the recommended behaviour (Uffen and Breitner, 2013). The theory of planned behaviour (TPB) has been employed in previous studies to explain user behaviour in the context of information systems (Uffen and Breitner, 2013). It has been widely utilized to assess user acceptance of information systems and predict individual behaviour within organizations (Safa et al., 2015).

In this current study, the three components of TPB are described as follows:

a) Attitude: An individual's favourable or unfavourable evaluation of a specific behaviour, specifically related to mitigating information security threats in the supply chain.

b) Subjective norms: Reflects how individuals perceive the opinions and beliefs of their closest friends and colleagues regarding a specific action.

c) Perceived behavioural control: Informed by Bandura's (1991) self-efficacy concept in social cognitive theory, this component refers to individuals' estimation of the difficulty involved in executing or facilitating a particular behaviour.

Hypothesis 3a: *There is a positive relationship between attitudes and information security threats in the SC.*

Attitude, as defined by Bandura (1999), is a psychological tendency that ranges from extremely negative to extremely positive evaluations. It represents an individual's personal evaluative reactions to socially significant matters related to specific items, events, persons, circumstances, or behaviours. This widely used definition highlights attitudes as the positive or negative feelings individuals have towards engaging in a particular behaviour (Susanto et al.,2011). Attitudes can be directed towards various objects, including places, people, events, ideas, or activities, within an individual's perception (Anderson et al., 2017) . Essentially, attitudes reflect an individual's rating or appraisal of an object, which can range from highly positive to highly negative. The study of attitudes has garnered attention from experts in different domains due to its potential to describe and influence individual behaviour (Passafaro, 2020).

Attitudes are also connected to an individual's past and present experiences and can shape their behavioural intentions (Susanto et al.,2011). Additionally, a person's beliefs about an object influence their attitude and subsequently impact their behavioural intentions. Positive attitudes tend to enhance behavioural intentions, while negative attitudes diminish them. Passafaro (2020) emphasizes that attitudes are complex constructs with distinct functioning, and researchers across domains should be mindful of this complexity to avoid complications and biased interpretations of their data.

Employee attitudes towards adhering to corporate information security policies play a critical role in policy compliance in the field of information security (Siponen et al., 2014). Positive attitudes towards an organization's Information Systems Security Policies (ISSP) increase the likelihood of employees conforming to established rules and norms. Conversely, individuals with unfavourable attitudes are less inclined to comply with such policies (Siponen et al., 2010; Ifinedo, 2014). Siponen et al., (2014) research also highlights the relationship between employee attitude, intention, and behaviour in information security. Researchers, including Bulgurcu et al. (2010), propose that an employee's attitude towards information security is influenced by two cognitive-mediated appraisals: threat appraisal (TA) and coping appraisal (CA). Anderson et al., (2017) and Herath and Rao (2009a, 2009b) suggest that employees who recognize potential security risks develop attitudes based on their perceptions of these threats and their coping responses. Furthermore, positive attitudes towards information security are expected to have a beneficial impact on addressing security threats in the supply chain. Building on this understanding, the following hypothesis is proposed:

Hypothesis 3a: *There is a positive relationship between attitude and information security threats in the SC.*

3.6.1 Subjective Norms and information security threats in the supply chain

Subjective norms, as defined by the Theory of Reasoned Action (TRA) and the Theory of Planned Behaviour (TPB), refer to individuals' perceptions of others' attitudes towards a specific behaviour. These norms play a significant role in influencing individual behaviour, as evident in studies related to the Theory of Planned Behaviour and its extensions (Botetzagias et al., 2015). Subjective norms encompass the expectations of endorsement and support from well-known individuals or groups for a particular behaviour, representing the pressure or influence from others to perform or refrain from performing that behaviour (Humaid and Balakrishnan, 2018). Users' perception of other people's thoughts regarding the adoption of proper behaviour shapes subjective norms (Steven et al., 2015). This influence can stem from significant individuals such as top management, friends, and colleagues who encourage employees to engage in specific behaviours related to securing the organization's information assets. While subjective norms generally consider the impact of influential individuals' opinions on individual decisions, this study specifically focuses on the behaviour of superiors, who are leaders within the organization, such as directors, managers, and supervisors.

Subjective norms act as normative stimuli, beliefs, and motivations that drive compliance with a particular behaviour, primarily informed by observing or consulting the behaviours of others (Lanzini and Thogersen, 2014). The behaviour individuals observe as the norm in their environment significantly affects their own behaviour (Warkentin and Johnson, 2010). Attitude and subjective norms have been identified by Ifinedo (2014) as motivators for an employee's intention to perform a certain behaviour. In the context of this study, subjective norms represent the perceived social pressure from others for individuals to behave in a specific manner, ultimately reducing information security threats in the supply chain. Employees within the organization are more likely to comply with instructions and respect their bosses, which can have positive or negative consequences (Humaid and Balakrishnan, 2018). Previous research has indicated that the behaviour of superiors has the most significant impact on employees' information security behaviour (Ifinedo, 2012; Safa et al., 2016). Leaders should exemplify security behaviour and encourage employees to adhere to ISP (Information Security Policy) guidelines (Siponen et al., 2010).

Subjective norms reflect people's attitudes towards specific behaviours, representing what influential individuals think about a particular behavioural pattern (Hutchinson et al., 2008). Employees experience societal pressure, or the lack thereof, based on subjective norms to engage or abstain from certain actions (Cheng et al., 2013). Numerous studies have shown that subjective norms, particularly from department leaders such as supervisors, managers, or coworkers, influence information security knowledge sharing as a competent strategy to enhance awareness and mitigate the risk of data breaches, issues, and policy violations (Cheng et al., 2013; Safa et al., 2018). In the context of ISSP (Information Systems Security Policy) compliance in the workplace, employees are more likely to adhere to the rules if they observe that their superiors, coworkers, and subordinates are doing the same (Chen et al., 2014). Studies by (Pahnila et al., 2007; Bulgurcu et al. 2010; Herath and Rao 2009) have confirmed that subjective norms significantly influence ISSP compliance within organizations. In this study, the behavioural patterns of supervisors, managers, and line managers are expected to positively influence employees, leading to a reduction in information security vulnerabilities within the supply chain. Consequently, subjective norms and supply chain information security threats are anticipated to have a favourable association, forming the basis for the following hypothesis.

Hypothesis 3b*: There is a positive relationship between subjective norms and information security threats in the SC.*

3.6.2 Self-efficacy and information security threats in the supply chain

Self-efficacy, a fundamental component of Bandura's theory of social cognition, is a crucial concept in understanding human behaviour. It refers to an individual's belief in their own ability to achieve desired goals (Bandura, 1986). Self-efficacy entails confidence in effectively planning and executing actions necessary for success. In the context of pro-environmental spillovers, self-efficacy has been identified

as a mechanism that can positively influence behaviour (Lanzini and Thogersen, 2014). It is a powerful tool for impacting behaviour through various processes, including cognition, motivation, emotion, and selection processes (Bandura, 1977).

The construct of self-efficacy determines how individuals feel, think, and what motivates them to behave in certain ways, influenced by cognitive, motivational, affective, social impact, and selection processes (Workman et al., 2008; Johnston and Warkentin, 2008). Self-efficacy strongly influences human behaviour as a self-appraisal of an individual's ability to plan actions based on motivation and cognitive resources (Bandura et al.,1991). It impacts various aspects, such as the type of behaviour individuals engage in, the level of effort and perseverance they exert when facing challenges, and ultimately, their mastery of the demonstrated behaviour. Overall, self-efficacy significantly influences an individual's actions and decisions (Cheng et al., 2020; Tu et al., 2020). Individuals with low self-efficacy lack confidence in their abilities, often approach new responsibilities with reluctance, and may try to avoid challenges altogether, fulfilling their own predictions of failure.

Improving individual self-efficacy can enhance the overall efficacy of an organization since organizations are composed of individuals. Prior research has shown that self-efficacy can influence an organization's efforts to engage in specific behaviours. For instance, individuals with high self-efficacy exhibit greater persistence compared to those with low self-efficacy (Hutchinson et al., 2008). This is supported by Ifinedo (2014), who suggests that individuals with higher self-efficacy regarding information security are more likely to adopt and utilize information security systems in their work compared to those with lower self-efficacy. Self-efficacy influences the level of effort, self-regulation, and initiation of coping efforts when facing problems (Uffen and Breitner,2013). It relates to individuals' capabilities and competence to handle tasks or make choices (Ifinedo, 2014) and has been found to have a significant impact on individuals' ability to accomplish tasks, including information system usage.

A high level of self-efficacy boosts an individual's confidence in their abilities, skills, and motivation. Consequently, they approach actions and activities with enthusiasm and utilize their cognitive resources to complete tasks (Hutchinson et al., 2008Tamjidyamcholo et al., 2013). Belief in the general controllability of information security risks is expected to influence the development of self-efficacy in information security (Steven, 2015). When organizations have a strong sense of self-efficacy for environmental protection and green behaviour, it can motivate them to make additional efforts to maintain these environmentally friendly practices (Lauren et al., 2016).

In the context of this study, self-efficacy is defined as employees' belief in their ability to apply and adhere to measures that reduce information security threats in the supply chain. This is supported by the finding that information security threats have a favourable and significant impact on employees' self-efficacy (Humaid and Balakrishnan, 2018). Self-efficacy encompasses not only the proper

application of security countermeasures, but also security-conscious behaviours related to computer and internet use. Based on the discussion, the following hypothesis is proposed:

Hypothesis 3c: *There is a positive relationship between self-efficacy and information security threats in the SC.*

3.7 Top management support and Attitude

Leadership's impact on shaping perceptions and beliefs within organizations is widely acknowledged (Wang et al., 2011). In the realm of information security, the significant influence of top management on employee behaviour has garnered considerable attention in the literature (Siponen and Puhakainen, 2010; Wang et al., 2011; Barton et al., 2015; Cuganesan et al., 2018). Previous studies have primarily focused on employees and their justifiable role in information security (Peng et al.,2021). Research has shown that top management support contributes to the successful implementation of information systems by demonstrating an understanding of the importance of information technology and information security, possessing adequate knowledge, and actively engaging in IT-related activities (Stemburger et al., 2011; Hu et al., 2012). While senior management support has been proposed as a significant influence on information security perceptions, beliefs, and attitudes in organizational research (Hu et al., 2012), its implications have not been extensively tested through experimental studies.

To ensure the effectiveness of information system security and create a secure environment for handling information, comprehensive management support is indispensable in any organization (Hu et al., 2012; Barton 2015). Such support is expected to foster confidence and reliance not only in the functionality of information security but also in the human aspects involved. Tepe and Tepe (2015) reinforce this viewpoint by asserting that top management should establish functional frameworks that enable the interconnected functionality of security systems and enhance their robustness across various organizational platforms. Therefore, it becomes apparent that apart from overseeing and regulating information security measures, top management is also responsible for motivating and enhancing self-efficacy in information security.

Although Young and Windsor (2010) advocate for the involvement of relevant top management in information security planning, there is limited actual evidence to substantiate the claims made in these studies. Puhakainen and Siponen (2010) stand out as one of the few studies that utilize empirical data to examine the role of top management and organizational cultures in information security. Only a handful of empirical research studies have explored the relationship between senior management support and information security attitudes, and the results have been mixed. In an action research study, Puhakainen and Siponen (2010) discovered that visible top management support, demonstrated through actively promoting information security and leading by example with their compliance behaviour,

influenced employee information security attitudes and was deemed necessary for employee information security policy compliance.

Hu et al. (2012), on the other hand, found no link between senior management involvement in information security activities and employee perceptions. Flores and Ekstedt (2016) found no significant link between these constructs in a more recent investigation. Furthermore, just one study looks at the direct effects of senior management on information security norms and attitude and finds evidence of a favourable relationship (Peng et al.,2021). From the perspective of employees, Hu et al. (2012) utilised top management participation (TMP) as the most direct indicator of top management's involvement in the organisation's information security-related concerns. Employees' beliefs, norms and attitudes about new programmes, initiatives or rules can be shaped by senior management. These projects, programmes and policies are given legitimacy by top management. Senior management support can empower employees to modify how they handle information security by signalling the importance of information security to the rest of the organisation (Karlsson et al.,2017; Flores and Ekstedt, 2016).

Senior management holds significant influence over all aspects of corporate activities and bears primary responsibility for them (Soomro et al., 2016). As information security is fundamentally a management and business issue, senior executives should be aware of the necessity to develop and implement information security policies and give due attention to the proper implementation of predetermined security controls (Soomro et al., 2016). In addition to formulating an information security strategy, the successful execution of the process heavily relies on the involvement of senior management.

The findings of Puhakainen and Siponen (2010), which establish a connection between senior management support and attitudes, need to be contextualized as they were obtained in a small business setting. On the other hand, Cuganesan et al., (2018) provide empirical evidence supporting the notion that senior management can directly influence employee attitudes toward information security, particularly in larger enterprises. According to Hu et al. (2012), contingent factors such as organizational structure and leadership style may impact the relationship between senior management and attitudes. In the case of LEA's operational challenges, the organization is known for its stable leadership structures, with senior managers often possessing frontline experience and expertise. Instead of the trickle-down effects observed in previous studies, the actions of organizational leaders are likely to directly impact employees' information security attitudes and behaviours (Hu et al., 2012). Understanding the role of senior executives in information security is crucial (Puhakainen and Siponen, 2010; Hu et al., 2012).

This study proposes that top management support can influence information security threats in the supply chain and contribute to their mitigation. Furthermore, important evidence was discovered to substantiate this claim. The findings of Hu et al., (2012) demonstrate that senior management's beliefs

regarding information security have an impact on their involvement in protecting information assets and ensuring information security. Therefore, it can be concluded that top management support enhances their engagement in information security. Considering these studies and drawing from previous research in the field of information security, one can observe a lack of comprehensive research on information security threats in the supply chain. Overall, the existing evidence on the effects of senior management support on information security attitudes and subjective norms is either conflicting or limited. The study hypothesizes that there exists a positive relationship between top management and attitudes towards information security threats in the supply chain.

Hypothesis 4a: *There is a positive relationship between Top management support and attitudes in information security threats in the SC.*

3.7.1 Top management support and Subjective norm

Subjective norms encompass the perception of approval and support from influential individuals or groups towards specific behaviours. They represent the perceived social pressure to either engage in or abstain from certain actions. This construct considers the impact of the opinions held by significant individuals on individual decision-making (Johnston and Warkentin 2010). In the context of information security, top management aims to encourage employees to adopt specific behaviours that ensure the protection of the organization's information assets. Subjective norms play a role in shaping an individual's intention to engage in a particular action.

Ifinedo (2014) stated that an employee's intention could be motivated by attitude and subjective norms. Subjective norms determine perceived social pressure from others for an individual to behave in a particular manner. Their motivation is to reduce information security threats in the supply chain with those people in view. Subjective norms are inputs, attitudes and incentives to perform a specific act that are mostly based on consultation or observation of others' behaviours (Vance et al., 2017). It has been examined how what an individual perceives to be the norms in his or her environment influence or motivate his or her behaviour (Johnson and Warkentin 2010).

Subjective norms are the result of people's attitudes about specific behaviours. In other words, it refers to what influential individuals think about a particular behaviour pattern. According to subjective norms, employees are under societal pressure to act, or not act (Cheng et al. 2013). The strength comes from department leaders, supervisors, managers, or even co-workers who see information security knowledge sharing as an active and beneficial strategy to raising information security awareness and reducing the risk of data breaches, threats and policy violations. As a result, the following hypothesis has been proposed:

Hypothesis 4b*: There is a positive relationship between Top management support and subjective norms in information security threats in the SC.*

3.7.2 Top management support and self-efficacy

In their research, Pattinson et al. (2015) emphasized the significant role of top management in determining performance outcomes and organizational functions. They highlighted that the responsibility for control and direction lies solely with top management. However, in the context of information security, senior management is expected to go beyond mere control and direction by fostering operational frameworks that instil confidence and reliability, not only in the functionality of information security systems but also in the human aspects involved. Tepe and Tepe (2015) support this perspective by asserting that top management should design functional frameworks that facilitate the interdependent functioning of security systems and ensure the robustness of operations across various organizational platforms. This indicates that top management is not only responsible for overseeing information security measures but also for motivating and enhancing self-efficacy in information security among employees.

The relevance of senior management support has also been established in empirical investigations. Johnson and Warkentin (2008) used TPB and the technology acceptance model to determine healthcare professionals' compliance with the Health Insurance Portability and Accountability Act (HIPAA) in The States. The findings revealed that both organisational support and SE influenced healthcare professionals' compliance intention behaviour. Brady (2011) discovered that top management was a major predictor of healthcare professionals' HIPAA security behaviour in the States.

A key factor identified in several studies (Zinn, 2013; De Meulemeester, 2013; Bronstein and Tzivian, 2013) as a major predictor of healthcare professionals' HIPAA security behaviour in the United States is competency, particularly in terms of training and development. This perspective aligns with the earlier viewpoint of Tepe and Tepe (2015), which emphasizes the crucial role of top management in the training and development of subordinates and users of information security systems. Sun et al., (2016) suggest that top management plays a significant role in determining the content and consistency of training programs based on the organization's information security goals and the skill levels and demographic characteristics of the users. The research conducted by Bronstein and Tzivian (2013) further supports the link between competency and self-efficacy, highlighting the strategic initiatives implemented by top management to drive self-efficacy in information security functions within the organization. Overall, these findings underscore the importance of top management in shaping self-efficacy outcomes in information security and demonstrate a strong consensus among studies in this area.

In this study, self-efficacy (SE) was defined as an individual's perception of their capability to safeguard information and mitigate threats. Enhancing SE can be achieved through the implementation of information security awareness programs and training initiatives, which aim to educate users about the significance of information system security and enhance their proficiency in utilizing security measures

(Humaidi and Balakrishnan, 2018). As users become more aware of information security, their SE can improve. Based on the findings from this review, there is a strong correlation in research supporting the role of top management in influencing self-efficacy in information security within the supply chain. Consequently, this study proposes the following hypothesis:

Hypothesis 4c*:* *There is a positive relationship between top management support and self-efficacy in information security threats in the SC.*

Hypothesis 4d*:* *There is positive relationship between top management and information security threat.*

3.8 Reward and attitude

Early researchers have described the phenomenon of discouraging offenders from engaging in criminal behaviour as extrinsic motivation, which often influences an individual's behaviour (Safa et al., 2018). In the context of information security, rewards have been identified by IS researchers as a form of extrinsic motivation that impacts offenders' interest in the organization (Bulgurcu et al.,2010). The perception of minimal interest by offender's acts as a deterrent to committing crimes. While sanctions alone may not effectively deter offenders, Chen and Yen (2014) argue that considering benefits is crucial when developing strategies to discourage criminal behaviour. Rewards, according to Skotnes et al. (2015), influence attitudes by emphasizing the environmental constraints that mitigate insider threats. Cheng (2010) study demonstrated that rewards have a significant impact on employees' attitudes towards preventing information security misbehaviour.

Bulgurcu et al. (2010) found that the use of rewards shapes employees' attitudes towards information security, and Safa et al. (2018) revealed a negative attitude towards information security misbehaviour and perceived behavioural control. However, there is limited empirical evidence regarding the influence of rewards on information security threats in the supply chain. Despite this gap, the existing literature provides a solid foundation for understanding how rewards may also affect employee behaviour in the context of information security threats in the supply chain. Furthermore, the provision of rewards as incentives has been widely recognized as a significant strategy for modifying behaviour in various fields, including education, organizational behaviour, and psychology.

Moreover, based on the research by Safa et al. (2018) and the findings of Cuganesan et al. (2018), it is suggested that rewards have a positive effect on mitigating insider threats. However, Cuganesan et al. (2018) found no significant impact of rewards on attitude. Considering this, the present study posits that employees will be more inclined to engage and contribute to information security in the supply chain if they perceive a reward system in place. Consequently, it is hypothesized that rewards have a positive influence on employees' attitudes. Based on the discussion, the following hypothesised was proposed:

Hypothesis 5a: *There is a positive relationship between rewards and attitudes in information security threat in the SC.*

3.8.1 Reward and subjective norms

The strategy of implementing rewards aims to create work environments and frameworks that prioritize the perceived benefits of engaging in secure practices. According to Son (2011), this process often involves structuring work and operations in a way that emphasizes information control and monitoring of data access. These actions are bound by certain parameters that become the norm for organizational members. Soomro et al., (2016) argue that rewards not only help management regulate employees' behaviour and approaches to work, but they are also supported by information security policies and regulations, which shape the organization's belief system and values. As a result, rewards can influence workers' behaviour and actions. Recent research has highlighted the potential role of incentives in promoting compliance and mitigating negative behaviours in information security. Although the practice of rewarding compliance and mitigating actions may not be widespread, scholars have discussed the potential of incentives in encouraging desirable behaviours in the context of information security (Booth, 2008; Pahnila et al., 2007; Safa et al., 2019).

Consequently, actions related to rewards can be seen as a deterrent to information security threats and crime. By offering rewards, potential threat situations are diffused, discouraging individuals from engaging in criminal activities or accessing sensitive information and data (Cuganesan et al.,2018; Hirschi and Stark ,1969). This indicates that rewards not only influence the perceptions of workers and members involved in information security functions throughout the organization but also shape their behaviour to align with the overall expectations of information security. Thus, there appears to be a potential relationship between rewards and subjective norms in the context of information security in the supply chain. Based on this discussion, the following hypothesis is proposed for further investigation.

Hypothesis 5b*:* *There is a positive relationship between reward and subjective norms in information security threats in SC.*

3.8.2 Reward and Self-efficacy

Rewards encompass both tangible and intangible benefits, including monetary and non-monetary incentives, provided by employers to employees as a means of encouraging compliance with the information security policy (ISP) (Bulgurcu et al., 2010). These rewards can take various forms such as promotions, salary increases, tangible or intangible rewards, recognition through verbal or written evaluations, reputation enhancement, or a combination of these elements. As mentioned earlier, the practice of rewarding not only aims to control information and shape perceptions but also involves creating work environments that emphasize adherence to ethical practices and actions. Ologbo et al. (2012) emphasize the importance of ethics and employee support in fostering trust and strong relationships between management and subordinates, which are crucial for enhancing employees' belief in themselves and their ability to perform their responsibilities effectively. According to Hu et al.,

(2012) the implications of rewards extend beyond their primary goal of preventing crime and deviant behaviour they also contribute to improving compliance and fostering self-efficacy in information security. Additionally, there is a recognized link between the control of employees' competency in information security, particularly in regulating information access, and outcomes such as self-reliance and self-efficacy.

The reward process encompasses a range of actions aimed at upholding confidentiality and control, as highlighted by Tsohou et al., (2015). This reinforces the viewpoint of Shemberger (2011), who emphasized that while many organizational functions can be easily specified and outsourced, information security remains a highly sensitive and integral aspect of the organization. The imperative for control and the need to minimize perceptions of benefit or reward in engaging in illicit activities necessitate the establishment of streamlined activities and the regulation of individuals with access to the relevant information. Consequently, this builds a controlled environment and framework for employees who interact with and have access to the information or data of significance, thereby fostering their self-efficacy in fulfilling their roles and responsibilities within the context of information security in the supply chain. Thus, a correlation exists between rewards and self-efficacy. Hence, the following hypothesis was proposed:

Hypothesis 5c*:* *There is positive relationship between reward and self-efficacy in information security threats in the SC.*

Hypothesis 5d*: There is positive relationship between reward and information security threats in the SC.*

3.9 Monitoring /Evaluation and attitude

The literature clearly highlights the significance of monitoring and evaluating information security, as evidenced by studies conducted by (Cuganesan et al. 2018; Moussa 2016; Humaidi and Balakrishnan,2015;Belcourt et al. 2008) A comprehensive review of existing literature indicates that this construct can have a positive impact on employee behaviour within the workplace, as demonstrated by Vance et al. (2012), Moussa (2015), and Cuganesan et al. (2018). Monitoring and evaluating employee performance in relation to information security have the potential to influence attitudes, subjective norms, and self-efficacy. Belcourt et al. (2008) found that employee monitoring and evaluation serve various purposes, including preventing inappropriate behaviour, optimizing the organization's time management, curbing employee gossip, blocking access to illicit websites, and safeguarding employees' personal information against potential misuse by hackers. Additionally, some employees may misuse company computers for personal purposes such as gambling, engaging in private enterprises, playing computer games, or pursuing personal matters. As a result, many employers are adopting a stronger and more proactive regulatory approach (Moussa, 2016). Monitoring systems can be employed to gather, process, and provide performance feedback on employees' work, assisting

managers in achieving performance improvement objectives and facilitating employee development. Monitoring practices have evolved beyond traditional methods such as monitoring phone calls and emails. Location monitoring, as observed by Dessler (2011), has become widespread, involving the tracking of employees' movements and whereabouts, especially when they work remotely from their supervisors, such as at home, hotels, or coffee shops, as noted by Dubrin (2009). Employee monitoring is driven by various reasons, including the potential legal liability of employers for the content of employees' emails to colleagues and external parties, as highlighted by Holdworth et al., (2019) also identify motivations such as hiring the best personnel and safeguarding company resources from misuse or mishandling. However, monitoring alone is insufficient to address insider threats, as it can capture the purpose but not the motive behind employee actions, making it challenging to identify patterns of misuse (Humaidi and Balakrishnan,2015)

In practice, monitoring techniques are used to direct employees towards positive outcomes and deter undesirable ones. This approach focuses on measurable aspects of performance (Merchant and Van Der Stede, 2007), placing the responsibility on employees to meet or exceed expectations in those areas. Therefore, monitoring and assessment often go hand in hand (Vance et al., 2012). In the realm of information security, employee monitoring is employed to detect breaches, address issues, ensure compliance, and promote effective information management practices, emphasizing the importance of security and defining employees' expected roles (Boss et al., 2009; Chen et al., 2015). This process not only fosters a sense of responsibility and accountability among employees (Vance et al., 2012), but it is also expected to positively influence subjective norms and attitudes towards information security (Da Veiga, 2016). By receiving feedback and being educated about information security requirements and practices through monitoring, employees can improve their understanding and compliance (Da Veiga and Martins, 2015).

Until now, information security research has primarily focused on formal awareness programs and monitoring of security breaches as strategies to influence attitudes, self-efficacy beliefs, and ultimately behaviour related to information security (Goo et al.,2014; Chen, 2013). These approaches enable individuals to assess their current situation and make necessary improvements (Boss et al., 2009). Evaluation, which is similar to monitoring, follows a comparable process. However, while monitoring primarily tracks ongoing processes, evaluation occurs at key stages and involves assessing outcomes against established standards (Siponen et al., 2012). Both processes are typically conducted simultaneously, with monitoring daily activities and processes consistently, while evaluation takes place at phase transitions to anticipate the need for system, function, or process modifications. Studies byMoussa (2014) and Arcury (2017) concur that the evaluation process shares the same objective as monitoring, which is to ensure compliance and, when actions or behaviours fall short, rectify and correct them.

Agutu (2014) proposed that evaluation serves as a corrective activity to realign any aspects that deviate from the organization's values or agenda. It acts as an effective mechanism for enhancing subjective norms by comparing outcomes with established standards. In contrast, monitoring primarily focuses on control, while evaluation is primarily geared towards correcting deviations. This implies that there may be distinct levels and types of impact or relationships with subjective norms for these two constructs. Therefore, further investigation is necessary to understand the unique characteristics of each factor and their roles in influencing subjective norms in information security. This study aims to address this gap by highlighting previous research that suggests the distinctiveness of these constructs and exploring the potential link between evaluation and subjective norms. The study proposes that the ability to receive feedback and address issues facilitated by monitoring and evaluation is likely to have a positive impact on attitudes, self-efficacy, and subjective norms. Hence, the following hypothesis was proposed.

Hypothesis 6a: *There is a positive relationship between monitoring/evaluation and attitudes in information security threats in the SC.*

3.9.1 Monitoring/Evaluation and subjective norms

Monitoring and evaluation are widely recognized and essential practices in the field of information security. Research suggests that monitoring behaviour and actions serve as a fundamental aspect that drives the progress and advancement of processes within various organizational functions, including information security. Hu et al., (2014) highlights that monitoring provides the necessary checks and balances to ensure that actions and behaviour align with established frameworks and parameters of information security. The monitoring process typically begins with the clear definition or identification of standards or expectations, which serve as the overarching goals of the organization, such as quality, quantity, or speed. Subsequently, it systematically assesses the progress of phases or stages to ensure that all processes adhere to the established standards or expectations (Chen, 2013).

Monitoring is crucial for the organization's success, and when considering its impact on subjective norms, it can be seen as addressing the alignment between observed or obtained outcomes and the envisioned or expected outcomes. In other words, monitoring helps bridge the gap between actual behaviour and the desired behaviour, reinforcing subjective norms within the organization.

According to Boss et al., (2015), monitoring plays a crucial role in concepts such as adaptability, responsiveness, and change. Its primary influence lies in aligning actions and behavior with preferred practices, expectations, and goals, reflecting the ideology of progress and organizational functions. Several studies (Cuganesan et al.,2018; Chen, 2013; Moussa,2016) support the idea that monitoring is responsible for ensuring adherence to specified details and processes, particularly in information security.

Monitoring systems are typically developed to integrate with the functions they oversee, often assessing functionality at intervals before progressing to the next phase. However, monitoring can also be conducted externally, focusing on contextual changes, quality, and efficiency. On the other hand, evaluation shares similarities with monitoring and follows a similar process. While monitoring primarily focuses on tracking ongoing processes, evaluation occurs during stage transitions, assessing outcomes against standards to identify any deviations or mismatches (Siponen et al., 2012). Both processes are usually carried out simultaneously, with monitoring daily activities and processes consistently, while evaluation occurs during phase transitions, guiding modifications to systems, functions, or processes.

Studies by Moussa (2016) indicate that the goal of the evaluation process aligns with that of monitoring, which is to ensure compliance and address shortcomings in actions or behaviour. The evaluation process serves to rectify and correct such actions or behaviour that may deviate from standards, promoting subjective norms within the organization. Ifinedo, (2014) adds that evaluation aims to correct and realign aspects that may be considered outliers with the organization's values or agenda, effectively enhancing subjective norms by comparing outcomes to standards.

Based on the information presented, it could be argued that monitoring is primarily aimed at control, while evaluation activities are primarily focused on correcting deviations. This indicates the possibility of distinct levels and types of impact or relationships with subjective norms, as both constructs have unique conceptualizations. This understanding highlights the importance of further investigations that not only explore the distinctiveness of these factors but also enhance our understanding of how monitoring/evaluation and subjective norms drive outcomes in information security within the supply chain. The current study is designed to address this need by specifically referring to previous research and its insights into the distinctiveness of these constructs. Hence, the study hypothesises as follows:

Hypothesis 6b*:* *There is a positive relationship between monitoring/evaluation and subjective norms in information security threats in the SC.*

3.9.2 Monitoring/Evaluation and self-efficacy

The role of monitoring in fostering self-efficacy is associated with the expectations and obligations placed on different components of the system to perform and meet requirements. According to Kuvaas et al., (2016) self-efficacy is also influenced by motivation, which can be connected to the trust and expectations of others or the system regarding an individual's abilities and actions. Monitoring serves to assess and control for deviations, while also relying on the competence and capability of the involved parties or groups to deliver effectively. Similar to evaluation and performance appraisal, monitoring assigns accountability for outcomes to specific workers, while also evaluating their compliance and expertise in aligning with established standards or functional frameworks (Moussa, 2016). Monitoring

acknowledges the possibility of failure while simultaneously trusting that the process will proceed as intended.

Evaluation, like monitoring, imposes expectations and actions, although it may not be as restrictive or controlling as monitoring. According to Goo et al), evaluation places a demand for responsibility and expertise on workers, thereby potentially emphasizing self-efficacy. When assessing functions, a considerable amount of expertise and self-efficacy is required to meet the expected standards. It is crucial to recognize that in the evaluation process, not only are information security functions or attributes considered, but the competence and capability of technical staff and key personnel are also scrutinized. Consequently, there is a pressing need for improved work outcomes and efficacy (Da Veiga and Martins, 2015; Cuganesan et al., 2018). Thus, a connection exists between monitoring/evaluation and self-efficacy. The relationship between evaluation and behaviour ensures that actions are streamlined, and workers act, behave, and perform in a manner that is satisfactory and aligns with the information security requirements of the organization (Moussa, 2015). While most studies on evaluation, as noted, are often integrated within the framework of monitoring, it is important to conduct distinct assessments of their influence on self-efficacy (Moussa, 2016).

While studies exploring the connection between monitoring and self-efficacy may be limited, theories such as the social bond theory shed light on how individuals exhibit desired behaviour within social contexts (Goo et al., 2014; Jaafar and Ajis, 2013; Safa et al., 2016). In addition to the influence of expectations and responsibilities, which are evident in delegation, responsibilities also signify value and recognition within organizations, providing workers with the opportunity to demonstrate their competence and usefulness in performing their roles or tasks. Thus, self-efficacy can be influenced by both explicit and implicit factors, one of which is the expectations associated with monitoring. Based on this understanding of the potential relationship between monitoring and self-efficacy in information security, the following hypothesis was formulated:

Hypothesis 6c: *There is a positive relationship between monitoring/evaluation and self-efficacy in reducing information security threats in the SC.*

Hypothesis 6d: *There is a positive relationship between monitoring/evaluation and information security threats in the SC.*

Table 3:1 The summary of the hypothesis

H1a	**There is a positive relationship between sanction severity and attitudes toward information security threats in the SC**
H1b	There is a positive relationship between sanction severity and subjective norms in information security threats in the SC
H1c	There is a positive relationship between sanction severity and self-efficacy in information security threats in the SC
H1d	There is a positive relationship between sanction severity and information security threats in the SC
H2a	There is a positive relationship between commitment and attitudes in information security threats in the SC
H2b	There is a positive relationship between commitment and subjective norms in information security threats in the SC
H2c	There is a positive relationship between commitment and self-efficacy in information security threats in the SC
H2d	There is a positive relationship between commitment and information security in the SC
H3a	There is a positive relationship between attitudes and information security threats in the SC
H3b	There is a positive relationship between subjective norms and information security threats in the SC
H3c	There is a positive relationship between self-efficacy and information security threats in the SC
H4a	There is a positive relationship between top management support and attitudes in information security threats in the SC
H4b	There is top management support and subject norms in information security in the SC
H4c	There is a positive relationship between top management support and self-efficacy in reducing information security threats in the SC
H4d	There is a positive relationship between top management support and information security threats in the SC
H5a	There is a positive relationship between reward and attitude in information threats in the SC
H5b	There is a positive relationship between reward and subjective norms in information security threats in the SC
H5c	There is a positive relationship between rewards and self-efficacy in information security threats in the SC
H5d	There is a positive relationship between rewards and information security in the SC
H6a	There is a positive relationship between monitoring/evaluation and attitudes toward information security threats in the SC
H6b	There is a positive relationship between monitoring/evaluation and subjective norms in information security threats in the SC
H6c	There is a positive relationship between monitoring/evaluation and self-efficacy in information security threats in the SC
H6d	There is a positive relationship between monitoring/evaluation and information security threats in the SC

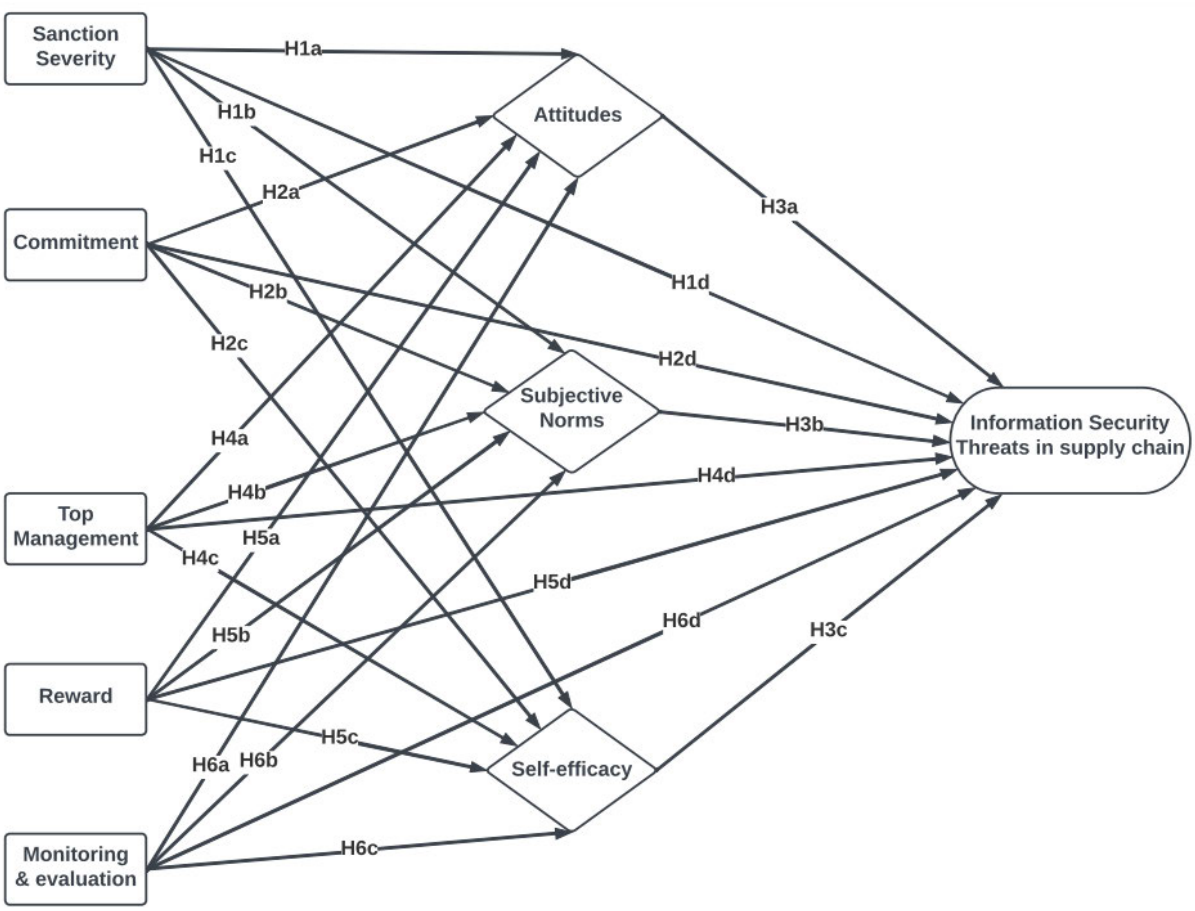


Figure 3.1: Proposed Framework

Table 3.2: Definition and Sources of Constructs

Construct	Definition	Source
Sanction severity	Sanction severity refers to the extent or magnitude of punishment or penalty imposed for a particular violation or misconduct.	Hu et al. (2010)
Commitment	Commitment refers to a psychological state or attitude in which an individual is dedicated, loyal, and deeply invested in a particular goal, cause, relationship, or course of action.	Safa et al. (2018)
Attitude	An individual's appraisal, belief, or opinion about a person, thing, concept, or situation is referred to as their attitude towards that person, object, idea, or circumstance. It is a manifestation of a person's sentiments, ideas, and propensity, all of which influence their actions and reactions.	Safa et al. (2018)
Subjective norms	Subjective norms refer to an individual's perception of social expectations and norms regarding a particular behaviour or action. It encompasses the perceived beliefs about whether important people in one's life (such as family, friends, colleagues, or superiors) would approve or disapprove of engaging in a specific behaviour.	Ahmad et al. (2017)
Self-efficacy	Self-efficacy refers to an individual's belief in their own capability to successfully perform specific tasks or achieve desired outcomes in each situation. It is a person's perceived confidence in their ability to effectively utilize their skills, knowledge, and resources to overcome challenges and accomplish goals.	Malik, Butt and Choi (2015)
Top Management Support	Top management support refers to the endorsement, involvement, and active backing provided by the highest level of management within an organization for protecting information asset and showing by example the importance of reducing threats in the supply chain.	Siponen (2010)
Reward	The term rewards refer to the monetary or non-monetary benefits, either real or intangible, that an employer bestows upon an employee in exchange for the reduction of information security threats in the supply chain.	Bulgurcu et al. (2010)
Monitoring/ Evaluation	Monitoring/evaluation is carried out for the primary purposes of preserving company records, deterring instances of theft, and protecting sensitive information. This emphasises the significance of security and what is expected of workers in terms of breaches, compliance, and effective information management practices.	Chen, Ramamurthy and Wen (2015)

3.10 Summary

This chapter focused on developing the theoretical framework. Based on the three well know theories, an integrated framework and control mechanism was proposed, which consists of six main hypotheses. Under the GDT factor, sanction severity was hypothesised to have a positive impact on attitude, subjective norms and self-efficacy in mitigating information security threats in the supply chain. Next, based on SBT, a commitment was identified as a predictive factor for mitigating information security threats in the supply chain. In addition, TPB attitude, subjective norms and self-efficacy were recognised as the determinant factor. Following are the three constructs from control mechanisms to management support, reward and monitoring/evaluation. Finally, the definition of the constructs was explained in Table 3.2. This chapter has provided the necessary theoretical foundation to answer the research questions. The next chapter focuses on the methodology for collecting data to test the proposed framework.

Chapter 4: Research Methodology

4.1 Introduction

In Chapter 3, the conceptual model for mitigating information security threats in the supply chain was proposed and described. In this chapter, the researcher explains how the current thesis, 'research issues' will be resolved, and the aim and objectives will be achieved. In the prior chapter, a review of the relevant literature and the theoretical framework that will be used for the study was conducted. Based on the study questions and research goals, the purpose of this chapter is to outline the research technique and design that was used in this research. The primary goals of this chapter are to 1) explain the study design, 2) explain the research philosophy, 3) discuss the process of sample selection, 4) explain the instrument design and the technique of data collection, and 5) discuss the statistical methods that were used to analyse the data.

The first part of the chapter provides a concise explanation of the study's goal as well as the context, all of which have a role in determining the research technique that will be used. This chapter goes on to describe, in a more concise manner, why the author chose to use a mixed methods research design for the investigation, as well as the philosophical justification behind their decision. In addition, it gives information on how the quantitative and qualitative stages would ultimately increase the study results in the end. The explanation of research ethics will come after the explanation of the population and the unit of analysis that are going to be focused on. The quantitative and qualitative approaches are then broken down and broken down individually before moving on to an explanation of the sampling strategy, the construction of the survey instrument, the Piloting, the administration of the data collection, the response rate, the validity and reliability, and the data analysis.

4.2 Research philosophy

Research philosophy describes the belief system assumptions that guide researchers 'effort in developing knowledge' (Saunders et al.,2019; Sekaran and Bougie, 2016). Creswell (2014) stated that a researcher's study may be different depending on their philosophical approach, which in turn affects the methodologies used for data collection, analysis and interpretation. Saunders et al. (2019) add that any researcher's research philosophy indicates how they perceive the world and what they believe to be important and useful. The belief systems, assumptions or worldview that leads researchers in developing knowledge are referred to as research philosophy (Sekaran and Bougie, 2016; Saunders et al., 2019). Saunders et al. (2019) believe that phenomenon has to do with important assumptions that researchers make about how they perceive the environment, which informs their study strategy and method of investigation. A research paradigm, in this context, is a conceptual understanding that guides the researcher through the data collecting, analysis and interpretation processes. It enables researchers

to make decisions regarding the most effective and appropriate research methodologies, which will have a direct impact on the findings of their investigations (Creswell and Clark, 2017).

4.2.1 Positivism

Positive thinkers focus on identifying and analysing the variables that affect the results of their research topics since positivism is an objective worldview that is based on the premise that an action can be described as the results or effects of a true cause (Creswell, 2017). Positivism is a deductive method that employs and tests existing theories (Saunders et al., 2019; Creswell, 2017; Bryman and Bell, 2015). Positivism emphasises the use of empirical methods testing hypotheses, and any results must be obtained in an objective manner using a scientific process. Saunders et al. (2019) claim that speculative justifications can be partially or fully proved or refuted, leading to the development of a new hypothesis that could then be evaluated through additional study. In positivism, data and analysis are devoid of the researchers' views and values; hence, data does not change simply because they are observed (Saunders et al., 2019). The researcher will attempt to maintain neutral and separate from the study and data in order to prevent influencing the conclusions. Bryman (2015) stated that paradigm allows researchers to be objective by distancing themselves from their study subjects (research participants) during data collection and analysis.

In addition, several scholars claim that the paradigm typically focuses on hypothesis testing because it assumes there are many facts to learn. As a result, the paradigm suggests that in-depth empirical investigation could reveal the true reality (Creswell, 2014). Therefore, to encourage replication, positivist research is likely to take a systematic approach. Positivism is frequently associated with the use of a logical theory testing technique to investigate research hypotheses.

4.2.2 Interpretivism

Saunders et al. (2016) state that the goal of interpretivism is to acquire data by looking into a social phenomenon in a few ways that could produce different interpretations. According to the paradigm, there is a distinction between human and social agents (Saunders et al., 2016). This implies that there is a difference between how people learn and how things like computers and machines accomplish it (Saunders et al., 2019). Creswell (2014) and Bryman (2015) opine that interpretivism rejects the idea that it can be understood experimentally. As a result, research participants may provide researchers with subjective meanings. Researchers' values and perspectives may be influenced when they attempt to understand a phenomenon by their interpretation, which is influenced by their own experiences (Creswell, 2014). Interpretivist researchers, unlike positivists, do not remove themselves from the research subjects since they communicate directly with them. According to Kivunja and Kuyini (2017), researchers rely onthe participant's perspective of the topic they are studying because reality is socially constructed, and their training and background have a direct impact on their findings. Reality is socially created, researchers rely on the participant's perspective of the phenomenon being studied, and the

researchers' background and experience directly influence any conclusions. Kuyini and Kuyini (2017) make the point that the fact that interpretivist researchers rarely start with theory is another important distinction between positivism and interpretivism. Interpretivism research is thus commonly linked to inductive reasoning. In contrast to positivists, interpretivism researchers often employ a qualitative data collection technique to investigate the phenomenon.

4.2.3 A pragmatic perspective

The nature of research questions and the research aim, present a pragmatic approach to research, establishing the research methodologies and instruments for this study. The researcher in a pragmatic research study first concentrates on the research problem (Creswell and Clark 2017). A pragmatic strategy, according to researchers, focuses on the study problem rather than methodologies and uses a variety of approaches to comprehend the problem. Additionally, Creswell (2017) outlines the basic philosophical assumptions underpinning pragmatic research, on which this study was founded:

- Each researcher is allowed to choose the research approaches, tactics and procedures that best meet their needs and goals.
- Pragmatists reject the idea that there is a single, perfect universe.
- The truth is what is effective at the time.
- Researchers concentrate on the "what and how" of the study.
- Exterior research happens in a range of social, political and other contexts. Pragmatists believed in both an exterior world independent of the mind and an internal universe.

The study of pragmatics provides access to a wide range of practices, viewpoints and presumptions, as well as different methods for gathering and analysing data. The ideas are all pertinent to our investigation. Points 5 and 6 show why, given the complexity and sensitivity of the phenomena under investigation, a pragmatic approach is preferable. By using a variety of data collection techniques, this study also applies assumption number 7. The research design has taken these philosophical presumptions into consideration.

Approaches and techniques for gathering and analysing data to address research problems are known as research methodologies (Saunders et al., 2019). Scientists can select a sample, collect information and develop a solution. Saunders et al., (2016) and Bryman (2015) mention that there are three primary research methodologies typically reported in the literature: qualitative methods, quantitative approaches and mixed methods (Saunders et al., 2016; Bryman, 2015).

4.3 Quantitative Research

Creswell (2014) claims that a positivist philosophy is connected to a quantitative approach. Bryman (2015) and Creswell (2014) maintain that quantitative methods collect precise, numerical data from participants, which can then be statistically analysed to produce the data necessary to find trends in a

large group of participants. It also investigates the link between variables in order to support a specific inquiry or hypothesis. This approach uses deductive reasoning to evaluate hypotheses and available data. Literature reports different terminology with a plethora of classifications and definitions (Saunders et al., 2019). Research strategies are procedures used to answer research questions. Meanwhile, the methodologies given by Saunders and Thornhill (2009) are categorised as research strategies or study designs (Bryman, 2015). Creswell (2012) uses the phrase "inquiry techniques in this study. The classification proposed by Bryman (2015) is preferred for this study because it gives a clear overarching framework for the entire research process.

Therefore, a research strategy is a wide way to carry out social research, according to Bryman (2015). For this, Bryman (2015) outlined a mixed methods study, which combines qualitative and quantitative approaches. The goals of the study and the researcher's philosophical stance have a significant impact on the choice of which of the listed methodologies to employ.

4.3.1 Qualitative Method

Creswell (2014) holds the point that qualitative approaches support interpretivism's position. Interviews, one way of gathering qualitative data, offer more in-depth details about the research topic. Qualitative research is conducted at a micro level and is unstructured and unplanned focusing on individual thoughts and actions to provide a detailed explanation for the phenomena under investigation (Creswell et al., 2012). Zikmund et al. (2014) argue that rich information returns from qualitative methods enable in-depth assessments of market phenomena and the assessment of phenomena that are challenging for statistics to capture. Given the research's goals and philosophical positions, a qualitative approach is the most appropriate strategy for this study. The characteristics illustrate numerous reasons for taking a qualitative approach (Bryman, 2016; Creswell, 2012). This study adopts an interpretive approach to epistemology, concentrating on the participants' statements rather than quantify in the data collected. This change in epistemology contradicts the conventions and practises of natural science as well as positivism's reliance on the quantitative method. Similarly, the ontological perspective used in this study suggests a qualitative approach (Cresswell et al, 2012; Bryman, 2016). A qualitative research strategy has been proposed by Bryman (2016) and Creswell and Clark (2017) as being particularly suitable for inductive research projects. The data will be used in a way that makes it impossible for participants to be recognised as unique individuals, and neither the general public nor any person will be able to relate any of the participant's data.

Given the benefits listed above, a qualitative technique could seem desirable, but it also has some drawbacks that need to be considered when conducting qualitative research. Qualitative data collection takes time, and the findings aren't generalisable because they are only applicable to a particular demographic or context (Creswell, 2017).

4.3.2 Mixed Methods

Mixed-methods research is used to promote a pragmatic perspective as proposed by Creswell (2014). The goal of mixed methods research is to expand the breadth and depth of knowledge about the research problems by combining qualitative and quantitative research approaches within a single study (Creswell, 2014). Almeida, (2018) maintains that the mixed method is such a complicated phenomenon, that it has been depicted in numerous ways in the literature. For example, Sahin and Ozturk (2019) provide 19 definitions of mixed techniques in their study. Based on these definitions, one may argue that the technique entails the use of both qualitative and quantitative approaches in a single study (Sahin and Ozturk, 2019). It enables researchers to combine descriptive data words, images and narratives with empirical data quantitative to get more knowledge for interpreting findings. A single study or research programme of inquiry must use aspects of both qualitative and quantitative studies to address the same research subject in order to be labelled a mixed approach (Sahin and Ozturk, 2019; Molina, 2017). One could argue that not all multi-method research uses mixed methodologies. Studies that commonly blend quantitative and qualitative methodologies do meet the mixed methods requirement.

Sahin and Ozturk (2019) reason that researchers are supposed to benefit by using a mixed techniques method. Researchers can utilise it to handle a larger range of research challenges because they are not limited to a single approach. Molina (2017) asserted that using just one methodology, such as qualitative or quantitative, has drawbacks and that, as a result, the mixed method can be effectively used to get over the drawbacks of each approach. Additionally, by combining and connecting findings, a mixed-method approach enables researchers to draw stronger conclusions.

The main objective of mixed methods research is to incorporate the benefits and drawbacks of each methodology into a single study, producing a better final product that is enhanced by the advantages of the two distinct procedures (Molina, 2017). Queiro et al. (2017) point out that the use of quantitative and qualitative will result in information that incorporates participants' real-life perspectives and experiences while also being generalisable to other participants and circumstances. However, the mixed methods design will only be complete when the findings are mixed, blended or merged at one point in the research (Almeida, 2018). Additionally, it can give data that might otherwise be lost when using a single approach, enhancing the generalisability of study results. In particular, a mixed-mixed strategy is regarded as a useful tool in IS research because it enables researchers to fulfil the objectives, they set out to accomplish and helps to successfully generate comprehensive results that are challenging to obtain using a single method (Queiro et al., 2017).

Triangulation, which checks the study's validity and correctness, is one of the most important criteria for using mixed methods (Fidel, 2008). According to Sahin and Zturk (2018),, triangulation can take four different forms: 1) data triangulation, which requires the use of multiple sources in a study; 2) investigator triangulation, which requires the use of multiple researchers; 3) theory triangulation, which

requires the use of multiple theories to explain a study's findings; and 4) methodological triangulation, which requires the use of multiple methods to investigate a phenomenon. Researchers can achieve a range of goals with a mixed method approach, such as achieving consistency of results through various data collection techniques, testing the consistency of different data sources within the same method, using multiple analysts to check study results, and interpreting data using various theories or perspectives (Almeida, 2018). The strategy benefits researchers greatly since it enables them to generalise their study findings, assists them in spotting differences, inspires them to be more inventive in the way they collect data, and boosts their confidence in their research findings (Queiro et al., 2017).

As Molina (2016) states, a mixed approach is also believed to be effective when researchers are unable to study a phenomenon using a single method entirely. Academics can research subjects in-depth and comprehensively, which is not possible with just one study technique. Additionally, it makes it possible for researchers to develop constructs and hypotheses that would normally be challenging to find or modify from prior research because of a dearth of studies in the area (Sahin and Ozturk, 2019). According to Almeida (2018), a mixed-method researcher can utilise a qualitative exploratory investigation to construct variables and hypotheses solely dependent on earlier studies, and then evaluate the developed hypothesis using a quantitative methodology.

Creswell's (2014) mixed methods research has shown to be a new and prominent trend in research methodologies; nonetheless, researchers must be watchful when selecting the sort of mixed methods research that best suits the study setting. Literature reports numerous mixed methods designs that have been identified based on the weight provided to each component (equal emphasis or one method given the focus) and the order in which they are conducted (whether the two phases are conducted sequentially or simultaneously) (Creswell and Clark, 2017; Creswell, 2014). Convergent parallel or concurrent mixed methods, explanatory sequential mixed methods, and exploratory sequential mixed methods are the most common mixed methods study designs. However, utilising a mixed-method approach has substantial disadvantages. For instance, it is challenging for a single researcher to perform qualitative and quantitative studies as part of a single research project since researchers must learn both methodologies, which takes time and effort. The differences between the three techniques are shown in Table 4.8.

Burgess et al. (2016) raised concern about the dearth of mixed research while describing the results of a thorough literature analysis on supply chain research. A survey of the articles published in one of the A-listed journals, Supply Chain Management, was done to support this concern: An International Journal from 2010 to 2022.Fewer studies were found to have utilised a mixed approach. However, research by Tsai et al. (2021) and Speire et al. (2014) came up in a broader journal search; this collection is by no means comprehensive but rather serves as evidence that supply chain studies have effectively used the mixed methods. The sequential mixed methods approach with a predominating quantitative

survey was used, although Tsai et al. (2021) do not explain or justify why. However, Voss et al. used a qualitative approach at first to evaluate respondents' perceptions of firms, security activities and performance, which led to the construction and administration of the survey. This approach is comparable to the methodology used in this study. As a result, the studies from the literature were applied as a guide when using the methodology of choice.

Table 4.1: Quantitative, Qualitative and Mixed Method Research

Items	Quantitative Research Method	Qualitative Research Method	Mixed Research Method
Philosophical Assumptions	Positivism	Interpretivism	Pragmatism
Characteristics	Deductive, confirmatory, theory/hypothesis testing, standardised data collection, statistical analysis	Inductive, exploratory, theory/hypothesis generation, researcher as the primary instrument of data collection, qualitative analysis	Deductive, inductive, abductive, inclusive, pluralistic and complementary
Research design	Experimental designs Correlation Designs Survey Designs	Narratives Ethnography Phenomenology Grounded Theory Case studies	Convergent Parallel Explanatory Sequential Exploratory Sequential
Focal Point	A systematic empirical investigation of a phenomenon	An in-depth understanding of a phenomenon	On in-depth understanding and systematic empirical investigation of a phenomenon
Aim	To measure and analyse casual relationships between variables	To find patterns and themes	To find patterns and themes and to measure and analyse casual relationships between variables.
Techniques for data collection, analysis and interpretation	Pre-determined Instrument based questions Performance, attitudinal Observation and census data Statistical analysis Statistical interpretation	Emerging methods Open-ended questions Interview observation document and audio-visual data Text and image analysis Themes, pattern interpretation	Both pre-determined and emerging method Open-ended and closed questions Multiple ways to collect quantitative and qualitative data Statistical and text analysis across databases interpretation
Sample size/Structured	Large sample /highly	Small sample/Flexible	Large and small samples/highly flexible
Data representation	In numerical formats	In textual formats	Both numerical and textual formats

4.3.3 Selecting a Research Method and Justification

The type of research questions posed, and the goals and objectives of the study are a few of the aspects that influence the choice of the research methodology to be employed. A mixed method approach can be suggested as more appropriate given these characteristics and the requirement for the investigation. For example, it would be challenging to respond to the type of research question posed using a single method; a) What are the elements that effectively affect employees' behaviour in reducing supply chain information security threats? b) What aspects of the supply chain's information security threats are mitigated? The purpose of this study was to look at supply chain threats' impact on information security. Even so, people are thought to be the weakest link in information security. As a result, this study project used a mixed methodology. In order to determine whether there is a measurable connection between supply chain risks and information security concerns, the study was expanded.

According to Mertens (2019), this type of investigation, whose main goal is to verify and evaluate hypotheses that have already been developed, explaining how and why particular events occur, is suited for quantitative research. The statistical analysis results can be used to describe the patterns in information security that have been seen among the different players in the Nigerian supply chain. It will be beneficial to collect qualitative data in addition to quantitative data, however, given the setting of this study, which is one of only a very small number of studies of its kind ever undertaken, in order to offer new insights and understandings regarding the issues that are being studied. When employing basic language, the research may still be able to gather rich data that may be categorised into a range of different themes that are pertinent to the current study, even though the phrases used in academic language may not be used in real life. Interviews with the management, senior employees and junior staff of the companies provide additional explanation to the outcomes of the quantitative results in light of this objective.

This study will use mixed methods, in which both the quantitative and qualitative data will be collected at the same time, to strengthen the research and support the findings. In Nigeria, a questionnaire survey will be administered to supply chain participants in the manufacturing, logistics, transportation, marketing, production and operation sectors. In-depth interviews with selected participants will be conducted concurrently with the survey questionnaire that was issued to a large group of professionals. The primary goal of interview data collection is to complement quantitative data by supplying in-depth information that will help understand and provide an explanation for the verified correlations between variables. This study employed a mixed-methods approach, it was necessary to select an appropriate research paradigm and research strategy design. These issues are covered in the following sections.

4.3.4 Research Strategy

In a mixed-method approach, selecting research is crucial and calls for considerable thought. The researcher's inquiries are guided by two main research approaches or techniques (Bryman, 2015; Saunders et al., 2015). Researchers use deductive reasoning to create theories or conceptual frameworks, which are subsequently put to the test through research methodologies. Therefore, researchers use this approach to start by conducting some significant literature studies in order to comprehend the topic being examined. Bryman (2015) and Saunders et al. (2015) propose that researchers will next create a framework, decide on the best study methodology, gather and analyse data, and test the framework. Researchers explore the facts first, then develop a theory or framework, which they subsequently apply to the literature, in contrast to deductive methodologies.

Deductive reasoning is used in the research process to go from data to theory, whereas inductive reasoning is used to move from data to theory (Bryman, 2015; Saunders et al., 2016). Data collection and processing typically take longer when using an inductive research method. In contrast, a deductive research approach is frequently seen as being considerably quicker to finish, and the time spent gathering data is typically thought to be shorter (Saunders et al., 2019). On the other hand, an inductive approach has a higher risk because the researcher is concerned about missing out on important data patterns or themes (Saunder et al., 2015). The generalisation of study results is a key contrast between the two approaches. An inductive technique is less concerned with generalisability than a deductive strategy, allowing for the selection of an appropriate sample to generalise the study's findings (Saunders et al., 2019). Additionally, researchers using an inductive methodology are participating in the research process, but researchers using a deductive methodology are not (Bryman, 2015). Finally, the reasoned approach is sequential, in contrast to the inductive technique. According to Bryman (2015), the deductive technique involves reviewing theories (literature review), creating hypotheses, gathering data, analysing and reporting the findings, hypotheses being confirmed or rejected, and revising the theory.

Table 4.2: Difference between Deductive and Inductive Strategies

Deductive Strategy	Inductive
Begin with developing theory or conceptual framework then test with data	Begin with data exploration, then develop a theory or conceptual framework
Moves from theory to data	Moves from to theory
Typically linked with a quantitative approach	Typically linked with a qualitative approach
It is a highly structured and rigid approach	A more flexible structure permits change
It normally takes short time to finish	It takes a longer time to complete
Needs an appropriate size for sample collection	The sample size is not a significant concern
Independence of data collection and analysis by researchers	Involvement of researchers in data collection and analysis
The research process is steady	The research process is monotonous
Generalisation is the aim of the study outcome	Less concern with generalisability

4.3.5 Selecting a Research Strategy and Justification

Both deductive and inductive procedures are applicable because they both include qualitative and quantitative elements. One of the key goals of this study is to put a framework to the test. To do this, the research began with a critical literature assessment, followed by the proposal of a conceptual framework which is required to be tested using a quantitative method. This corresponds to the steps of deductive reasoning (Bryman, 2015). As a result, it might be claimed that both tactics should be combined, resulting in the hybrid or abduction strategy, in which researchers switch back and forth between deductive and inductive reasoning (Venkatesh et al., 2013). The choice of abduction is also in line with the research paradigm. As a result, a hybrid strategy was used for this research.

4.3.6 Research Design

According to Creswell (2014), a pragmatic worldview is strengthened by a mixed-methods research approach. In order to get a more comprehensive and detailed knowledge of the research topics being investigated, it is becoming more common for researchers to combine qualitative and quantitative methods within a single study (Creswell, 2008; Johnson et al., 2007; Tashakkori and Teddlie, 2003). Researchers doing mixed-method research confront several challenging issues, one of the most difficult of which is selecting an acceptable research design (Rocco et al., 2003; Fidel, 2008).When planning a mixed-methods study, it's important to consider things like which methods will be prioritised, in what order data will be collected and analysed, and what steps will be taken to integrate quantitative and qualitative findings (Ivankova et al., 2006). Despite these concerns, it enables researchers to include

descriptive data (such as words, photos and narratives) into their empirical data (Onwuegbuzie and Leech, 2004).

Different mixed methods designs have been discovered and identified based on the level of importance set on every element (either each of them is given equal weight or whether one method is given the dominant emphasis) and the order in which they are implemented (whether the two phases are implemented sequentially or simultaneously) (Rocco et al., 2022;Venkatesh et al., 2013; Creswell and Clark, 2011; Johnson and Onwuegbuzie, 2009; Creswell, 2008; Fidel, 2008). In giving the consideration of mixed method taxonomies (Rocco et al., 2003; Creswell, 2007; John et al., 2007), one might suggest that it would be difficult to choose one of these research design as they are either unnecessary or are made too complicated. Johnson et al. (2007) adds they are too simple and provide little information to guide researchers. However, the taxonomy devised by Leech and Onwuegbuzie (2009) comprises eight research design categories and is based on three factors: mixing dimension (partially mixed or entirely mixed), time dimension (concurrent or sequential) and emphasis dimension (equal status or dominant status). Table 4-3 provides more information about the mixed method design type.

Table 4.3: Mixed method design type

Research design type	**Description**	**Reference**	**Research design type**	**Description**	**Reference**
Confirmatory investigation	Entails the combination of qualitative data and statistical analysis	Rocco et al. (2003)	Exploratory investigation	Quantitative data and statistical analysis	Rocco et al. (2003)
Confirmatory investigation	qualitative data and qualitative analysis	Rocco et al. (2003)	Exploratory investigation	Qualitative data statistical analysis	
Confirmatory investigation	quantitative and qualitative analysis	Rocco et al. (2003)	Exploratory investigation	Quantitative data qualitative analysis	Rocco et al. (2003)
Triangulation design		Creswell (2007)	Embedded design		Creswell (2007)
Explanatory design		Creswell (2007)	Exploratory design		Creswell (2007)
Qualitative dominant	Where the research findings are based purely on the qualitative approach	Johnson et al. (2007)	Partially mixed concurrent equal status design	Quantitative and qualitative phases have approximately equal weight	Leech and Onwuegbuzie (2009)
Equal status	Where the research findings are based on both approaches	Johnson et equal status. (2007)	Partially mixed concurrent dominant status design	Two facets that occur concurrently, such that either facet has the greater emphasis	Leech and Onwuegbuzie (2009)
Quantitative dominant	Where the research findings are based purely on the quantitative approach.	Johnson et al,(2007)	Partially mixed sequential equal status design	The quantitative and qualitative phases having equal weight	Leech and Onwuegbuzie (2009)
Partially mixed sequential dominant status design	The quantitative or qualitative phase has the greater emphasis	Leech and Onwuegbuzie (2009)	Fully mixed concurrent dominant status design	The quantitative and qualitative phases are mixed concurrently at one or more stages or across the components. Both elements are given approximately equal weight	Leech and Onwuegbuzie (2009)
Fully mixed concurrent equal status design	The quantitative and qualitative phases are mixed concurrently at one or more stages or across the components. Both elements are given approximately equal weight	Leech and Onwuegbuzie (2009)	Fully mixed sequential equal status design	This involves conducting a study that mixes qualitative and quantitative research within one or more of, or across the	Leech and Onwuegbuzie (2009)

4.3.7 Selecting a research design justification

The suggestion has been made that researchers in the field of Information Systems (IS) should carefully consider the appropriateness of using a mixed-method approach in their studies (Venkatesh et al., 2013). Generally, the choice of a mixed-method design should be aligned with the research questions, objectives, and content of the study (Venkatesh et al., 2013). According to Creswell (2017), the research design should match the research problem, purpose, and questions. Taking these recommendations into account, it could be argued that selecting the "Fully mixed concurrent equal status design" from Leech and Onwuegbuzie's (2009) framework would be a logical choice for this particular study. This design allows for quantitative research to test and validate existing theories on how and why certain phenomena occur (Johnson and Onwuegbuzie, 2004). The results obtained through statistical analysis can describe the trend of how information security threats in the supply chain are mitigated within the Nigerian context.

However, considering the context of this study where there is a scarcity of such research, it would be valuable to also collect qualitative data to gain additional insights and understanding of the issues being investigated. Using simpler language during interviews with employees in different positions can provide rich information that can be categorized into various themes relevant to the study. In line with this objective, conducting interviews alongside the quantitative research will offer further complementary perspectives to the findings. This research design is also consistent with the selected research strategy of "abduction" and aligns with the majority of IS studies that have adopted a mixed-method approach.

For instance, Venkatesh et al. (2013) examined thirty-one IS articles published between 2001 and 2007 in six IS journals. They discovered that researchers in IS employ mixed methods for several main purposes, including complementarity, completeness, development, expansion, corroboration /confirmation, compensation, and diversity. Further analysis of the revised articles in Venkatesh et al.'s (2013) study revealed that the majority of IS studies used a mixed-method approach primarily for developmental purposes. These studies involved conducting qualitative research to develop constructs and hypotheses, followed by quantitative research to test those hypotheses. In contrast, in this research, the qualitative component complements the quantitative approach. Therefore, it was found that the quantitative approach dominated in the majority of the articles reviewed.

The chosen research design is in line with the 'variable discovery' research design (Zikmund et al.,2014) and the quantitative-dominant mixed-method research design (Johnson et al., 2007). The primary distinction between the convergent parallel or concurrent mixed sequential quantitative dominant design and other similar research designs is that greater emphasis is placed on the quantitative approach. Consequently, the qualitative study is conducted with less rigor compared to the quantitative approach, and the study outcomes primarily rely on the quantitative results (Venkatesh et al., 2013).

To enhance the research and support the findings, this study will utilize a mixed-methods approach, incorporating both quantitative and qualitative data collection concurrently. The selected design is the convergent parallel or concurrent mixed methods, which allows for a comprehensive analysis of the research issues by integrating quantitative and qualitative data to interpret the overall results. A questionnaire survey will be administered to various members of the supply chain, with a specific focus on manufacturing companies. Alongside the survey questionnaires distributed to a large sample, in-depth interviews will be conducted simultaneously with selected participants. The primary objective of collecting interview data is to complement the quantitative data by obtaining detailed information that can aid in understanding and explaining the underlying reasons for the validated relationships between variables.

4.4 The Link between conceptual framework, literature, research design, and method

This section provides a comprehensive overview of the research process, which encompasses six stages: planning, framework development, data collection, data analysis, and discussion and conclusion. These stages are composed of seven main steps. Figure 4.1 visually represents the research process, depicting the input and output for each step. The following explains the details of the steps. When doing research based on evidence or empirical, the initial phase was to explore information security threats in the supply chain. It was the narrowed down to address human factor. An extensive relevant literature on the related topic was processed and the formulation of a research problem was established. The literature review in Section 2.8 pinpoints an applicable research domain and highlights a gap (Human behaviour in the supply chain) in the literature. Furthermore, a conceptual model was created (Section 3.4) which has the integration of three theories and control mechanisms.

However, several research concerns are revealed by the literature study in Section 2.8 which outlines and explains threats in the supply chain (research problem). This reveals a research need and points to a particular field of study. Subsequently, a conceptual model (Section 3.2) was created to describe the proposed empirical research, and empirical studies will be used to examine various features of the model. Based on the requirements of the empirical investigation, a conclusion has been made to utilise mixed methodology in the research design. As shown in Figure 3.1(see chapter 3), a conceptual model is created based on literature analysis to represent the desired empirical investigation. Empirical studies were used to test the framework to stand in for the actual empirical study, with the model's details to be explored by means of these investigations. Figure 4.1 shows how the literature review informs the creation of a conceptual model of the planned research, (validation of mitigation factors)., The model was empirically studied to explore its many components. The researchers opted to use a fully mixed concurrent equal status design from the study of Leech and Onwuegbuzie (2009), since it best fits the requirements of the empirical investigation through the employment of quantitative and qualitative

research methods. The justification for selecting a fully mixed concurrent equal status strategy is given in Section 4.5.

The remaining stages in in Figure 4.1 are to collect data from industries in an understandable and reasonable structure (questionnaire survey and semi-structured interview) After all necessary data has been gathered from companies, explain features and abilities within in research context. The data analysis to the discussion, the contribution of the research and lastly, the conclusion. To ensure that the research will adhere to a predetermined plan and to trace the steps that led to knowledge development. The following sub-sections provide the full details of the work during the procedures.

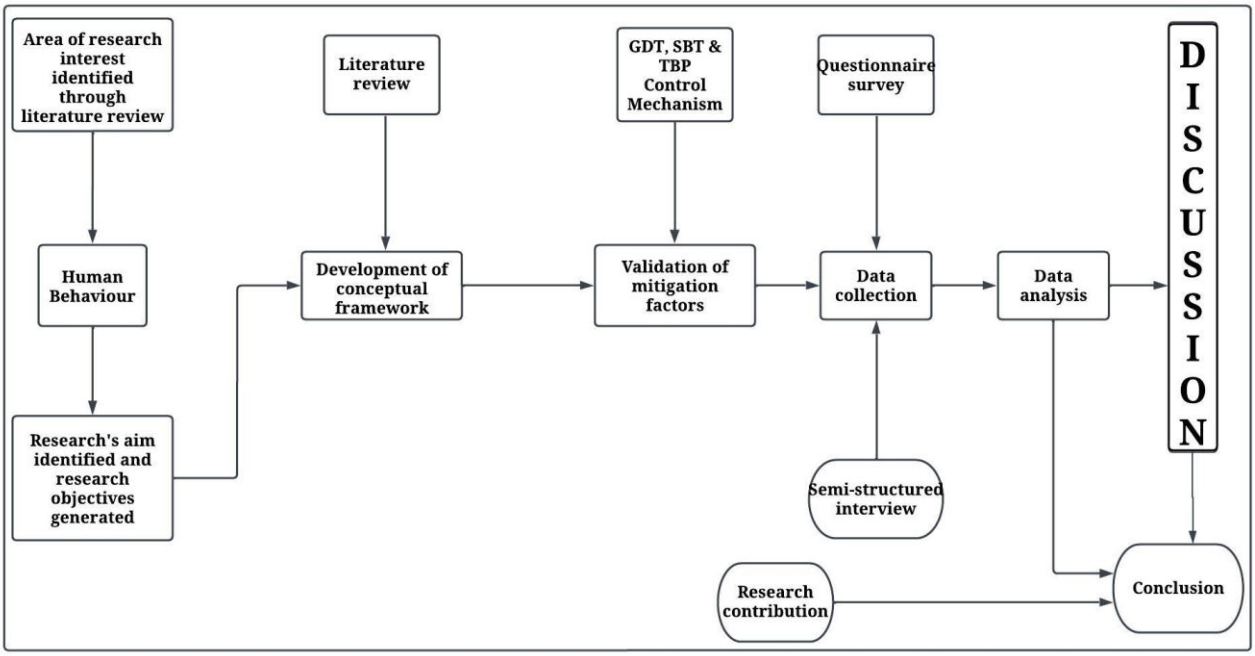


Figure 4.1: Research Process Relationship

4.5 Sampling procedure

Choosing a valid technique of sampling was the next critical stage of the research. Due to cost constraints, it is not feasible to reach out to the whole population or to use an online survey to uniquely identify each member of the population. When conducting online surveys, researchers ensure that their samples are representative of the whole community. May and Perry (2022) state that sampling procedures allow researchers to decrease the quantity of data they acquire by focusing on a smaller subset of instances or elements.

The population is the whole of all persons, businesses, groups or other entities that share the same characteristics and from which a sample is drawn (Creswell, 2017; Saunders et al., 2019). Andy (2018)

notes that while the population can be broadly specific, generic discoveries will have more influence than specific ones. It would be preferable if data could be gathered from every member of the population. Due to limitations in money and time, it is challenging for researchers to reach every individual in the population. To determine the overall trend in the attitudes and behaviours of the entire community, the researcher must utilise sampling to select a subset from the target group.

There are numerous kinds of probability sampling methods, including simple random sample, stratified random sample, cluster sample, and systematic sample (May and Perry 2022). In contrast, non-probability sampling is utilised in research when the sampling frame cannot be determined (May and Perry, 2022). Several techniques for non-probability sampling have been reported in the literature. Included among these are convenience sampling, judgement sampling, and snowball sampling.

Reflecting on the above sampling techniques, non- probability procedure was selected. For some reason, time and cost constraints, the extraordinary difficulty of obtaining probability samples, and the need to investigate a specific sample from a population. Since the objective is to obtain in-depth information about the information security in the supply chain. It is prudent to choose individuals who are believed to provide the most assistance in comprehending the phenomenon (Creswell ,2008; Saunders et al.,2009). This technique satisfies the requirements of this study to acquire in-depth information from a limited number of respondents through interviews snowball sampling, were utilised because they allow researchers to find one participant in the research, conducts the research with that participant and then asks that participant to recommend the next participant who are easily accessible to participate in the interview (Creswell and Creswell 2017; Zikmund et al., 2014; Creswell, 2012). One participant each from 9 companies out of 150 selected made themselves available because most of the respondents changed their minds and declined to be interviewed. In particular, maximum variation sampling was used to select participants that differ on some traits, such as manufacturers, and logistics (Creswell and Clark 2011). The target population of this study comprise majority of manufacturers and it is easy for the researcher to select more manufacturers for interviews. The use of Maximal variation sampling will minimise this bias by avoiding the selection of manufacturers only.

Since the primary purpose of conducting interviews was to gain a deeper understanding of the topic and complement the quantitative data, it was expected that the number of participants for the interviews would be smaller compared to the questionnaire survey. The aim of interviews is to reach a point of saturation, where further interviews are unlikely to provide new information (Creswell et al., 2012). For this study, nine large and medium-sized businesses were selected from the sample frame for the interviews. The selection was based on the size of the business, determined by the total number of employees. Large and medium-sized businesses were chosen as potential interviewees because they were expected to have knowledge about supply chain management and information security, and they

were more likely to invest in human resources rather than solely relying on technology if they had sufficient funding. Small firms may not have provided significant insights for this study.

The survey questionnaire was developed by modifying existing items from the literature to suit the requirements of this research. According to Kline (2015), a sample size of 200 is considered large, while Malterud, Siersma, and Guassora, (2016) defined it as the critical sample size. The collected data set consisted of 520 respondents, which is considered a large sample size according to Kline (2015), exceeds the critical sample size limits defined by Hoe (2008), and meets the minimum recommended sample size of 200 for Structural Equation Modelling (Hair et al., 2017).

Convenience sampling was employed based on prior discussions, and a sample size of 650 employees from 150 companies was selected through the websites of MAN (Manufacturers Association of Nigeria) and the Ministry of Transport and logistics in Nigeria, with the assistance of a key informant. Participation in the study was based on individuals' willingness to participate, and companies with unfavourable time constraints for the researcher were excluded. Careful attention was given to reducing bias and enhancing the response rate.

4.6 Data Collection

The second step, which required collecting data, came once the right method of sampling had been chosen. When collecting data from supply chain manufacturing companies and logistics through convenience sampling, there are a few things that need to be taken into consideration first**.**

Both quantitative and qualitative data were gathered concurrently for this investigation. A sample survey was used to collect quantitative data, and telephone via video calls for interviews were used to gather the qualitative data. A survey design was used as the quantitative data collection method in this investigation. According to Creswell and Creswell (2017), a survey is designed to gather a significant amount of data by examining a sample of the relevant population in order to explain its trends, traits, behaviours, attitudes and opinions. Saunders et al. (2019) add that questionnaires with present questions delivered to a sample of respondents believed to represent the target population are used in survey designs to collect data. The main goal of survey design is to generalise the findings from a sample to the complete population. The best and most economical method for gathering data that offers insight into people's thoughts and attitudes is through surveys. However, it is entirely dependent on how eager people are to respond to these questionnaires. Surveys were administered to representatives of several supply chain member organisations for the current investigation. They serve as a representative sample of the population being studied, and the findings will aid in illuminating the attitudes and behaviours of various supply chain participants toward internal and external information security threats. A cross-sectional survey was conducted. Considering the setting of Nigeria, where electronic and mail surveys

were expected to generate appropriate response rates, the goal was to conduct it by sending email and phone contact to participants. Additionally, direct visitation was used on behalf of the researcher.

The participants were first contacted by phone to extend an invitation to take part in the study. Only individuals who accepted the invitation and agreed to take part in the study that received the questionnaire in a sealed envelope were physically met. In Nigeria, information technology development is progressing at a high standard, and businesses do obtain as many surveys as businesses of other wealthy nations. This suggests that while not all businesses check their emails frequently, those who do might not be persuaded to complete the survey provided by a stranger. The survey may also be completed online, and participants could get an email with an electronic copy of it. All the required paperwork (cover letter, initial invitation letter and information sheet; see Appendices E) was sent to them via email after the initial phone call. The invitation letter contained links to the study and the electronic version of the survey (See Appendix A). Parallel to the survey, semi-structured interviews with corporate representatives were performed. Answering what, why and how questions require the use of qualitative data from interviews (Bryman, 2016). The primary goal of gathering qualitative data is to learn more about the research questions based on the respondents' perceptions and experiences with the topic. This will make it easier for the researcher to explain quantitative data gathered through surveys in detail. The qualitative data will be used by the researcher to illuminate the "why" behind any trends that emerge from the quantitative data.

There are numerous techniques to conduct interviews. Face-to-face interviews by Via (video call) were done for this investigation. The researcher enquired about respondents' interest in participating in an interview when representatives visited the companies to conduct the survey. Depending on the respondent's option, some interviews took place during the visit, and others were held at a later time that the respondent had selected.

4.7 Questionnaire Design (Measures)

According to Saunders et al. (2009), the design of the survey instrument is one of the most important factors to consider when trying to achieve credible results. This is because the design of the survey instrument will influence the response rate, as well as the reliability and validity of the data that is gathered. The reliability of the results will increase with the usage of validated and tried questions. All of the construct-related questions were taken directly from other studies. A self-administered questionnaire with pre-existing scales that were operationalised and peer-reviewed was used to perform the quantitative survey. A 5-point Likert-type scale was used to evaluate these items after they were reworded to suit the research topic better. The survey tool will be displayed in Appendix B. Figure 4.2 illustrates the process of questionnaire development.

Developing Measures

A significant portion of the indicators utilised to gauge the framework's structures came from previously substantiated studies. Measures from earlier studies can be modified to improve the variable's validity and reliability (Ifinedo, 2014). The three indicators rule was utilised to make sure that each construct was measured with at least three indications, as recommended by experts. The indicators used to gauge the framework's structures are discussed in the sections that follow.

4.7.1 Measures of Information Security Threats in the Supply Chain

The supply chain information security threat measures were modified from earlier studies. These indicators are relevant to supply chain participants who are looking into potential threats to their business, including harmless, severe, sabotage, data destruction caused by insiders and outsider, and identification and mitigations of threats. In danger research and information security challenges, the seven items are trustworthy and validated (Cilliers, 2020; Workman et al., 2008; Jouinia et al., 2014). The components used to measure the construct are listed in:

Table 4.4: Indicator used to measure information security threats in the supply chain.

Code	Information security threat in the supply chain	Source
ISS 1	Threat to the information security of my company's supply chain is severe	Workman et al. (2008)
ISS 2	Threats to the information security of my company supply chain are harmless	Workman et al. (2007)
ISS 3	My company involve our supply chain partners in the identification and mitigation of potential supply chain threat	Cilliers (2020)
ISS 4	My company has processes in place to reduce information security threats in our supply chain	Workman et al. (2008)
ISS 5	Active monitoring of information assets by my company reduces information security threats in the supply chain	Workman et al. (2008)
ISS 6	My company has the technical and administrative controls to detect information security threats	Jouinia et al. (2014)
ISS 7	My company involve our customers in identification and mitigation of supply chain threats	Workman et al. (2008)

4.7.2 Measures of General Deterrence Theory (Sanction Severity)

A broad deterrence theory concept, such as sanction of severity, was applied. Items used to measure the sanction severity were modified from earlier studies. Employees' perceptions of the consequences of improperly handling the information asset in their supply chain were represented in the measures for this concept. These could include punishment, penalties, sales or transfers, and a refusal to share information outside the organisation. Studies on information security also modified and validated these (Vance et al., 2012; Safa et al., 2019; Bulgurcu et al., 2010). The items used to measure sanctions are listed in Table 4.8.

Table 4.5: Indicator used to measure General Deterrence Theory

Code	Sanction	Source
SCT 1	I will be punished if I manage my company's supply chain information inappropriately	Bulgurcu et al. (2010)
SCT 2	I will incur penalties if I do not manage information the way the company information demand or expect me to	Bulgurcu et al. (2010)
SCT 3	I think punishment will be severe if I sell or transfer supply chain information outside	Safa et al. (2019)
SCT 4	There will be consequences if I violate the confidentiality of my company's supply chain information	Safa et al. (2019)
SCT 5	My firm defined consequences for supply chain partners who fail to comply with supply chain security procedures	Vance et al. 2020
SCT 6	I prefer not to disclose my company information asset to individuals or third-party companies (suppliers) due to the punishment that may follow	Safa et al. (2019)

4.7.3 Measures of Social Bond Theory (Commitment)

Six items that were modified from previous studies by Cheng et al. and Safa et al. (2018) and Safa et al. (2013). Employee commitment was the key performance indicator for this construct, defined as a firm belief in and acceptance of the company's objectives and values, as well as a readiness to protect the information asset. These indications demonstrated the perception of supply chain workers that reducing information security vulnerabilities in the supply chain will be accomplished by securing, devoting time and effort, showing business concern and refraining from improper behaviour. Studies on information security compliance additionally modified and validated these items (Ifinedo et al., 2014; Cheng et al., 2013). The construct's indicators are displayed in Table 4.6.

Table 4.6: Indicator used to measure Commitment.

Code	Commitment	Source
CMT 1	I am committed to safeguarding organisational information asset	Safa et al. (2018)
CMT 2	I invest my energy and effort to ensure my company information security threats are reduced	Safa et al. (2018)
CMT 3	I am committed to my company's concern about information security threats in the supply chain	Cheng et al. (2013)
CMT 4	I am committed to avoiding any actions that jeopardise supply chain information of my company	Safa et al. (2018)
CMT 5	Employees of my company have a responsible disposition towards proper information security practices	Safa et al. (2018)
CMT 6	Supply chain partners of my firm willingly spend time and effort to reduce information security threats	Safa et al. (2018)

4.7.4 Measures of Theory of Planned Behaviour (Subjective Norms)

Five items that were modified from earlier studies were used to measure subjective norms (Safa et al., 2019; Cuganesan et al., 2018; Safa et al., 2019). The measurements in this construct centre on the workers' perceptions of the importance of people like co-workers, the top manager, line managers and friends in terms of their approval and support for minimising supply chain information security threats. Additionally, studies of compliance behaviour in the information security domain confirmed these measures (Ifinedo, 2014; Cheng et al., 2013) The table used to measure subjective norms is shown in Table 4.10.

Table 4.7: Indicators used to measure subjective norms.

Code	Subjective norms	Source
SJN 1	My company expectations concerning the security of information influence the way my colleagues think I should handle my company information asset	Cuganesan et al. (2018)
SJN 2	Line managers believe that we should protect the information assets of my company's supply chain	Safa et al. (2019)
SJN 3	I am well in line with the expected processes preferred by my supervisors in the security of information in this organisation	Safa et al. (2019)
SJN 4	My friends in my office encourage me to have safe information security actions	Safa et al. (2019)
SJN 5	My colleagues think that we should behave safely to protect the organisational security features	Safa et al. (2019)

4.7.5 Measures of Theory of Planned Behaviour (Attitude)

Four items that were modified from earlier Safa et al. (2019) studies were used to measure attitudes. The measurements for this construct concentrate on the employees' attitudes on lowering information security risks in the supply chain through appropriate, safe and safe information behaviour. Studies on information security additionally modified and evaluated the components (Cuganesan et al., 2018; Bulgurcu et al., 2010). The measurement indicators are displayed in table 4.12.

Table 4.8: Indicators used to measure Attitude

Code	Attitude	Source
ATD 1	Safe information security actions protect information assets in company supply chain	Safa et al. (2019)
ATD 2	Appropriate information security actions help in mitigates the risk of information security threats in my company's supply chain	Safa et al. (2019)
ATD 3	To me, securing information the way my company requires me is valuable	Safa et al. (2019)
ATD 4	Safe information security behaviour decreases information security incidents in my company supply chain	Safa et al. (2019)

4.7.6 Measures of Self-Efficacy

Ifinedo (2014) and Cuganesan et al. (2018) measured self-efficacy using seven items adapted from prior studies. The measures needed for this construct are when a supply chain member focuses on securing information, necessary skills, expertise to protect, and knowledge and control to reduce information security threats in the supply chain. The items were also adapted and validated in the information security domain (Leering et al., 2020; Warkentin and Willson, 2009). Table 4.11 shows the indicators used to measure self-efficacy.

Table 4.9: Indicators used to measure self -efficacy.

Code	Self -efficacy	Source
SE. 1	For me, securing supply chain information the way my company requires and expect me to is difficult	Ifinedo (2014)
SE. 2	I have the expertise to protect my company business and private data	Ifinedo et al.(2014)
SE. 3	I have the necessary skills to secure information the way my company requires and expect me to	Cuganesan et al. (2018)
SE. 4	My company exchanges information with our trading partners electronically	Ifinedo (2014)
SE. 5	I have the necessary knowledge to secure supply chain information the way my company requires and expects me to	Ifinedo (2014)
SE. 6	My company's supply chain partners can provide actionable information needed to respond to information security threats	Cuganesan et al. (2018)
SE. 7	My company can ensure the security of information of supply chain partners in the supply chain	Ifinedo et al. (2014)

4.7.7 Measure of Top Management

Six items developed that were modified from earlier studies by Cuganesan et al. (2018) were used to gauge top management support. The measurement items centre on employees' expectations and attitudes regarding top management support for information security (such as actively supporting information security, security concerns and setting a good example through their own behaviour). Additionally, these criteria evaluated importance, obvious support, interest, actions and words. Additionally, these components were modified and verified in numerous information security investigations (Flores and Ekstedt, 2016; Hu et al., 2012; Puhakainen and Siponen, 2010). The indicators used to measure the construct are shown in Table 11.

Table 4.10: Indicators Used to measure Top management support.

Code	Top management support	Source
TMS 1	Top management in my company is interested in information security threats in the supply chain	Cuganesan et al. (2018)
TMS 2	Evident support for information security goals by top management in my company is clear	Cuganesan et al. (2018)
TMS 3	Top management considers information security in the supply chain an important organisational priority	Cuganesan et al. (2018)
TMS 4	Top management decision on supply chain information security is relevant to supply chain	Cuganesan et al. (2018)
TMS 5	Top management collaborates with supply chain partners to reduce information security threats	Cuganesan et al. (2018)
TMS 6	Top management words and actions in my company demonstrate that information management is a priority	Cuganesan et al. (2018)

4.7.8 Measures of Reward

Three items that were modified from earlier studies by Cuganesan et al. (2018) were used to measure rewards. These measures for this build concentrate on rewarding supply chain participants with wage increases or promotions, personal mentions, or awards for handling information as the business demands. These might aid in reducing the supply chain threat. Studies on information security additionally modified and evaluated the components (Hannah and Robertson, 2015; Tsohou, 2015; Johnston et al., 2015). The indicators used to calculate rewards are displayed in Table 4.7.

Table 4.11: Indicators Used to measure Reward.

Code	Rewards	Source
RWD 1	My pay rises and/or promotions depend on whether I manage supply chain information the way my company requires and/or expects me to	Cuganesan et al. (2018)
RWD 2	I will receive a person mention if I manage supply chain information the way my company requires and/or expects me to	Cuganesan et al. (2018)
RWD 3	I will be given awards for managing supply chain information the way my company's supply chain requires and/or expects me to	Cuganesan et al. (2018)

4.7.9 Measure of Monitoring/Evaluation

The monitoring/evaluation process included seven items to reflect on computer activities, employee behaviour, active monitoring, routine information security tasks and activities. These indicators from both constructs were modified based on earlier research (Cuganesan et al., 2018). Studies encouraging a sense of duty and accountability in information security have also justified these methods (DangPham et al., 2022; Da Veiga and Martins, 2015). The items used to measure monitoring and evaluation are listed in Table 4.9.

Table 4.12: The indicator used to measure monitoring/evaluation.

Code	Monitoring/Evaluation	Source
MNT 1	My company uses security audits to determine if relationships should be maintained with supply chain partners	Cuganesan et al. (2018)
MNT 2	When it comes to information security in supply chain, my company actively monitors the conduct of workers	Cuganesan et al. (2018)
MNT 3	The evaluation of information security behaviour of employees is a regular activity in my company	Cuganesan et al. (2018)
ELT 4	There are many information security tasks which actively monitors the conduct of workers	Cuganesan et al. (2018)
ELT 5	The evaluation of information systems provides my company's supply chain	Cuganesan et al. (2018)
ELT 6	The evaluation of information systems provides my company's supply chain partners with valid information they need to respond to information threats	Cuganesan et al. (2018)
ELT 7	The monitoring of our information systems provides our supply chain partners with the timely information they need to respond to information security threats	Cuganesan et al. (2018)
ELT 8	My company regularly monitors employee computing activities to see how well employees follow information management policies and procedures	Cuganesan et al. (2018)
MNT 9	My firm uses security audits to determine if relationships should be maintained with customers.	Cuganesan et al. (2018)

The survey (Appendix B) was designed in a such a way that it provides anonymous answers so that participants may provide feedback without identifying themselves. The main aim of the questionnaire was to find out the view on mitigating information security threats in the supply chain. Furthermore, according to the developed hypotheses in Chapter 3, the questionnaire was created. In addition, to make it simpler for the participants to respond to the questions a 'Likert Scale' was used throughout the questionnaire. The purpose of each question that was asked was to test the identified variables, measurements and correlations in the framework that was constructed. The questionnaire was divided into two sections, the first question is demographic information about the individual and the company background. The second section contained all the items in GDT, SBT, TPB, Top management, Monitoring/Evaluation, Reward and information security threats in the supply chain. After the questions have been loaded, the next stage is piloting testing.

4.8 Interview question design

Interviews provide new information by integrating the perspectives of the interviewee and the interviewer (Magnusson and Marecek, 2015). Semi-structured face -to face interviews were chosen as a tool to collect data about the sample members' descriptions of how employees mitigate information security, and what are the factors that reduce information security threats in the supply chain. While semi-structured interviews include a list of topics and questions to be covered, the interviewer has the flexibility to change the order and format of the questions as the conversation progresses (Saunders et al.,2009**).** It was recommended to use queries that are straightforward (devoid of academic jargon),

concise and easy to comprehend. The interview queries should be structured so that the 'why' and 'what' questions are addressed before the 'how' questions (Magnusson and Marecek, 2015)

One-on-one interviews with sample members were conducted as part of the qualitative research. This process served as an additional check to complement the survey in this thesis. Malterud,Siersma and Guassora, (2016) add that it was meant to raise the standard and validity of the research. Furthermore, response rates were noticeably high when pre-arranged interviews were conducted with subjects who were regarded as reliable (Malterud, Siersma and Guassora, (2016). However, due to the expense, time constraints and the pandemic (COVID-19) related to interviews, the number of interviews was very limited (Magnusson and Marecek, 2015) are of the view that a qualitative research interview is appropriate for examining subjects where several levels of meaning must be investigated. Quantitative research can scarcely be used to do this. The author emphasises that interviews may concentrate on facets of organisational life. Prior to gathering the quantitative data from members of the supply chain for this thesis, in-depth interviews with key leaders in the supply chain organisation and information security experts were helpful.

As was already indicated, this thesis bases the gathering of qualitative data on the findings of quantitative research. Prior to its distribution, the quantitative questionnaire was reviewed after in-depth interviews with the top executives provided a different viewpoint that helped researchers better grasp the research topics. However, qualitative research in and of itself does not test the hypotheses identified in Chapter 3. To learn more about minimising information security threats in the supply chain from the standpoint of an individual, quantitative data will be gathered. Three in-depth face-to-face interviews were conducted to gather the quantitative data since qualitative data was used to support quantitative data. The interview subjects were chosen at random; one of them was the key author in this research and a lecturer and two PhD students. The next stage was to go to the field to hear the views and opinions of employees from the supply chain setting. The subsequent section highlights the piloting. The interview questions are provided in Appendix C.

4.9 Ethical considerations

Ethics was taken into consideration as an essential obligation for the completion of this thesis, as is the case with all academic business research. CU Ethics committee did the approval. When sending the information invitation letter, assurance was given to all the participants that the information provided **would be confidential** and used solely for the purpose of this study. The data will be collected and stored in accordance with the Data Protection Act 1998 and will be disposed of in a secure manner. The approval letter is included in Appendix A.

4.10 Pilot Testing

According to the literature reports, pilot testing should be carried out in the same manner as it will be utilised in the main study. For instance, questionnaires sent through the mail should be piloted by sending them through the mail (Andrew et al., 2010; Leech and Onwuegbuzie,2009). Bryman and Bell (2022) add that pilot studies should preferably be conducted on a separate group from the actual respondents; it is acceptable for them to be comparable to members of the population from which the sample will be drawn for the main research. Andrews et al. (2010) demonstrate that earlier researchers created a method for piloting online surveys. The research carried out by Andrew and his colleagues in 2010 identified four crucial phases within the pilot testing of the online survey. Consequently, the four stages described above were utilised in the preliminary testing of the online survey (Figure 12). The questionnaire was piloted with three industry professionals, five workers in the manufacturing industry and a few students pursuing doctoral degrees. This was done to ensure that the wordings are clear, comprehensible, relevant, efficient and consistent in their interpretation and that all questions have been answered in a format that is suitable. Second, a sample of more than seventy-five workers from a variety of manufacturing organisations in Nigeria was used to validate the survey. This was quite helpful in reducing the overall number of questions and pinpointing any concerns that may have been there. In the final round of the pilot survey, which was conducted with individuals who had no prior connection to the survey, further typos and inaccuracies were discovered. In this report, concerns about information security threats in the supply chain companies were analysed and discussed below. The reliability test, case summaries for missing values, outliers, demographic distribution, R Squares and casual relationships were the primary focuses of the report.

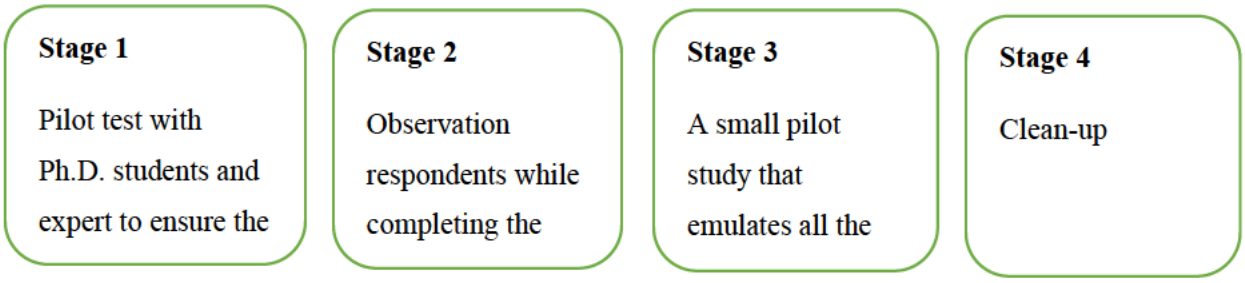


Figure 4.2: Stages in the pilot test

4.10.1 Distributing the questionnaire through the companies

Prior to distributing questionnaires to produce a high response rate that can be applied to the entire company is selecting key informants. A key informant is someone who can communicate with the researcher while also being knowledgeable about the topic of the study (Open Education Sociology Dictionary). Key informants were chosen for this study using a set of criteria. As key informants with the expertise of their supply chain partners, information security threats and the importance of

information security, the top decision-makers of the focal firms were chosen. The majority of the firm information gathered from the lists listed above includes the contact information for the key decision-makers. Contacting the offices of the remaining firms will yield the contact information of their decision-makers.

Table 4.13: Methods used to increase participation.

Methods	Result after applying to the current result
• Colleague and insider referral's introduction	• Privileges exist due to the researcher being a student.
• Contacting manufacturing firms that had supported surveys	• Several emails were sent, and few responses. • Left messages, few responses.
• Contacting leading logistics and distribution	• Several emails were sent, and responses were encouraging. • Left messages.
• Contacting the Marketing and Distribution department with a visible presence in information security	• Several emails were sent, and few responses. • Left messages with few responses.
• Contacting several employees in the Production and Operation company	• Relevant employees were contacted, and there were email communications. The final reply was that they would assist.

4.10.2 Participants in the Interview

At each participant's workplace, the researcher performed nine semi-structured interviews in total. However, the semi-structured questions were open-ended to offer participants as many opportunities as possible to express their opinions. This reduced the likelihood of missing important information and prevented the predefinition of potential replies by allowing flexibility in the interview's direction and unrestrained knowledge flow. All were reached through phone and WhatsApp videos at the participant's workstation. As a result, the participants were in a relaxed setting where they did not feel constrained or uneasy about disclosing information, and each conversation lasted 35 minutes. The interviewees' comments are analysed in Chapter 5 (section 5.11). The questions can be found in Appendix (II).

Table 4.14: Interviewees

Organisation Type	Positions	Experience	Interview type
Somal enterprises	IT expert	15	Phone
Real concept	Management	10	Phone
Nigeria Breweries	Senior Manager	12	WhatsApp call
Nigeria Tobacco	Senior Manager	8	WhatsApp call
Real concept	Management	8	Phone
Dangote Group	Senior Staff	10	Phone call
Honeywell Flour Mills	Management	15	WhatsApp (Video call)
Dansa Food Ltd	IT expert	12	WhatsApp (Video call)
May & Baker Ltd	Senior Manager	15	WhatsApp (Video call)

4.11 Data Analysis

SEM-PLS variance was utilised in the processing of the survey's responses in order to conduct the statistical analysis. PLS is more suited for explaining complicated relationships due to its effectiveness in avoiding two significant disadvantages: PLS Variance has been successfully utilised in a variety of information security research and supply chains, some of which are examples in Bulgurcu et al. (2010). Because information security is inherently intrusive and necessitates a high level of trust between the organisation being researched and the researcher conducting the study (Sekaran and Bougie, 2016), there was a concern that insufficient participants would be recruited to carry out a quantitative analysis that would be useful. The sample size in PLS should be at least 10 times the number of incoming paths to the construct with the most incoming paths, which is called the 10 times rule, it is commonly believed that PLS gives more leverage and is more appropriate than statistical estimation methods. A software known as SmartPLS was utilised in order to conduct a PLS analysis for the purpose of calculating the structural path significance of both the outer model and the inner model. This analysis was made much easier by the incorporation of a built-in algorithm known as Bootstrapping. This algorithm generated the t-statistics that were used to verify the significance of the research hypotheses that were proposed in this study.

4.11.1 Data analysis for Qualitative

Content Analysis (CA) is a comprehensive method for analysing and presenting qualitative data in a descriptive format. According to Selvi (2019), it is a method for studying the relationship between text and speech and the context in which they are employed. Researchers may utilise CA to find recurring ideas in the texts they're given to analyse, which can then be used to deduce what topics were discussed

during an interview. Therefore, CA examines the topics that generate the greatest discussion and the connections between them.

The researcher manually transcribed the interviews after uploading the audio file to a computer programme (Window Media Player). Then, we utilised content and thematic analysis to determine what concepts were being discussed throughout the interviews and how those concepts were connected to one another (Selvi 2019; Forman and Damschroder, 2007). Items were determined by analysing the frequency with which participants used certain keywords throughout the interview, the relationship between keywords and constructs, and the substance of participants' remarks on the different constructs. Common themes and items that emerged after comparing the themes and items produced by each interview were chosen.

4.12 Data Triangulation

In common usage, triangulation combines data from several sources to increase precision, ensure reliability and establish consensus on a conclusion (Jankowicz, 2013). Jankowichz, (2008) adds that triangulation helps distinguish between overlapping and distinct realities. Noble and Heale, (2019) states that triangulation involves multiple data-gathering methods and is also an indicator of a good research design. Denzin (2012) outlined four primary methods of triangulation. These are discussed:

- **Data triangulation –** This refers to contrasting and cross-checking information from multiple sources and employing several sample methodologies during a research project. There are three distinctly different kinds of triangulation; those involving persons, those involving space and those involving time. Person triangulation refers to gathering information about a phenomenon from multiple individuals, communities and institutions. Taking measurements of the same phenomenon in multiple locations is known as space triangulation, whereas taking measures at different time intervals is known as "time triangulation".

- **Researcher triangulation** - This refers to the method wherein many researchers examine the same dataset as opposed to depending on the results of a single study.

- **Theoretical triangulation -** This refer to two or more theoretical viewpoint that may be applied to the same data to determine how the outcomes vary when different assumptions and principles are utilised.

- **Methodological triangulation** - This refers to research that employs many techniques simultaneously. There are two types of this: triangulation inside a single technique and triangulation between different methods. Denzin (2012) distinguishes between multimethod research (using two or more techniques within the same research paradigm) and mixed-method research (including both qualitative and quantitative approaches).

This thesis employed a triangulation methodology, which is aligned with the philosophical paradigm adopted for the research. The chosen paradigm falls within the positivism-interpretivism continuum. By utilising triangulation, the researcher was able to draw upon various methodologies and sources of information, allowing for a comprehensive and robust approach. Triangulation served several purposes: it ensured convergence in results, minimized or eliminated alternative explanations for conclusions, and clarified any divergent aspects of the study (Jankowicz,2013). Furthermore, it compensated for the weaknesses of individual methodologies by leveraging the strengths of each (Jankowicz,2013; Noble and Heale, 2019). Ultimately, triangulation enhanced the researcher's ability to derive meaningful findings and offer clear recommendations to management (Noble and Heale, 2019).

4.13 Summary

This chapter presents the research methodology and design implemented in this study, focusing on aspects such as research philosophy, research design, sampling strategy, instrument development, data collection, and statistical methods used for data analysis. The research objective and context were discussed, with consideration given to the conceptual framework, ultimately leading to the selection of pragmatism as the appropriate research philosophy. To address the research question effectively, a mixed methods design incorporating both quantitative and qualitative approaches was deemed necessary. The use of quantitative, qualitative, and mixed methods was considered most suitable for obtaining comprehensive answers to the research question. Specifically, a convergent parallel mixed methods design was employed in this investigation. Individual representatives from various organizations served as the unit of analysis, while the target population comprised members of different manufacturing companies within the supply chain in Nigeria. It was noted in Chapter Two that there were limited studies employing blended methodologies to address the research problem. By incorporating qualitative data alongside quantitative data, the study aimed to validate the quantitative results, provide a more thorough explanation of the findings, and gather additional information regarding the topic under investigation.

This chapter provides a comprehensive description of both the quantitative and qualitative phases of the study, including details on the research tools used (surveys and interviews), sampling strategy, instrument design, piloting, data collection, response rate, and data analysis. Quantitative data was collected through surveys, while qualitative data was gathered through interviews. Given the limited access to email and the Internet in Nigeria, the survey was conducted through personal contact with each participant. However, to provide respondents with options, they were given the choice to either

complete the survey online or receive an electronic copy of the questionnaire. This approach allowed for flexibility and catered to the respondents' preferences.

During the data collection process for the survey, the researcher visited several businesses, and respondents were also given the opportunity to participate in an interview if they wished to do so. This decision was made due to constraints in terms of both time and resources. This approach proved successful, as seven out of the nine interviews were conducted during the initial visit, while the remaining two interviews were scheduled for a later time based on the respondents' recommendations.

Having provided an overview of the study philosophy, research methodology, and data collection processes in this chapter, the subsequent chapter will delve into a detailed discussion of the results and the process of data analysis.

Chapter 5: Data Analysis and Result

5.1 Introduction

The methodology for conducting the study was discussed in the previous chapter. Also included was a description of how the survey questionnaire and interview instrument were developed and finalised. This chapter explains the data analysis process used for the research questions in the previous chapter. This chapter is divided into two sections. The first section explains the quantitative data analysis including the coding technique, cleaning data, missing value analysis, demographic data analysis, data normality, outliers' observations, linearity and co-linearity tests, and the checking of the sample size. The analysis was conducted using partial least square structural equation modelling (PLS-SEM) assessment of validity, reliability, discriminant validity and test the relationships between variables. A range of statistical techniques were used to provide the most accurate answers to the research questions. The second section provides an overview of the qualitative data analysis process, which includes demographic information, transcribing and coding technique, among other things.

5.2 Section One

5.2.1 Data Coding and Editing

The questionnaire was gathered using Qualtrics, as was covered in the preceding chapter. Following collection, the data was exported to an SPSS file. The data was then thoroughly examined before any kind of analysis was carried out. This was done to make sure there were no errors made throughout the data exportation process. The approach began by looking for errors because any errors could have a significant impact on the study's outcomes. This preliminary analysis of the data revealed that the SPSS file did not contain any odd entries or typographical errors. Thirty records were randomly chosen from the exported data set and compared to the original data set in the Qualtrics system to further corroborate this. Again, no differences were discovered, so it was determined that the data had been imported to SPSS accurately and without any mistakes or typos. The variables were then coded using a combination of characters and numbers to facilitate the next phases of data processing. As a result, each question was represented by an acronym code. For example, the first question in the survey asked respondents to specify their gender (male and female). As a result, instead of using the gender in SPSS, each choice of gender was given number from 1 and 2 (Field, 2018). For instance, Attitude was measured by four questions, and these were represented as ATD1, ATD2, ATD3, and ATD4 inside the SPSS database. Some of the open-ended questions were transformed into category data and then classified appropriately. For example, response for question 5 (What business sector are you?) was classified into four main categories: Manufacturing, Logistics, Marketing /Distribution and Production/Operation. Hence, in SPSS, each option was assigned a number, 1 through 4 instead of using the business sectors (2018). For the other sections, each question or statement had numbers to label the responses. The

responses for each section were coded as 5 = Strongly agree, 4 = Agree, 3 = Neutral, 2 = Disagree, 1 = Strongly disagree. In the data file, all the recorded answers to these questions were inverted.

5.2.2 Data Entry, Screening and Cleaning

The data was ready to be entered into SPSS after coding. While online survey software allows data to be immediately transmitted to SPSS, respondents in this study responded in three different ways. Some respondents completed the survey online, and some responded to the electronic version via email, while others completed the form on paper. As a result, the data was manually input into Word Excel and then transferred to SPSS. Manual data entering has a higher risk of creating errors. While meticulous attention was paid to data entry, it was also necessary to screen the data for any inaccuracies. The data was reviewed for mistakes when it was entered into SPSS. Outliers that are far above or below the other score are caused by data entry errors, resulting in a distorted result (Pallant, 2013). The frequency, mean, standard deviation and box plot for each variable were evaluated using SPSS to discover any out-of-range values.

5.2.3 Respondents' Demographics Profile

The survey instrument included a few demographic variables to collect the information that will help to define the characteristics of the respondents. The first section of the survey instrument included nine questions related to the company/respondent profile such as the gender, age, qualification, respondent's position in the company, number of years the company has been established, company's main business/business, number of employees and company information sharing platform. Table 5.1 provides the demographic information of the respondents which is discussed in the next paragraphs.

5.2.4 Gender of the respondents

The data shows that the majority of respondents in supply chain companies were male (54.2%), while females accounted for 45.7% of the total respondents. This gender disparity suggests that there is a gender imbalance in the representation of employees in these organizations. This finding aligns with observations made during the interviews, where fewer females were present in the participating organizations. It is important to understand how this gender imbalance may influence the attitudes, perspectives, and behaviours related to information security in the supply chain.

5.2.5 Age of the respondents

The highest proportion of respondents (38.6%) fell within the age range of 31-40. This indicates that the majority of respondents were middle-aged individuals. It is worth considering how age may impact the level of experience, expertise, and familiarity with information security practices. Middle-aged

individuals might possess more experience and knowledge in dealing with information security threats, potentially influencing their attitudes and behaviours in this domain.

5.2.6 Educational Background

The data reveals that a significant portion of respondents held a master's degree (32.7%), followed by those with a bachelor's degree (31.1%) and a PhD (11.8%). This indicates that a considerable proportion of respondents had higher educational qualifications. The educational background of individuals can shape their understanding and awareness of information security principles and practices. It is plausible that higher educational qualifications may influence the attitudes and commitment of individuals towards safeguarding information assets

Table 5.1: Respondents gender

Gender	Frequency	Pct. (%)
Male	270	54.2
Female	227	45.7

Table 5.2 Respondent age distribution

Age	Frequency	Pct. (%)
18-20	3	0.6
21-30	95	19.1
31-40	192	38.6
41-50	163	32.7
51-60	32	6.4
61-Above	3	0.6

Table 5.3: Respondents Educational background

Qualifications	Frequency	Pct. (%)
SSCE	10	2.0
NCE	37	7.4
Diploma	64	12.9
BSc	156	31.3
MSc	163	32.7
PhD	59	11.8

5.3 Respondents' Business Characteristics Profile

5.3.1 Position of the respondent

Position in the Company: The data shows that senior staff members constituted the largest group of respondents (42.8%), followed by management (33.7%) and junior staff (22.7%). This distribution suggests that individuals in higher positions within the company, such as senior staff and management, are more actively involved in mitigating information security threats in the supply chain. This finding highlights the significance of organizational roles and responsibilities in shaping attitudes and behaviours towards information security.

5.3.2 Work Experience of the Respondent

Regarding the number of years, the respondents have been working. Table 5.2 illustrates that over half of the employees had 5 years of working experience, with a percentage of 64.3%, 26.1% of the employees had 3-5 years of working experience, and 7.2% had less than 2 years working experience. The survey needed to be answered by a well-established company with good knowledge of employees that has a good number of working experiences in safeguarding their information security in the supply chain and reducing threats in the supply chain.

5.3.3 Company History

The companies involved in the survey were established at different period. 43.1% of the respondents' companies were founded between 10 – 20 years ago, 38.2% of the respondents' company have been established for more than 20 years, and 17.7% were also established less than ten years ago. This means that the majority of the companies have been in business for quite a long time. This signifies that the respondent companies know the industry well and might have gained or had experience dealing with information security in the supply chain.

5.3.4 Main Business

The next question the respondents answered was about their primary business, and they were told to choose all the appropriate options because a company might be involved in more than one business (for example, a company can be in production and operation, as well as a manufacturer). Table 5.2 indicates that out of 98.6 % of respondents, 34.5% are manufacturers. Production and operation constitute 32.1%, whereas marketing and distribution account for 20.9%. Transport/logistics service providers account for 11.0%, the lowest. While manufacturers include the highest percentage, the respondent pool represents the target population well.

5.3.5 Number of employees

The number of employees is the one way to determine a firm size (Lee et al., 2009). Table (5.2) shows the size of the respondent company based on the number of employees. Akinyomi (2012) categorise

the companies in Nigeria as small, medium and large if their employees are 10-50, 50-99 and more than 100, respectively. A little below half (43.0%) of the firms have more than 50 employees, out of which 22.9% have 31-50 employees. The remaining 17.1% of the companies employ between 1-10 employees, and 14.5% have above 20 employees. This result matched with Afolabi and Lasaide's (2019) findings, where large companies were 58%, and medium companies were 18%, indicating that the composition of the respondents adequately represents the targeted population in terms of the firm size.

Table 5.4: Position of the staff

Position	Frequency	Pct. (%)
Junior Staff	113	22.7
Senior Staff	210	42.8
Management	167	33.7

Table 5.5: Work experience of the staff

Work Experience	Frequency	Pct. (%)
1-2 years	36	7.2
3-5 years	130	26.1
5 years and above	320	64.3

Table 5.6: Company history

Company Age	Frequency	Pct. (%)
Less than 10	88	17.7
10-20	215	43.1
Above 20	190	38.1

Table 5.7: Main business

Main Business	Frequency	Pct. (%)
Manufacturing	172	34.5
Logistic & Transport	55	11.0
Marketing & Distribution	104	20.9
Production & Operation	160	32.1

Table 5.8: Number of employees

No. of Employee	Frequency	Pct. (%)
1-10	84	17.5
11-30	72	14.5
30-50	114	22.9
50-Above	214	43.0

5.3.6 Communication tools

Various companies employ unique methods to share and safeguard their information both internally and externally. The majority of participants (52.4%) preferred utilizing email as their primary communication medium due to its widespread use, ease of identifying threats, ability to monitor correspondences, and avoidance of phishing email links. The remaining responses consisted of company information sharing platforms (CISP) at 33.5%, Instagram at 7.2%, blogs at 2.6%, and Twitter with the lowest percentage at 2.2%.

Table 5.9: Respondent communication tools

CISP	Frequency	Pct. (%)
Blog	13	2.6
Email	261	52.4
Twitter	11	2.2
Instagram	36	7.2
CISP	167	33.5

Overall, the demographic data provides important context for understanding the characteristics of the respondents and how these characteristics relate to their attitudes and behaviours regarding information security. By considering gender, age, educational background, and position within the company, communication one could gain insights into potential factors that influence the responses and actions of individuals in the supply chain context.

5.3.7 Independent Sample Test

The comparisons between different groups of respondents were done to provide more detailed information about the characteristics of each group. A cross-tabulation of gender demographic variable

was measured to see if there are mean statistically significantly differences for male and female groups in their participation because each group was independent to each other, so independent t-test was utilised for comparing the two means of the participants of the two sample groups in table (5.2). The comparisons were done for qualification, age, and main business sector, number of employees, position and work experience to see the respondent level of participation of the gender. This highlighted the need for extra analysis in order to know the involvement of both genders. The 'Independent T-Test', or 'Levene's Test', which assumes equal variances and can be simply performed through SPSS, is the most widely used test for this purpose (Field, 2017). Table 5.2 illustrates the T-Test, which shows that the two samples' groups participated differently, although males engaged more than female.

Table 5.10: Independent Samples test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
									95% Confidence Interval of the Difference	
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Qualification	Equal variances assumed	11.290	.001	1.542	487	.124	-.165	.107	-.374	.045
	Equal variances not assumed			-1.517	430.119	.130	-.165	.109	-.378	.049
Position	Equal variances assumed	.520	.471	-2.703	485	.007	-.184	.068	-.317	-.050
	Equal variances not assumed			-2.712	476.926	.007	-.184	.068	-.317	-.051
Age	Equal variances assumed	.095	.758	-.677	490	.499	-.058	.086	-.227	.111
	Equal variances not assumed			-.674	465.126	.500	-.058	.086	-.228	.112

Main Business	Equal variances assumed	.192	.662	-1.883	488	.060	-.216	.115	-.441	.009
	Equal variances not assumed			-1.883	472.646	.060	-.216	.115	-.441	.009
Employee	Equal variances assumed	12.247	.001	-1.998	485	.046	-.207	.103	-.410	-.003
	Equal variances not assumed			-2.018	483.726	.044	-.207	.102	-.408	-.005
Work experience	Equal variances assumed	5.627	.018	1.523	476	.128	.086	.057	-.025	.197
	Equal variances not assumed			1.509	438.513	.132	.086	.057	-.026	.198

5.4 Section Two

5.4.1 Selecting a Data Analysis Method and Justification

There are various approaches available for conducting model analysis, each with its own advantages and disadvantages. Choosing the appropriate approach requires careful consideration. Data analysis can be categorized into two groups: first-generation approaches (such as simple linear regression, multiple regression, ANOVA, and MANOVA) and second-generation approaches (such as structural equation modeling, SEM). The literature suggests that second-generation techniques offer several advantages over first-generation techniques. Ronkko et al. (2015) state that second-generation approaches have gained popularity across different disciplines for the past two decades, as they often yield better results compared to first-generation techniques (Rigdon, 2016). Additionally, second-generation approaches, like SEM, allow for the estimation of error variance parameters (Hair et al., 2019). When measurement error is present, using first-generation approaches can lead to erroneous results because they overlook measurement error. However, this issue can be addressed by employing a second-generation strategy like SEM. Hair et al. (2017) explain that researchers can evaluate both the measurement model and the structural model in a single test using a second-generation approach. Moreover, compared to first-generation approaches, this enables researchers to complete the analysis in fewer steps (Hair et al., 2019).

One of the main disadvantages of first-generation techniques is that researchers can only investigate one layer of correlations between independent variables (IVs) and a dependent variable (DV) in a single analysis (Hair et al., 2017). This means that researchers may be unable to examine multiple layers of interactions between IVs and DVs simultaneously using first-generation techniques, and it is not possible to test a model with multiple DVs in a single study. This is where the second-generation approaches, like SEM, have a significant advantage over the first-generation approaches, as they facilitate the analysis of multiple layers of interactions easily (Hair et al., 2019). SEM consists of two sub-models: the inner model (structural model), which explains the relationships between latent independent and dependent variables, and the outer model (measurement model), which specifies how the latent variables relate to the observed indicators (as shown in Figure 5.1).

The proposed framework in this thesis includes both the DVs and IVs and this requires conducting a series of regression analysis in a single test. One would argue that the above appraisal reports about second generation is seen as a rational choice for this study. Hence, SEM was chosen as the data analysis approach for this study.

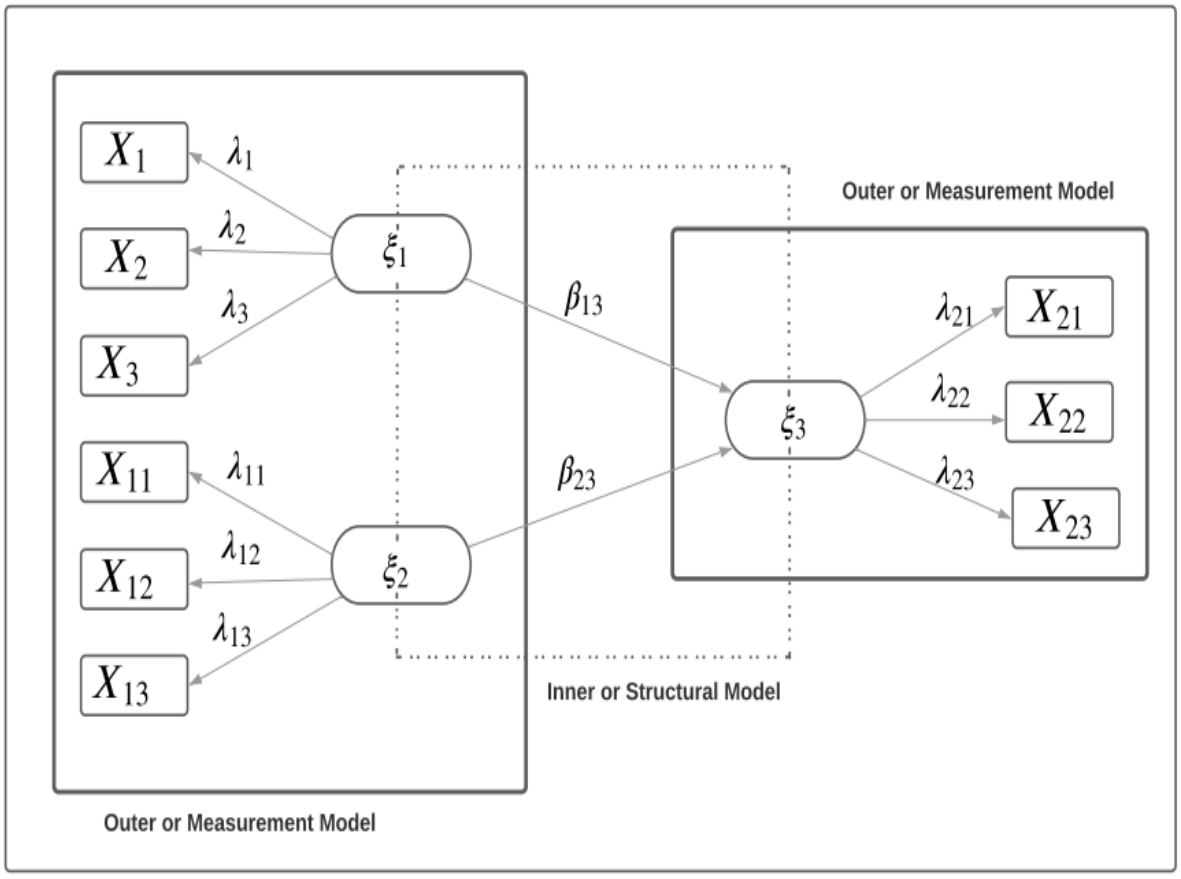


Figure 5.1: SEM representation

Figure 5.1 depicts a simplified representation of Structural Equation Modelling (SEM). The ellipses represent the latent variables (LVs), which are explained by observed indicators (X) referred to as manifest variables (MVs). The arrows indicate causal relationships between variables, with the direction of the arrow indicating the direction of the relationship. The variables connected by the arrows represent the specific relationship under consideration. When the variables in the path model are latent variables inferred by a set of observed indicators, the subsequent analysis is referred to as SEM. Each SEM model consists of two levels of relationships: the first level focuses on the relationships between the MVs and their corresponding LVs (Measurement model), while the second level examines the causal relationships among the LVs (Structural model).

In this study, the model presented in Figure 5.2 consists of five exogenous variables and four endogenous variables, with a respective number of MVs describing these variables.

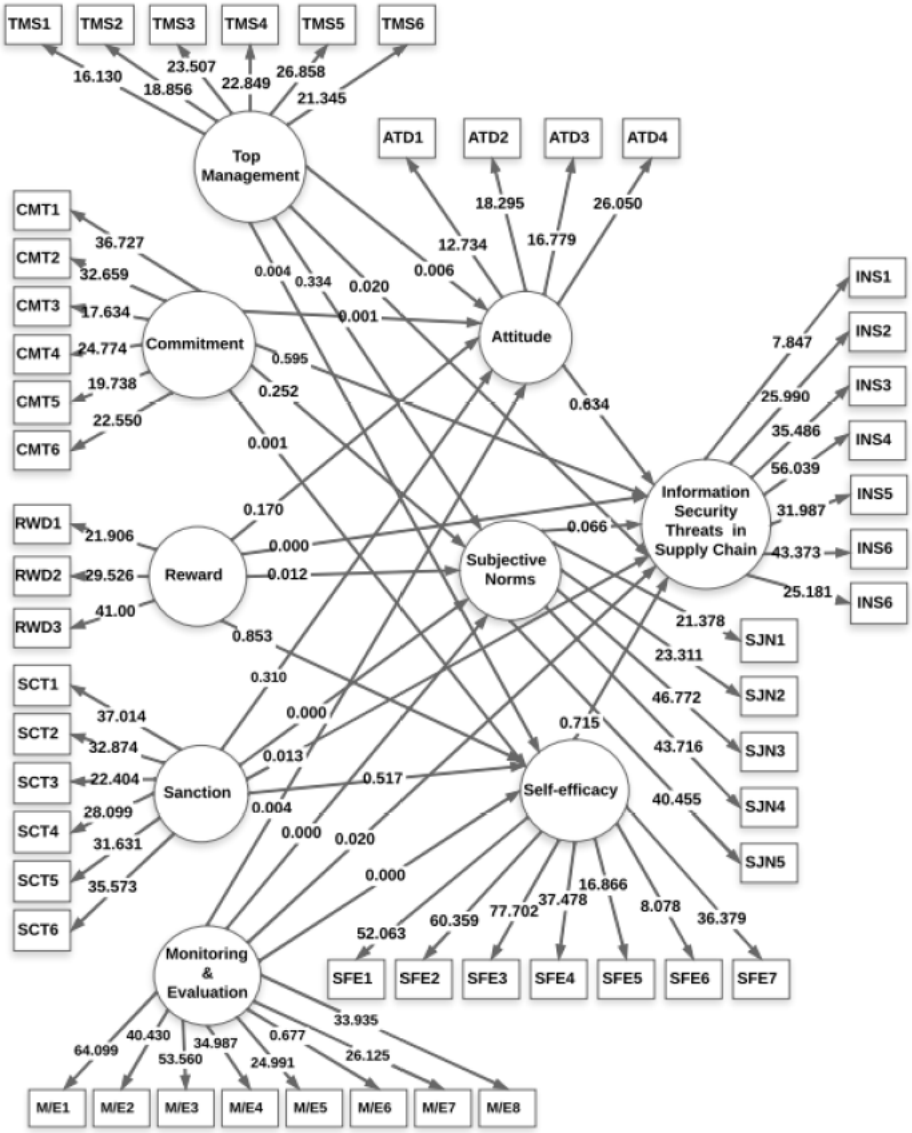


Figure 5.2: The SEM used for this study.

	Exogenous	No of MVs	Endogenous	No of MVs
	Sanction	6	Attitude	4
	Commitment	6	Subjective norms	5
	Top management support	6	Self-efficacy	7
	Reward	3	Information security threats in the SC	6
	Monitoring/Evaluation	8		

5.4.2 Structural Equation Modelling

According to Ringle et al. (2020) Structural Equation Modelling (SEM) has become increasingly popular. SEM is a second-generation multivariate data method (Hair et al., 2017). Kline (2016) points out that SEM is also a large sample approach. Tabachnick and Fidell (2013) argue that SEM is used most often to confirm a prior hypothesis, in contrast to the exploratory nature of factor analysis, thus planning is crucial for any SEM analysis. Henseler et al., (2015) believe that the advantage of SEM is that it allows for a "one step approach", in which researchers estimate both the measurement model and the structural model (causal relationship) simultaneously. The reliability and validity of the constructs should be tested in the first step, and the theoretical framework or structural model should be tested in the second step (Hair et al., 2017).

Sarstedt et al. (2020) argued that structural equation modelling (SEM) allows for more rigorous testing of construct reliability, convergent validity and discriminant validity than other methods. Hair et al. (2017) adds that the reason for this is because SEM incorporates the evaluation of validity and reliability into the overall process. Furthermore, according to IS scholars, the two most crucial elements that researchers should consider when choosing an analytical technique are their level of knowledge and their available time.. Hair et al. (2017) propose that SEM approaches are classified into two categories: CB-SEM (Covariance-Based Structural Equation Modelling) approach and component-based or PLS-SEM (Partial Least Squares-Structural Equation Modelling). The next section explains the classification of SEM and the justification.

5.4.3 Classification of SEM

In the earlier section SEM was classified into two categories: CB-SEM (Covariance-Based Structural Equation Modelling), whilst PLS-SEM is referred to as variance based (Partial Least Squares-Structural Equation Modelling), as it accounts for the total variance and uses the total variance for estimate parameters (Hair et al., 2017). Covariance-based structural equation modelling (CB-SEM), which examines intricate correlations between observable and latent variables, has long been the method of choice. Hair et al. (2017) state that until approximately 2010, more publications using CB-SEM rather than partial least squares structural equation modelling (PLS-SEM) were published in social scientific journals. Compared to CB-SEM, the number of studies published in recent years that used PLS-SEM has greatly grown (Hair et al., 2017). In fact, PLS-SEM is now widely applied in many social science disciplines, including organisational management (Sosik et al., 2009), international management (Cho and Luo 2019), human resource management (Christy et al.,2017), management information systems (Ringle et al., 2020), operation management (Colicchia and Menachof, 2019), market management (Collier et al., 2014), management accounting (Caputo 2020), strategic management (Chen and Yen, 2014), hospitality management (Dessler, 2011) and supply chain management (de Barros et al.,2015)

Several textbooks (Garson 2016; Dubrin 2009; handfield and Nicholas, 1991), edited volumes (Flynn and Zhao, 2010;Frank and Odundayo,2013), and special issues of scholarly journals (Hajmohammad and Vachon, 2014; Gunasekaran and 2007) illustrate PLS-SEM or propose methodological extensions. PLS-SEM approach has much fewer prerequisites than the CB-SEM method, it still yields consistent estimation results when compared to the CB-SEM method (Sarstedt et al., 2016). As a result, SEM does not have a well-defined global optimisation criterion, and thus there is no global fitting function to assess the goodness of the model. However, it is a variance-based model that is strongly oriented to prediction, and it is more concerned with the model's predictive capability than it is with the statistical accuracy of the estimated values.

Table 5.11: Summary Comparison of PLS-SEM and CB-SEM Approaches

Basis of Comparison	**PLS-SEM**	**CB-SEM**
Objectives	Prediction oriented	Theory oriented: Parameter oriented
Approach	Variance based	Covariance based
Assumption	Predictor specification (nonparametric)	Multivariance normal distribution and independent observation
Relationship between a latent variable and its measures	Can be modelled in either formative or reflective mode	Typically, only reflective indicators
Implication	Optimal for prediction accuracy	Optimal for parameter accuracy
Model Complexity	Large complexity (100 constructs, 1000 indicators)	Small to moderate complexity (e.g.<100 indicators)
Sample size	Power analysis based on the model with large number of predictors. Recommendations for minimum number of observations range from 30 to 100 cases	Ideally based on power analysis of specific model. Recommendation for the minimum number of observations range from 200 to 800

.

It is common to see SEM (PLS-SEM) applied across a different discipline, including organisation research (Sosi et al., 2009) and social science (Hair et al., 2017).Mateos-Aparicio (2011) believes that using a combination of principal components analysis and regression-based path analysis, PLS-SEM estimates the parameters of a set of equations in a structural equation model, thereby reducing error.According to the Ringle et al. (2020) study, the method offers various advantages for researchers who are using cause-effect relationship models to explain or predict a specific construct, such as job satisfaction (Buonocore and Russo, 2013), commitment (Ringle et al., 2020) and behaviour (Schlagel and Smarted, 2016). The ability to (1) handle very complex models with many indicators and constructs, (2) estimate formatively specified constructs, (3) handle small sample sizes with the necessary level of care, and (4) derive determinate latent variable scores, are just a few of the advantages (Richer et al., 2016).In recent years, there has been a significant increase in the number of articles that use PLS-SEM in business research (Hair et al., 2014), and there has been debate about its advantages and limitations (for example, Ringle et al., 2020; Safa et al., 2019; Cugansan et al., 2018; Sarstedt et al., 2016; Rooney

and Cuganesan 2015; Chen and Yen 2013). One would argue that with the explanation in the section, PLS-SEM has many advantages over CB-SEM, that is why it was chosen over PLS-SEM.

The PLS analysis in this research was conducted using Smarts. PLS path modelling, also known as PLS-SEM, is a component-based technique that aims to maximise the explained variance of the dependent latent constructs by incorporating as many components as possible (Hair et al., 2017).

5.4.4 Selecting PLS-SEM approach and the justification

Literature indicates PLS-SEM method as an influential approach in the IS research and supply chain research (Hair et al., 2019; Hair et al., 2017), testing a theoretical framework from a predictive perspective Ringle et al. (2020) add that PLS-SEM has also been a common method in other discipline operation management, marketing management, organisation and human resource. One of the objectives of this research was to develop and test a framework. Towards this goal the research started with a critical literature review and then proposed a conceptual framework in Chapter 3, and this is needed to be tested through PLS-SEM. This is in line with the overview points that is considered in Hair et al. (2018). It is preferred in this study because it offers solution with sample sizes because the small population restricts the sample size. In addition, it has the prediction, orientation and capabilities to handle complex models with many constructs, indicator variables and structural paths, without imposing distributional assumptions on the data and small sample sizes.

Sarstedt et al. (2016) describe that, regardless of whether the data comes from a common or composite model population, PLS-SEM provides solutions when approaches like CB-SEM create unacceptable results or do not converge with complex models and limited sample numbers. PLS-SEM shows a higher robustness in these situations (Sarstedt et al., 2016). PLS-SEM provides greater statistical capability for researchers to work with (Hair et al., 2017b; Reinartz et al., 2009). Sarstedt et al. (2016b) point out that this characteristic still applies with common factor model data estimation, which is what CB-SEM does. According to Hair et al. (2017), goodness of fit is much less in this case, and is more likely to detect associations as significant when they are in existence in the population since it has better statistical power.

In this study to ensure the integrity and consistency of the collected data, vigilant consideration was given to the missing data by following the three step guidelines introduced by Henseler et al., (2016). The PLS analysis in this research was conducted using SmartPLS. PLS path modelling, also known as PLS-SEM, is a component-based technique that aims to maximise the explained variance of the dependent latent constructs by incorporating as many components as possible (Hair et al., 2017).

In recent years, there has been a significant increase in the number of articles that use PLS-SEM in business research (Cugansen et al., 2018; Gharib et al., 2017; Henseler et al., 2016). However, PLS-SEM is still new to many researchers. It is common to see PLS-SEM being applied across a different

discipline including psychology research (Sosik et al., 2009), social science (Hair et al., 2017) and business community active participation in OC (Gharib et al., 2017). PLS-SEM was selected over covariance-based SEM because the research objective was exploratory and oriented more towards predictions and theory-building, rather than theory-confirmation (Sosik et al.,2009).

5.4.5 Missing Data

In statistics**,** missing data is a frequent occurrence and a problem in social science research. Even in initially large cohorts, participant dropout can drastically limit the sample size available for research Hair et al. (2017) explain that missing data occurs when no data value is stored for any variable, or when data has been stored incompletely. For example, a respondent either purposely or inadvertently failing to answer one or more question(s) can be seen as missing data. Missing data (also known as missingness) can lead to bias and will always decrease efficiency. Allison (2019) points out that analyses that account for missing data must consider the reasons for the missing data. The authors also added that failure to account for missing data appropriately in studies may lead to bias and loss of precision. For example, lack of records, item non-response, system failure to capture observation during the period of answering the questionnaire, loss of documents and other factors might result in missing value. When one or more observations are missing, estimating the missing values is necessary to understand the data's nature better. For analysis to be completed, Andy (2018) state that imputing missing values using an appropriate approach is critical. Missing data has been identified and dealt with using a variety of methods. Even though the relevance of missing data and its effects on study outcomes has long been recognised in the literature, there were numerous articles that made no mention of the practices in details.

5.4.6 Reasons for missing data

Missing data causes (also known as missingness mechanisms) are often categorised into three as, Missing Completely at Random (MCAR), missing at Random (MAR) and missing not at Random (MNAR). Allison (2009) state that when data is MCAR, there are no systematic differences between observed and missing data. Conceptually, data that is MCAR is not usually attributed to a question in the survey or other phenomenon, whether observable or unobservable. For example, a question being asked relates to top management support and is represented by TMS 1, while another question relates to commitment and is represented by CMT2. In MCAR, the reason for TMS1 having a missing response is not because of TMS OR CMT that is neither the survey question, nor another confounder is the reason for the missing value (Little and Rubin, 2019). When MCAR is suspected, Little's Test of Missing can be used to determine whether the missing values meet the specification of MCAR (Allison,2009).

When data is MAR, any systematic differences between observed and missing data can be explained by associations with the observed (Little and Rubin, 2019; Allison, 2009). Data that is MAR is missing based on another observable instance, such as an underlying or confounding factor causing respondents

to not answer questions (Allison,2009). For instance, individuals that have involved in breaches event would not like to answer a question related to it. MNAR is used when the missingness mechanism is neither MCAR nor MAR, and associations with the observed data cannot explain all systematic differences between the observed and missing data (Rocco et al. 2003). Data that is MNAR, on the other hand, can be attributed to an observable factor that is directly affecting the reason that the data values are missing (Little and Rubin,2019).

5.4.7 Data Treatment Methods

Ringle et al. (2020) suggested three ways of handling missing data. In mean value replacement, the lost values of an indicator variable are replaced with that indicator's mean of valid values. While easy to implement, mean value replacement decreases the variability in the data and likely reduces the possibility of finding meaningful relationships. This type should be used only when data exhibit deficient levels of missing data—for example, less than 5% of values missing per indicator. The option to remove all cases from the analysis that include missing values in any of the arrows used in the model is referred to as case-wise deletion CD, or list-wise deletion (LD). When case-wise deletion is being utilised, two issues warrant further attention. First, there is a need not to systematically delete a particular group of respondents (Drost 2011). For example, committed respondents are more likely to refuse to answer questions related to information security threats in their company. Running case wise or list wise deletion would systematically omit this group of respondents and, therefore, likely yielded biased results. Secondly, case wise deletion can dramatically diminish the number of observations used in the final model estimation when this type of missing value treatment is used.

Instead of discarding all observations with missing values, pairwise uses all comments with complete responses to calculate the model parameters, for example, in a model with three indicators (RWD1, RWD2 and RWD3). All valid values in RWD1, RWD 2 and RWD3 are used in the computation to estimate the model parameters. If a respondent has a missing value in RWD3, the valid values in RWD1 and RWD2 are still used to calculate the model. Consequently, different calculations in the analysis may be based on different sample sizes, which can bias the results (Ringle et al., 2020). Rocco et al. (2003) point out that in most situations, LD and PD are ad hoc and notorious for biased or inefficient estimates. Since it is simple to use and is automatically selected as the default in most statistical tools, such as SPSS, this method gained widespread acceptance among researchers in the recent past. However, researchers have discovered that there are several drawbacks to using this technique, which has led to its demise in popularity. One of this method's most significant disadvantages is data reduction. Some researchers, therefore, call this approach “unwise deletions”, and experts also generally advise against its use.

Newer and more principled methods, such as multiple-imputation (MI), complete information maximum likelihood (FIML), expectation-maximisation (EM), Complete case analysis (CCA), hot-desk imputation and regression imputations, consider the circumstances in which missing data occurred and provide better parameter estimates than LD or PD (Drost 2011). Principled missing data methods do not directly replace a missing value. Instead, they combine available information from observed data with statistical assumptions to statistically estimate population parameters and the absent data mechanism. Complete case analysis (CCA) is a common approach and default in most statistics packages. Dealing with missing data in complete case analysis (Little and Rubin, 2019; Allison, 2009) restricts the analysis to individuals with unlimited data. An alternative to CCA is multiple imputations (MI), which creates copies of the dataset, replacing the missing values under a specific model. CCA is not biased by missing data when the data is MCAR because the complete cases are representative of those with missing data.

Contrary to the widespread belief that MCAR is required for CCA to be biased, CCA can give unbiased results in a situation where data is MAR or even MNAR. Little's MCAR test was conducted to assess whether the missing values occurred randomly. The test suggested that the missing values occurred entirely at random (P=1.00), suggesting that the problems were less serious (Tabachnick and Fidell, 2013). Based on this output, Expectation-Maximisation (EM) method was adopted to generate missing data values, as suggested by Tabachnick and Fidell (2013).

5.4.8 Selecting a Treatment Data Method and Justification

According to Feild (2018), statisticians recommend a few treatments for handling missing data, which researchers in business and management routinely ignore. It is sometimes relatively harmless to ignore the advice of statisticians in this way. Still, it can also be quite harmful at times, depending on the amount of missing data, the pattern of missing data and whether the data is missing in a highly systematic manner. Before in the previous section, 5.4.1, a different type of data treatment was mentioned. Further, Little's MCAR test was done, and it confirmed that the data was MCAR because it meets the expectation and expected range between (5%-30%), according to the advice of researchers (Ringle et al., 2020; Hair et al., 2019). Therefore, it has been discovered that most of the data treatment methods discussed can be used to treat the missing values. However, as mentioned in Section 5.4.1, most of these methods can produce skewed results and a loss of statistical power in some situations. For example, Listwise was considered a reasonable option, but it would have resulted in a loss of 10% of the data if it had been implemented. However, one could argue that the sample size could have remained relatively large despite the small number of participants. Despite this, the method was abandoned to avoid any bias and to ensure that the study's generalisability was maintained.

Pairwise was also eliminated from consideration because it was discovered that both techniques had the potential to produce biased results (Ringle et al., 2020; Hair et al., 2019). Complete case analysis (CCA)

is a common approach and default in most statistics packages. Hair et al.,(2019) propose that for dealing with missing data in complete case analysis which restricts the analysis to individuals with complete data, an alternative is multiple imputation (MI).As a result, the only two options left were EM and MI, both of which would have resulted in less biased results if they had been implemented (Hair et al., 2017; Tabachnick and Fidell, 2013). However, in this study EM was selected over MI, since it is easier to use and less complex compared to MI. EM unlike MI can be easily implemented using SPSS without the need for any additional software or the need for researcher inputs. It is discovered that both approaches produce similar results, and as a result, they concluded that neither approach was superior to the other. Thus, the missing data were treated with EM, which was then applied in the appropriate way.

5.4.9 Normality

Mishra et al., (2019) stated that it is well known that the data distribution must be checked prior to the application of any statistical tests. Lumley (2002) points out that normal distribution is a frequency distribution that represents the relative number of occurrences as each value of a variable. Lack of data normality has an impact on the study outcomes because it affects goodness fit indices and standard errors, which in turn affect the overall results of the CFA and structural model (Hair et al., 2017). Hair et al. (2017) add that the normality can be checked through observing the normal P-P Plots and standard residual histogram. The statistical approaches that assess univariate normality often begin with the measures of skewness and Kurtosis value that hover around zero, which are obtained through the explore procedure. As illustrated, the figures of some of the data appear to be normally distributed (with no notable difference between the tallest bar of the histogram and the bell-shaped normality curve). The following numerical and visual output must be investigated. Skewness and kurtosis z –values should be somewhere in the span of -1.96 or +1.96. On the other hand, Shapiro-Wilk test P –value should be above 0.05. Mishra et al., (2019) stated that histograms, Normal Q-Q plots and Box Plots should indicate that data is approximately normally distributed. In this study, the data is approximately normally distributed. Linearity needs the relationship between the independents and dependents variable to be linear. This means that with a scatter plot of scores one should see a straight line (roughly) not a curve.

5.5 Outliers

Outliers can cause increased error rates and significant misrepresenting parameter and statistics estimates in both parametric and nonparametric tests. Ringle et al., (2020) defines an outlier as an observation to arouse suspicions that a different mechanism generated it. According to the Dictionary of Statistics, outliers are an observation that appears to deviate markedly from the other observations of the sample in which it appears. An outlier is an observed value that is so extreme (either large or small) that it seems to stand apart from the rest of the distribution (Hair et al.,2019). Outliers significantly impact study results, particularly in studies with small sample size, according to social science and information science researchers (Hair et al., 2017). Outliers can arise from several different methods or

causes. In addition, outliers can occur in two categories: those arising from errors in the data and those deriving from the natural variability of the data.

5.5.1 Detecting outliers

Detecting outliers are not a new concern (Sarstedt et al.,2016, Saunders and Galletta 2016). Indeed, Sahin and Ozturk (2011) presented how significant results could easily be false positives if outliers are dealt with only flexibly and post-hoc. Saunders and Thornhill (2009) showed that researchers took insufficient care to detect outliers by employing ineffective methods or failing to report critical information about the detection process. They offer a reliable method for analysing univariate outliers. However, one will argue that this issue is also relevant for multivariate outliers.

5.5.2 Discussion

Looking at the result: the outliers were done by removing the extremes that represent the symbol (*) and retaining the (o) symbol. Some researchers have advised that outlier cases be removed from the study, the great majority of scholars have emphasised that outliers should always be kept ensuring generalisability to the overall population (Pallant 2020; Hair et al., 2017). In this study the outliers were retained using the winsorizing method to treat the outliers (Creswell and Creswell,2019). That is assigning outliers the next highest or lowest value found in the sample that is not an outlier.

5.6 Adequate Sample Size

It is essential when designinga study to have an acceptable sample size, or more precisely, sample power (Tabachnick and Fidell, 2013). The researchers estimate the minimum required sample size to achieve the maximum level of statistical control for a hypothesised effect size under a specified statistical significance level (Kyriazos, 2018) Thus, the sample size impacts the precision of all statistic estimates. It is generally accepted that problems may arise due to small sample size (Kyriazos, 2018). Instead, when the luxury of a large sample is available, a better research strategy is suggested (Kline, 2016). In addition, 498 suitable questionnaires were gathered in response to the researchers' recommendation based on sample size adequacy.

5.7 Construct Reliability

Nunnally (1978) defines reliability as the extent to which measurements are repeatable, i.e. consistency, stability, accuracy and dependability of the measurements regardless of the circumstances, environmental conditions, instruments and person performing the measurement (Andy 2018; Hair et al., 2017). They are methods to assess reliability such as Test-retested reliability, Split-halves, Inter-rater reliability, Internal consistency, Composite reliability and Cronbach’s alpha (a) (Drost, 2011). This is dependent on what sources of variation one considers important, such as the passage of time and the use of different items, when determining which reliability test to perform (Andy 2018). Internal

consistency (the degree to which items are related to one another) estimation, also known as Cronbach alpha, was assessed in the current study. Due to this decision, the primary concern for this study was the error factors associated with the use of multiple items (that is, how well a set of objects could measure a construct). The Cronbach's alpha value is used to determine the internal consistency of constructs, and it is calculated. The alpha value is determined by the degree to which each item on the scale is correlated with at least one other thing on the scale, as determined by the correlation coefficient (Drost, 2011). Alpha value closer to 1.0 suggests greater internal consistence of the items in the scale. According to Kline (2016), a threshold of 0.5 may be accepted for early exploratory work and psychological constructs because of the diversity of the constructs being measured in social science research. Hair et al. (2017) suggested that any value less than 0.7 may be acceptable, depending on the objectives of the study. It is preferable, however, if the reliability values are 0.7 or higher (Hair et al., 2017; Tabachnick and Fidell, 2013; Mertens 2019; Nunally, 1978). Low alpha values can be due to small number of items in the scale or a newly developed scale. Cronbach's alpha is widely used methods for estimating reliability; it can be easily implemented with the aid of SPSS and Smart-PLS as well, and there is no need to collect data twice.

Cronbach's alpha is a conservative measure of reliability. As a result, this method was chosen in order to estimate the reliability of the measured variables. A Cronbach's alpha value for a construct equal to or greater than 0.7 indicates high reliability for that construct (Hair et al., 2017).

5.7.1 Construct Validity

Construct validity is the extent to which a test measures the concept or construct that it is intended to measure. Construct Validity is classified into two types: Convergent Validity and Discriminant Validity (Hair et al., 2017).

5.7.2 Convergent Validity

The degree to which a measure correlates positively with other measures of the same construct is known as convergent validity (Hair et al., 2017). This means that all items in a construct should have a high degree of intercorrelation with one another and should share a high proportion of variance. To evaluate convergent validity of constructs, researchers consider the outer loadings of the indicators and the average variance extracted (AVE). SEM can be used to conduct the test SPSS; AMOS can also be used because it generates standardised loading estimates for each item within a construct, which are comparable to factor loading in SPSS. According to Hair et al. (2017), higher outer loadings on a construct suggest that the linked indicators share a lot of information, which the construct captures. The size of the outer loadings is also known as a reliability indicator. The outer loadings of the indicators should be statistically significant at a minimum. A typical rule of thumb is that standardised outside loadings should be 0.70 since a substantial outer loading can still be fairly weak (Hair et al., 2017), and some researchers stated that good convergent validity is indicated by standardised loading estimates of

0.5 or higher (Hair et al., 2019). Construct validity can also be assessed with AVE. The total of all squared standardised factor loadings divided by the number of items under that construct is the AVE value for that construct. Hair et al. (2010) found that AVE values of 0.5 or higher indicate good convergent validity.

5.7.3 Discriminant Validity

The amount to which a construct is distinct from other constructs according to an empirical criterion is referred to as discriminant validity. Thus, demonstrating discriminant validity implies that a construct is distinct from other constructs in the model and captures phenomena that are not represented by other constructs in the model (Hair et al., 2017). It implies that items belonging to one construct should have little in common with those belonging to others. When an item from one construct has a high correlation with items from another construct, this is an indication of a problem with discriminant validity (Henseler et al., 2015). When comparing AVE with Squared Interconstruct Correlations (SIC) (Hair et al., 2017). Discriminant Validity is more rigorously assessed. The AVE for a construct should be greater than the SIC associated with that construct to achieve discriminant validity (Chin et al., 2020; Hair et al., 2017). Pallant (2020) argues that in addition to considering indicator and construct reliability, a thorough validation procedure necessitates assessing the discriminant validity of a measurement (or structural) model.

In Smart-PLS, this is accomplished by determining whether the square root of the AVE for each latent variable is greater than the correlation between the variables (Peng and Lai,2012). Table 5.5 shows that all of the square roots of each AVE (bold values in the diagonal) are greater than the correlations between the latent variables, proving discriminant is established.

5.7.4 Constructs Reliability Test Result

The indicator reliability of the different scales is measured using the Cronbach's alpha method, where alpha values greater than or equal to 0.70 are an indicator of internal consistency and discriminant validity of the scales (Hair et al., 2019). Table 5.4 shows the reliability measures having Cronbach's alpha equal to or greater than 0.70. Cronbach's alpha was chosen as a tool for conducting the reliability test. Following the reliability test, it was discovered that it had no reliability problem because the Cronbach alpha for the construct some was 0.7 and higher than the acceptable threshold.

For internal consistency and reliability, researchers recommend using composite reliability as a measure of internal consistency and reliability. It is further suggested that the values should be 0.7 or higher, but 0.6 and higher could be acceptable if it is exploratory research (Hair et al., 2017). Table 5.4 shows the composite values were well above 0.7. Hence, it can be concluded the indicators are reliable and internally consistent.

The table 5.4 shows the successful factor analysis with reliable results. All the nine variables are reliable because Cronbach's alpha reliability statistics are high. This is robust and exceeds the requirement.

Table 5.12: Result of variables with Composite reliability, Cronbach's alpha reliability statistics

Construct	Composite Reliability	Cronbach's alpha
Information security threat in SC	0.914	0.885
Top management Support	0.890	0.855
Commitment	0.897	0.862
Reward	0.853	0.743
Sanction	0.924	0.901
Monitoring/Evaluation	0.928	0.899
Attitude	0.852	0.767
Subjective Norms	0.916	0.884
Self-Efficacy	0.933	0.909

5.7.5 Discriminant Validity Test Result

Henseler et al. (2015) explain that discriminant validity, which can be assessed at the construct and indicator levels, is concerned with whether constructs that are thought to be conceptually different are sufficiently different from one another. Using the Fornell–Larcker criterion, adequate discriminant validity is evident at the construct level if the AVE of a construct is greater than the highest squared correlation between that construct and each of the other constructs in the model (Hair et al., 2017; Henseler et al., 2015). In this study, this condition was met for all constructs. Cross-loadings can be used to assess discriminant validity at the indicator item level (Henseler, et al., 2015). To demonstrate adequate discriminant validity, an item's loading with the construct was designed to measure should be greater than its loading with other constructs, i.e. its cross-loadings (Ringle et al., 2020; Hair et al., 2017). However, in the absence of clear-cut loading thresholds when evaluating discriminant validity, the size of the difference between an indicator item's loading on its assigned construct and its cross-loadings should be considered. Adequate discriminant validity was demonstrated in this study because all items had significantly higher loadings for their respective constructs than for other constructs.

Table 5.13: Discriminant Validity

	ATD	CMT	INSC	M/E	RWD	SACT	SFE	SJN	TMS
ATD	***0.769***								
CMT	0.272	**0.771**							
INSC	0.235	0.247	**0.784**						
M/E	0.371	0.312	0.356	**0.804**					
RWD	0.314	0.752	0.273	0.308	**O.812**				
SACT	0.322	0.355	0.310	0.471	0.351	**0.818**			
SFE	0.477	0.409	0.360	0.343	0.448	0.402	**0.822**		
SJN	0.326	0.312	0.271	0.455	0.299	0.649	0.318	**0.828**	
TMS	0.272	0.775	0.246	0.321	0.752	0.466	0.383	0.267	**0.759**

Table 5.14: Outer loading of construct

Items Outer Loading		Items Outer loading	
ATD 1 – Attitude	0.693	TMS 1 - Top Management Supt	0.706
ATD 2 - Attitude	0.738	TMS 2 - Top Management Supt	0.734
ATD 3 - Attitude	0.794	TMS 3 - Top Management Supt	0.782
ATD 4 - Attitude	0.841	TMS 4 - Top Management Supt	0.777
CMT 1 - Commitment	0.846	TMS 5 - Top Management Supt	0.793
CMT 2 - Commitment	0.830	TMS 6 - Top Management Supt	0.793
CMT 3 - Commitment	0.711	SJN1 1 - Subjective Norms	0.750
CMT 4 - Commitment	0.775	SJN 2 – Subjective Norms	0.782
CMT 5 - Commitment	0.720	SJN 3 – Subjective Norms	0.871
CMT 6 - Commitment	0.732	SJN 4 Subjective Norms	0.880
INSS 1- Infor Sec threat in SC	0.395	SJN 5 – Subjective Norms	0.850
INSS 2 - Infor Sec threat in SC	0.775	SCT 1 – Sanction	0.852
INSS 3 – Infor Sec threat in SC	0.833	SCT 2 Sanction	0.822
INSS 4 - Infor Sec threat in SC	0.895	SCT 3 Sanction	0.778
INSS 5 – Infor Sec threat in SC	0.818	SCT 4- Sanction	0.800
INSS 6 – Infor Sec threat in SC	0.875	SCT 5 Sanction	0.814
INSS 7 – Infor Sec threat in SC	0.783	SCT 6 Sanction	0.841
M/E 1 – Monitoring/Evaluation	0.918	SFE 1 – Self-efficacy	0.905
M/E 2 – Monitoring/Evaluation	0.877	SFE 2 – Self efficacy	0.923
M/E 3 - Monitoring/Evaluation	0.900	SFE 3 - Self -efficacy	0.938
M/E 4 - Monitoring/Evaluation	0.858	SFE 4 – Self -efficacy	0.872
M/E 5 – Monitoring/Evaluation	0.816	SFE 5 - Self- efficacy	0.681

M/E 6 – Monitoring/Evaluation	0. 031	SFE 6 – Self -efficacy	0.423
M/E 7 – Monitoring/Evaluation	0.815	SFE 7 – Self -efficacy	0.875
M/E 8 – Monitoring/Evaluation	0.829		
RWD 1 - Reward	0.773		
RWD 2 - Reward	0.815		
RWD 3 - Reward	0.846		

5.7.6 Hypotheses Test Result

The last step was to evaluate the causal linkages (hypotheses) between the latent constructs after creating a suitable model. This was done by looking at the estimated path coefficients, standard errors and t-values. The strength of the associations between the latent construct is reflected in the path coefficient estimations.

Evaluation of the structural component of the model involved examining the amount of variance explained for each dependent variable, as well as the sign and significance of the path coefficient. Calculations were performed with Smart-PLS 3 using the PLS algorithm bootstrapping resampling procedure. The results obtained for the structural model are presented in table (5.7). The table illustrates those paths that were found to be both statistically significant and non-significant and reports the path coefficients, P-value, hypotheses and R^2. The plus and arrow signs associated with the calculated path coefficients can be used to determine the direction of the relationships, with (+) indicating positive correlations and (-) indicating relationships between the indigenous and exogenous factors. The hypothesis outcomes are summarised in Figure (1). Table 5.7 provides more information.

Table 5.15: Summary of hypothesis results

Hypothesis	Construct	Relationship	Construct	Original Sample	Sample Mean	Standard Deviation	T- Statistics	P-Value	Symbol (*)	Support
H1a	SCT	→	ATD	0.144	0.145	0.056	2.589	0.010	*	Yes
H1b	SCT	→	SJN	0.347	0.342	0.094	3.687	0.000	***	Yes
H1c	SCT	→	SFE	0.034	0.035	0.071	0.483	0.517		No
H1d	SCT	→	ISTSC	0.131	0.138	0.139	0.945	0.345		No
H2a	CMT	→	ATD	0.137	0.141	0.052	2.647	0.008	**	Yes
H2b	CMT	→	SJN	0.012	0.013	0.051	2.242	0.809		No
H2c	CMT	→	SFE	0.168	0.173	0.071	2.381	0.001	**	Yes
H2d	CMT	→	ISTSC	0.131	0.138	0.139	0.946	0.345		No
H3a	ATD	→	ISTSC	0.194	0.177	1.256	0.154	0.878		No
H3b	SJN	→	ISTSC	-0.114	-0.121	0.062	1.845	0.026	*	Yes
H3c	SFE	→	ISTSC	0.007	0.006	0.037	1.193	0.845		No
H4a	TMS	→	ATD	0.193	0.197	0.058	3.349	0.001	**	Yes

H4b	TMS	⟶	SJN	0.049	0.053	0.055	0.880	0.334		No
H4c	TMS	⟶	SFE	0.237	0.236	0.058	4.114	0.004	**	Yes
H4d	TMS	⟶	INSC	0.244	0.245	0.058	4.247	0.020	*	Yes
H5a	RWD	⟶	ATD	0.196	0.185	0.086	2.268	0.024	*	Yes
H5b	RWD	⟶	SJN	-0.229	-0.228	0.083	2.774	0.012		Yes
H5c	RWD	⟶	SFE	0.027	0.026	0.119	0.227	0.853		No
H5d	RWD	⟶	ISTSC	0.946	0.949	0.082	11.533	0.000	***	Yes
H6a	M/E	⟶	ATD	0.172	0.174	0.058	2.938	0.003	**	Yes
H6b	M/E	⟶	SJN	0.455	0.459	0.063	7.259	0.000	***	Yes
H6c	M/E	⟶	SFE	0.236	0.237	0.058	4.052	0.000	***	Yes
H6d	M/E	⟶	ISTSC	0.226	0.226	0.061	3.702	0.020		Yes

*p-value for the inner model (*p<0.05, **p<0.01, ***p<0.001)*

The SEM investigation results provide solid evidence for supporting H1a and H1b under the GDT, because sanction severity and attitude, sanction severity and subjective norms were both found to be positively related to information security threats in the supply chain (SCT → ATD = 0.010 at P< 0.001, CT → SJN=0.000, at p<0.001). No positive and direct relationship between sanctions severity and self-efficacy, sanction severity and information security threats in the supply chain (SCT →SFE=0.517; SCT → ISTSC = 0.345). There is supporting evidence for SBT this is because there is signification relationship between commitment and attitude as well as commitment and self-efficacy (CMT → ATD = 0.008 at P < 0.001, CMT → SFE = 0.001 at P<0.001). During the model modification stage, another path between commitment and information security threats in the supply chain was added and the relationship was found not to be significant and the relationship between commitment and subjective norms has no significant relationship too (CMT → SJN = 0.845, CMT → INTSC = 0.345). Furthermore, the variables in TPB have no direct relationship with information security threat in the supply chain (ATD → INTSC=0.878, SFE → INTSC 0.845) except subjective norms that has a positive relationship with information security threats in the supply chain (SJN → INTSC = 0.026 at P<0.001). Top management support has positive relationship with (TMS → ATD = 0.001 at p<0.001) and this evidence support H4a, (TMS → SFE=0.004 at p=0.001) H4c and (TMS → INTSC =0.020 at <0.001) H4d. Surprisingly, top management support has no direct relationship with Subjective norms (TMS → SJN = 0.334) with supporting evidence H4b. In addition, the construct reward has a significant relationship with (RWD → ATD =0.024 at p <0.001) and this support H5a, (RWD →SJN = 0.012<0.001). H5b, (RWD → INTSC=0.000 at p<0.001). Reward has no positive relationship with self-efficacy (RWD →SFE = 0.853) H5d. The analysis provided evidence supporting all the hypotheses on monitoring/evaluation. A positive relationship was found in (M/E → ATD = 0.024, at p<0.001), (M/E → SJN=0.000 at p< 0.001) (M/E SFE 0.000 at p< 0.001), (M/E → INTSC=0.000 p<0.001) this evidence supports H6a, H6b, H6c and H6d.

Table 5.16: Summary of the findings in Relation to Hypothesis

Hs	Hypothesis	
H1a	There is a positive relationship between sanction severity and attitude to information security threats in the SC	Yes
H1b	There is a positive relationship between sanction severity and subjective norms in information security threats in the SC	Yes
H1c	There is a positive relationship between sanction severity and self-efficacy in information security threats in the SC	No
H1d	There is a positive relationship between sanction severity and information security threats in the SC	No
H2a	There is a positive relationship between commitment and attitude in information security threats in the SC	Yes
H2b	There is a positive relationship between commitment and subjective norms in information security threats in the SC	No
H2c	There is a positive relationship between commitment and self-efficacy in information security threats in the SC	Yes
H2d	There is a positive relationship between commitment and information security threats in the SC.	No
H3a	There is a positive relationship between attitude and information security threats in the SC.	No
H3b	There is a positive relationship between subjective norms and information security threats in SC.	Yes
H3c	There is a positive relationship between self-efficacy and information security threats in the SC.	No
H4a	There is a positive relationship between top management support and attitudes in information security threats in the SC	Yes
H4b	There is a positive relationship between top management support and subjective norms in information security threats in the SC	No
H4c	There is a positive relationship between top management support and self-efficacy in information security threats in the SC	Yes
H4d	There is a positive relationship between top management support and information security threats in the SC	Yes
H5a	There is a positive relationship between reward and attitude in information security threats in the SC	Yes
H5b	There is a positive relationship between reward and subjective norms in information security in the SC	Yes
H5c	There is a positive relationship reward and self-efficacy in information security threats in the SC	No
H5d	There is positive relationship between reward and information security threats in the SC	Yes
H6a	There is a positive relationship between monitoring/evaluation and attitude in information security in the SC	Yes
H6b	There is a positive relationship between monitoring/evaluating subjective norms in information security threats in the SC	Yes
H6c	There is a positive relationship between monitoring /evaluation and self-efficacy in information security in the SC	Yes
H6d	There is a positive relationship between monitoring/evaluation and information security threats in the SC	Yes

Yes ⟶ *Supported*
No ⟶ *Not Supported*

5.8 Qualitative Data Analysis

As mixed-method research, this study comprised of quantitative and qualitative aspects. The quantitative discussion was presented in Section 5.2 of this chapter. This section focuses on qualitative data analysis and its result. While there are no strict rules for the study of qualitative data, it largely depends on the researchers' judgement, intuition and ability to highlight issues (Carcary, 2016).

In this research, content analysis was used to analyse interview transcripts to complement the results from the quantitative data analysis. Content analysis aimed to attain a broad description of a phenomenon through concepts or categories. It is a systematic and objective analysis technique (Elo et al., 2014). Different words and phrases that share the same meaning are grouped into the same categories. The reliability of the analysis can be increased by crafting a link between the results and the data which could be done by describing the analysis process in as much detail as possible. Content analysis is a flexible analysis tool and requires the researcher's skills, insights and analytical abilities cautiously to come up with valid and reliable result (Elo et al., 2014).

Interviews were conducted with four groups of companies in the supply chains: manufacturers, distributors/logistics, marketing and operation. Open ended questions were asked followed by probes to explore participants' opinion on the subject matter (Burnard et al., 2008; Hsieh and Shannon, 2005). All interviews were recorded and transcribed verbatim. Since the aim is to test previous theories, deductive content analysis was employed. The themes of the interviews were pre-determined based on the previous knowledge. However, it remained open to new topics that might emerge from the interviews. Due to the small size of participants (nine interviewees), a manual contents analysis technique was used rather using any qualitative data analysis software such as N-vivo (Carcary,2016).

5.8.1 Response Rate and Demographics

From the list of medium and large-scale supply chain companies in Nigeria, 15 companies were chosen for interviews. The selected sample represents 15 companies that operate at different stages of supply chains. When the researcher contacted the companies for the survey, the respondents were asked if they would be able to do an interview on the same subject matter as the survey. Out of the selected fifteen companies, nine agreed to do the interviews. The nine interviews were designated as participant 1, 2, 3, 4, 5, 6, 7, 8 and 9, respectively. The participation of nine companies from a sample size of fifteen, response rate of 60 percent. Of the remaining six companies, four did not participate in the interview due to time constraints as the survey had already taken enough of their time. While their busy schedule was one of the prime reasons for the rejection of four interviews, the remaining two interviews could not be conducted due to time limitations. The proposed dates by the two companies were beyond the researcher.

Table 5.17: Result of interview

Interviewees	Main Business	Years of Est.	Position	W/experience	No of Employees
11	Manufacture-food	>20 Years	IT expert	>10 Years	120
12	Manufacture-Tobacco	>20 Years	Senior manager	12 Years	200
13	Manufacture-drinks	>20Years	Senior manager	>10 Years	<500
14	Manufacture-drinks	>20years	Senior IT manager	16 Years	400
15	Manufacture-cement	25 Years	Senior IT manager	15 years	225
16	Logistics	<20	Station manager	<20	120
17	Logistics	22 Years	Station Manager	<20	<100
18	Marketing	<10	Marketing Manager	>10	100
19	Distribution	<10	CEO	15 years	<10

5.8.2 Data immersion, Reduction (coding) and Representation

The content analysis method was used to analyse the qualitative data. A thorough reading of the transcribed data was performed in the first stage, with the goal of developing a general understanding of the information. Following the reading of the transcripts, notes were made in the margins of the transcripts to link the thoughts that had been triggered to the relevant themes in the transcripts. According to Creswell (2017), a theme is something that captures important information from the data in relation to the research question. All the pre-identified themes that emerged while reading the transcripts and could be used to explain the research and its context were highlighted. Then, the highlighted passages were first condensed and then coded using the predetermined codes based on the questions asked in the interviews. The rationale for using the predetermined codes was to check whether the responses correspond to the various factors identified in the literature. Text that could not be categorised with the initial coding scheme was given a new code. In addition, there were instances when the participants talked about something that was not related to the topic under study and, hence, careful attention was paid as to looking for only those contents that have relevance to the research (Bell, Bryman and Harley 2022).

When data is coded, the goal is to reduce the amount of information by categorising it into different categories in a way that makes interpretation easier and allows the researcher to address the research questions. First, the information was divided into 9 categories. In Microsoft Excel, a data display matrix was created, with analytically meaningful themes displayed vertically and the cases or participants displayed horizontally across the top. Texts summarising the characteristics of the theme are placed in each cell of the matrix to create a visual representation of the information. To draw preliminary

conclusions, it was necessary to examine the matrix and identify patterns in the data that would lead to additional coding.

The iterative coding process continued with the second stage where the initial nine themes were compressed into four main pieces: information security, employee perception factors mitigating information security threats, communication tools and IT, and the effect of information security in the supply chain. The aim was to combine or synthesise the more minor themes into major themes that would result in a high-quality conceptualisation. With these four themes, the researcher aims to find out 1) Their view about information security; 2) Information security threats; 3) employees' perception of mitigating threats (attitudes, subjective norms and self-efficacy); and 4) factors mitigating information security threats; Top management, commitment, reward, sanction, monitoring/evaluations.

5.8.3 Qualitative result

In qualitative research, the results are derived directly from the analysis and discussion of the evidence gathered, particularly in relation to the emerging themes from the data (Creswell and Clark, 2011). To ensure the credibility of the findings, several strategies were employed, such as including specific quotes from participants, utilizing multiple data sources to provide diverse evidence, and presenting various perspectives to showcase differing viewpoints within the study (Creswell and Clark, 2011). The present study utilized the nine themes identified in the previous section as a framework for analysing the results.

Information security threats in the supply chain

The findings indicate that information security plays a crucial role in enhancing coordination and safeguarding information among supply chain companies (Maskey et al., 2017). Five interviewees expressed the belief that protecting information assets provides a competitive advantage for firms. Consequently, they prioritize internal information security measures to prevent unauthorized access by third parties. For instance, participants P11, P12, P13, P14, P15, and P18 emphasized the importance of securing the foundation and integrity of the supply chain to derive maximum benefit. Participant 16 further emphasized this viewpoint, stating."

"*It will not make sense if you cannot secure information*".

The interviewees perceived that information, when secure, will provide mutual benefits, improve coordination, strengthen the relationship, improve business and help in decision making to improve supply chain performance (P11, P12, P13, P14, P16 and P19). The majority of the participants believed that information security threats are important to reduce so as to improve their business. One participant mentioned that it is because of the strength of supply chain that doing business in the present context is impossible (P18). Another participant (P19) considered it as an integral part of his business.

On information security threats, interviewees believed that even though people are aware of threat in the supply chain in information security, they are not preventing it enough. While the awareness is there, some firms do prefer to invest more on technology because they still believe that technology can do what is necessary. According to one interviewee, the status of information security in the firm is neither very good nor bad. Another manager (P19) believed that:

"*The importance given to information security is increasing now as people have realised.*

Its significance".

Almost all organisations gave restricted access to all employees to the information system/computer. Though there was also joint agreement in standards and policies to protect information and information systems, some of the firms believed they operated in a very trusting and peaceful environment as far as IS in SC is concerned (P11). Another (P19) believed that:

"The threat is not harmful in this firm because of the different levels of access".

- **Sanction**

Sanction severity is defined by principles derived from GDT. According to Merhi and Ahluwalia (2019), sanction is an essential construct of the GDT. Sanctions deter potential offenders from unlawful behaviour. The degree of illegal behaviour reduces as sanctions rise. In the organisational context, the interviewees believed that management has a generalised attitude towards reducing or preventing information security threats in their supply chain network. This is to say that because some employees do not comply, sanctions have to be implemented. In the comments below there is evidence that the employees believed that there should be a sanction put in place by the firms to reduce threats in the system. This belief is in line with Cuganasen (2018), who argues that sanction is a necessary construct that can affect employees' violation intentions. Hence, it can be inferred that the respondents consider sanction as a factor impacting on their behaviour towards reducing information security threats.

"*If you don't follow the rule you need to be punished" (P11).*

"The sanction is capital in the sense that it is the sack" (P12).

"The fact is that they know that their rule will terminate their appointment" (P19).

- **Commitment (SBT)**

Commitment has gained much interest in the field of management and behavioural sciences because of the predictable outcomes of commitment. Nature and the commitment concept believe that a person has a sense of responsibility to the organisation he or she works for (Safa et al.,2018). According Ifinedo(2014), commitment can be defined as a set of internal thoughts and feelings, or as a set of

intents, that strengthens an employee's desire to stay with the company and accept its major aims and values. In line with this argument, the data shows that the employees collectively believe that their commitment exerts a strong influence on what they should do and how they should behave as far as security of information is required. A common theme was that they all wanted to be seen as employees who are committed to their task in order to build a secure environment free from threats. The following comments are evidence that commitment is a relevant factor in this research context. The comment below provides support evidence for H2c Two comment of interviewee:

"I am definitely committed to ensuring that everything is secure because if anything happens to the network it comes back to bite me hard" (P18).

"*Very committed because information is key, and I am a strong believer and strong advocate of information security*" (P12).

Analysis led to the inference that to prevent or reduce information security threats in the industry, the respondents felt they had to be committed to the security requirement. The way to prove that to their firms was ensuring that their information flow was without leakage. Hence, it can be inferred that commitment influences the mitigation of information security threats.

"*It is depending on their perspective of work, and you can really tell because you know them, and you don't know their perspective at work*".

"*All I can say is that the system that was put in place at least reduces the threat of whether they want to comply or they don't want to comply based on lay down rules".*

- **Attitudes**

On attitude, studies based on planned behaviour theory show that individual behaviour is influenced by attitude, subjective norms and self-efficacy (Ifinedo, 2012). Many behavioural studies have used perspective to explain behavioural intentions. When a perspective successfully elicits a significant mitigation of threats, cognitive processes employ strategic responses to avert the threat as a result of the attitude towards it (Susanto et al., 2011). The interviewees understood there were information security threats, and they know the implication, such as loss of reputation, can halt the system and so on. The value placed on information security in their supply chain enables them to rethink how they handle information and information systems. One interviewee commented:

"*In my company, we place very high value and priority to information security. I do support the protection and safeguarding of information* (P13).

Hence it can be inferred that there is positive attitude among the respondents, proving the relevance of attitude in the given context.

- **Subjective norms**

Subjective Norms refer to the expectation that a well-known person or group of people will endorse and support a particular behaviour or an individual's perception of what people important to them think about a given behaviour (Ifinedo, 2014). The interviewees believe that senior managers, friends and colleagues have high expectations towards them to protect information and prevent information security threats (Humaid and Balakrishnan, 2018). This indicates the relevancy of subjective norms in the given context. One interviewee commented:

"*Because they have particular role expectations of me and believe that I am highly competent to live up to those expectations, thus, I guard my conduct all the time to ensure that I do not perform below their expectations" (P12).*

- **Self-efficacy**

Self-efficacy and information security are interrelated and interdependent (Ifinedo, 2014). The participant confirmed that self-efficacy is a factor that is necessary to reduce information security threats in the supply chain**.** The interviewees stated that they are led to believe that information provided is accurate and complete and they have the skills to prevent threats. As the comment below exemplifies, there was general understanding among the respondents when the vulnerability of the supply chain network is high, there is tendency of high self-efficacy with the employee the comment below by three interviewees was supported for H2c.

"It is not negotiable if the expertise helps" (P11) so proficiency is highly needed" (P15).

"Expertise and proficiency help me to protect my company information asset by equipping with the requisite skills, knowledge and experience I need to perform my tasks well" (P12).

"*Confident*" (P16).

- **Top management support**

Interviewees agreed that their top managers were aware of the security requirements of the firms. The companies were also commonly concerned about information that if gets into wrong hands or leaks due to threats, it could result in loss of reputation and loss of customers to one of their competitors. The interview data reveals that in order to keep their information asset secure, the top managers that were interviewed ensured that they closely followed their employees as much as they could within their means. Pattinson et al. (2015) pointed to the level of supervision and support from top management as

a determining factor in outcomes of performance and functions. Thus, the interview data suggests that top management support influence plays a role in reduction of information security threats in their supply chain:

"*I can say that for top management is more or less of total 100%, because they are the top most people in the company you want to give because you have a lot to lose if anything happens, any way at that length to give almost everything to secure the network" (P11*)

"*That is the first thing you will be introduced to as a modus operandi, once you get into the system and you are employed you are already given the guidelines, that once you violate you already know the implication of the system, some might even lead to legal issues. But it is a lay down rule that people know, even if you are coming in as a fresher." (P16*).

- **Rewards**

Rewards contribute to the shaping of employees' attitude towards information security. Hashim et al. (2015) stated that the process of rewards captures a variety of actions geared towards maintaining confidentiality and control. The interviewees believed that reward plays a major role in the system. As the comment below exemplifies, there was general understanding among the respondents that if there was reward, information security threats will not be severe. For example, amongst the interviewees, three companies (P12, P16 and P18) always reward their staff for reporting the traces of threats and sanction any staff that default. From the responses it can be inferred that reward is an industry package; thus reward is relevant to this context. One interview comment

"I think it reduces it because once award is given to a member of staff, it encourages you going ahead with whatever you want to do that will help the firm" (P12).

Monitoring /Evaluation

Monitoring/evaluation is a well-known and critical practice in information security. Studies suggest that monitoring behaviour and actions is a fundamental action upon which phase developments and processes advance in any organisational function, such as information security (Cugansan et al., 2018). The majority of the participants felt that monitoring and evaluation is a relevant factor to explore in this context. The comment below by two interviewees was supported for H6a, H6b, H6c and H6d.

"*The review every month through the meeting*" (P19).

"*Well by checking the updated weekly or monthly of what goes around*" (P13**).**

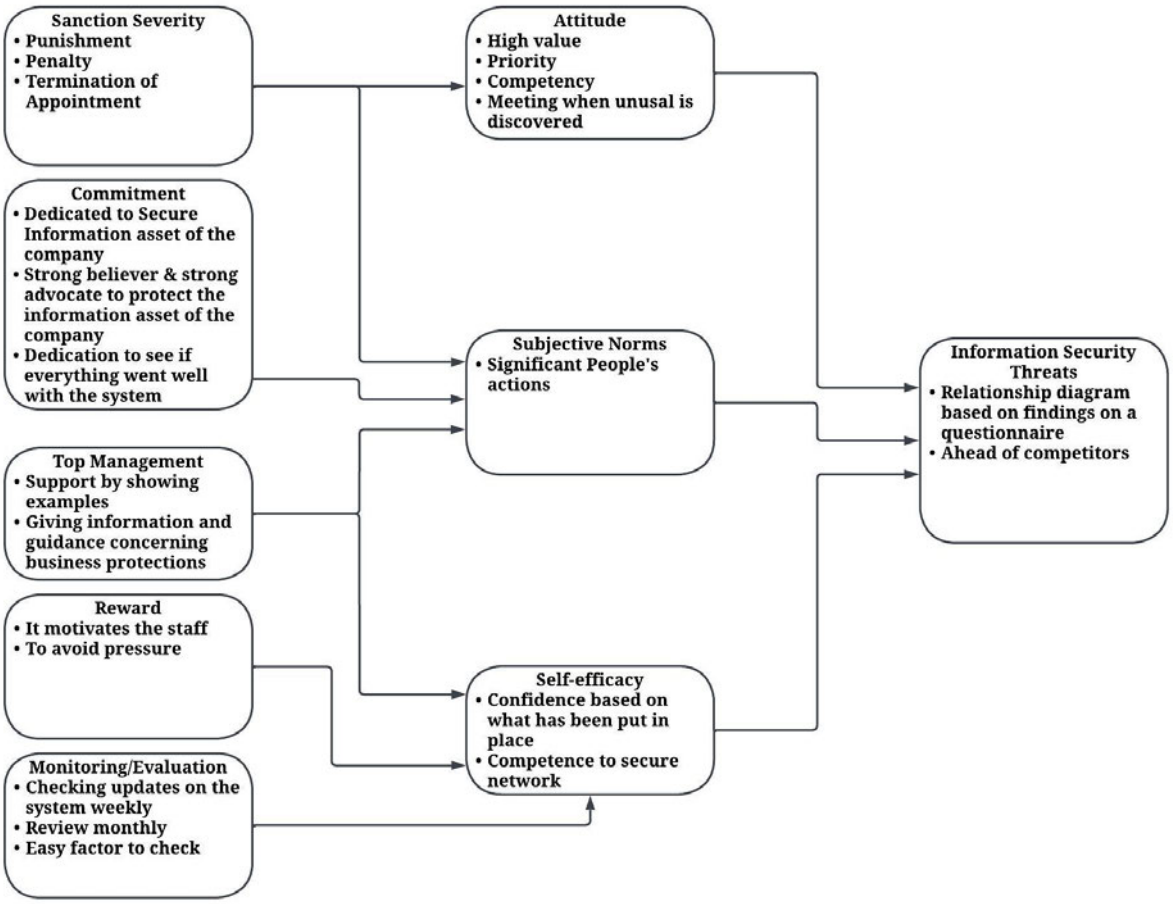


Figure 5.3: Connection of Qualitative Results

The analysis results, depicted in Figure 5.3, align with the broad categories outlined in the conceptual model shown in Figure 3.1 and the hypotheses presented in the table. This finding serves to confirm and validate the constructs identified from the literature, which were utilized to develop the conceptual model.

- **Summary**

This chapter detailed how this study's quantitative and qualitative data was analysed to answer the research questions. The procedure of quantitative data analysis was explained first, followed by qualitative data analysis. Convergent validity, discriminant validity, Cronbach's alpha for reliability testing and path coefficient to examine the link between constructs were all part of the quantitative analysis phase**.**

First, the data coding and data screening/cleaning processes were explained to prepare the data for future analysis in SPSS. The demographic data was analysed to determine the respondents' appropriateness. Most of the respondents are manufacturers, who, compared to other business sectors (operation/ distribution, marketing. logistic/transport), operate rather large enterprises in Nigeria. Other industries are often modest or medium-sized, with a few significant players.

The measurement instrument was evaluated based on the measured items' reliability, convergent validity and discriminant validity. To establish the survey instrument's validity, exploratory factor analysis was performed nine times, eliminating a different item each time. Using this method, the researcher was able to compare different factor structures and choose the best one. A factor's structure with sixteen factors was derived after eliminating items with loadings below 0.5 and those with cross-loadings. Convergent and discriminant validity were both confirmed when all items loaded considerably and substantially on their underlying constructs. For each construct, Cronbach's alpha values were determined. All had alpha values greater or equal to 0.7, which shows that it met the threshold.

To supplement the quantitative results, content analysis was utilised to analyse the qualitative data. Information security, attitude, subjective norms, self-efficacy, top management support, commitment, sanction, reward and monitoring/evaluation were all identified as important factors influencing the mitigation of information security threats by the interviewees. It explained how supply chain players felt about information security threats and how it affected their supply chain system and performance. While the qualitative findings matched the quantitative findings, they revealed additional characteristics that were not detected numerically.

Chapter 6: Discussions

6.1 Introduction

Underpinned by three theories (GDT, SBT and TPB), this research proposed a theoretical framework for factors mitigating information security threats in the supply chain. The chapter provides a detailed discussion of the key research findings presented in Chapter 5. The discussion findings will be organised based on the research questions. Following the first research question, 6.2 will discuss how supply chain companies mitigate information security threats in the supply chain. 6.3 will discuss the factors that effectively influence employees' behaviour and what factors mitigate information security threats in the supply chain. It also presents the study findings in connection to previous studies. The sections provide a detailed discussion on the hypothesis result.

- **The overarching research question:**

How do the supply chain companies mitigate information security threats in the supply chain?

Sub research questions

[RQ1] What are the factors that effectively influence employee's 'behaviour'?

[RQ2] What factors mitigate information security threats in the supply chain?

Figure 6.1 shows the research model used to seek answers to the research questions and which of research hypothesis developed were supported. The model shows the p-values and the R^2 values from the analysis. The p-values represent the coefficient of the structural path that explains the strength of the path, while the R^2 value represent the explanatory power of the endogenous variable. In the following subsections, the discussion, of the findings is geared towards answering the above question. In the discussion, these p-values alongside with R^2 are used to explain the significant of the endogenous variable influence on exogenous variable.

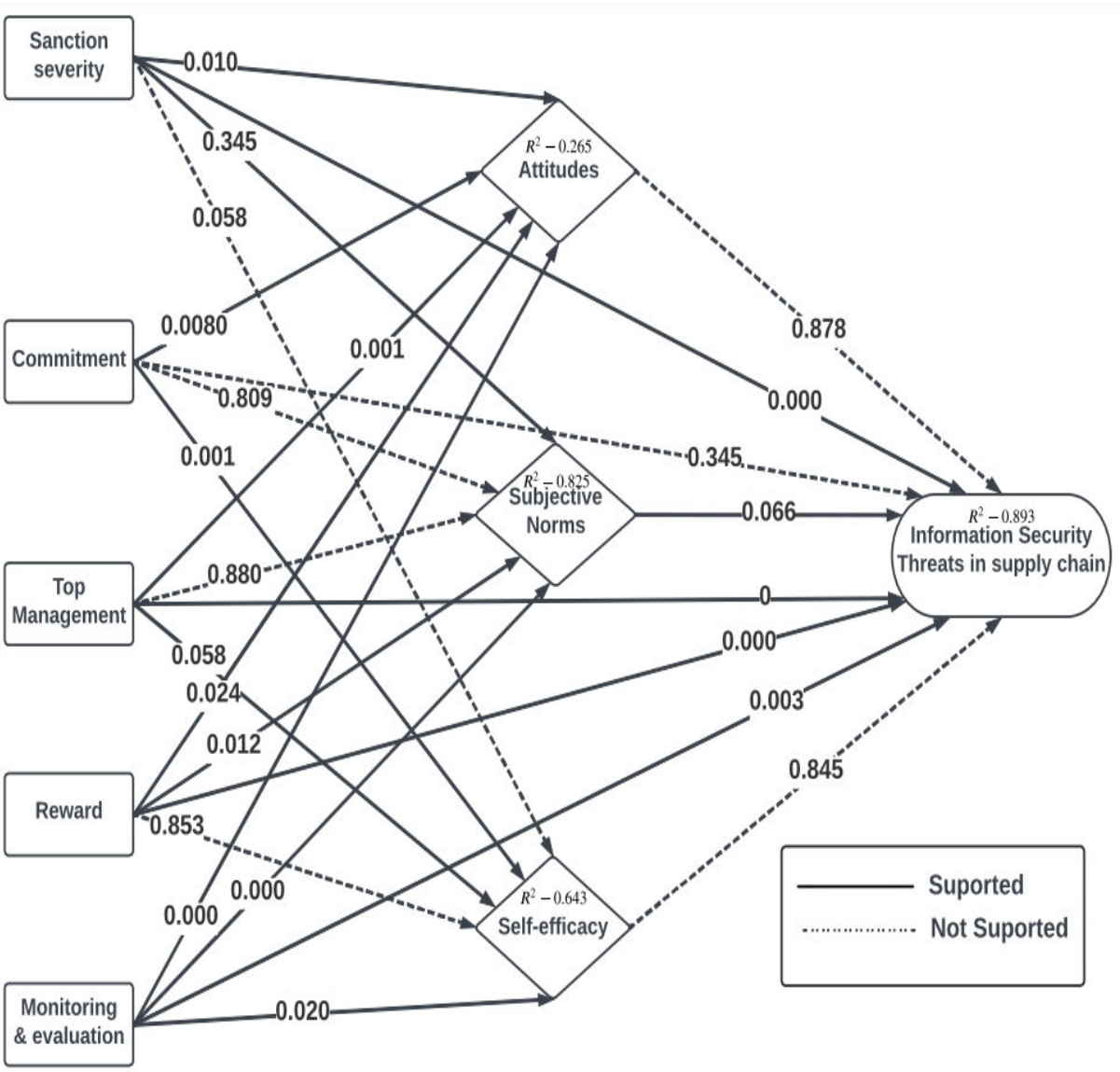


Figure 6.1: Research Model

- **Overarching Research Question**

How do the supply chain employees mitigate information security in the supply chain?

The literature identified that the human factor represents an essential issue in information security in organisations, as the human factor determines the employees' behaviour towards information security (Alhogail et al., 2015). This study shows that employee influence can mitigate supply chain threats. Based on the way information security threats are measured for this research, using operationalisation of this construct (Spears and Barki 2010; Workman et al.,2008), responses showing a higher level of interest in their attitude affect their behaviour through identification of the threats and active monitoring of the system and information asset. In this respect, this study's findings align with the literature, where employees attempt to exhibit activities superfluously to prevent threats (Safa et al., 2018).

- What are the factors that effectively influence employee's 'behaviour'?

6.2 Attitudes

The literature suggests that an individual's positive or negative feelings towards a behaviour can be expressed through their perception of a place, person, or situation (Herath and Rao 2009a). The research model was developed to investigate whether top management support has a positive impact on attitude, which, in turn, leads to a reduction in threats within the supply chain. However, the moderately explaining R^2attitude = 0.257 indicates a relatively low explanatory power, suggesting a prevailing low level of attitude within the supply chain environment.

Interestingly, the findings indicate that a positive attitude is associated with a higher level of positive information security behaviour among employees, resulting in a decrease in information security threats within the supply chain. This is supported by the significant relationship observed between attitude and information security threats (β=0.878, t=0.154). These findings contradict the results of several previous studies that identified a positive relationship between attitudes and information security (Passfaro, 2020).

6.2.1 Subjective norms

The analysis reveals that the variable of subjective norms can be substantially explained by the exogenous variables, as indicated by the R^2value of 0.825. The findings suggest that employees' perception of social pressure and intention to conform to certain behaviours are inclined towards reducing information security threats (β = 0.066, t = 1.154, p < 0.001). Surprisingly, the results indicate that subjective norms play a much more significant role in mitigating information security threats than what is commonly perceived by most researchers. Subjective norms directly and significantly impact information security threats within the supply chain.

These findings are consistent with the research conducted by Safa et al. (2019), which identified the influence of subjective norms on individuals' intentions to avoid security misbehaviour. They also align with the findings of Herath and Rao (2009a), who concluded that social influence has a significant effect on security behaviour. Additionally, the pressure to comply with norms is recognized as an effective deterrent according to Ifinedo (2014).

6.2.2 Self-efficacy

The analysis indicates that the variable of self-efficacy is moderately explained by the exogenous variable, as reflected by the R^2 value of 0.643. The findings further reveal that individuals with a higher perception of self-efficacy are more confident in their ability to gather the necessary drive and take appropriate actions to complete a task ($\beta = 0.007$, $t = 1.193$, $p > 0.05$). This suggests that a greater sense of self-efficacy leads to the minimization of threats in information security within the supply chain.

These findings align with the study conducted by Rajivan et al., (2017), which found that when individuals possess self-efficacy regarding the protection of organizational information assets, the impact of reducing threats is positively influenced. They are also consistent with the findings of Bulgurcu et al. (2010), who concluded that cognitive resources such as self-efficacy have a significant impact on employees' confidence in their abilities to safeguard systems against various threats. Moreover, the pressure for prudent behaviour control, coupled with self-efficacy, serves as an effective deterrent according to (Cai et al.,2010)

Workman et al., (2008) and Bandura (1986) explain that individuals with high levels of information security self-efficacy are better equipped to protect themselves from breaches in supply chain information security. They can take preventative measures and identifying security breaches even in the absence of assistance or prior experience with similar circumstances. Therefore, this study demonstrates that by influencing users' motivation and behaviour, self-efficacy in information security among system users can promote better end-user behaviour and enhance security effectiveness.

- **Research Question 2**

What factors mitigate information security threats in the supply chain?

6.3 General Deterrence Theory (GDT)

This research study is grounded in the principles of General Deterrence Theory (GDT), which has proven to be a valuable framework. Initially developed to explain how to discourage individuals from

engaging in deviant behaviour, GDT was originally applied to control criminal behaviour in the supply chain. The underlying premise of GDT suggests that imposing harsher punishments can effectively reduce criminal behaviour. Scholars have also successfully utilized this theory to examine employees' intention to comply with Information System Security (ISS) policies (Cheng et al., 2013). In line with this, GDT is also employed in the present study.

Based on the theory, it is postulated that individuals' criminal behaviour regarding information security threats in the supply chain can be deterred through sanctions. Drawing from GDT, one specific factor, namely Sanction Severity, is hypothesized to positively influence attitude, subjective norms, self-efficacy, and information security threats in the supply chain (H1a, H1b, H1c, and H1d). The results and implications of these hypotheses are discussed in the subsequent sections.

6.3.1 Sanction severity and attitude

H1a: There is a positive relationship between sanction severity and attitudes in reducing information security threats in the SC.

Sanction severity in the context of information security refers to the extent of punishment an offender will face for intentionally engaging in acts such as cyber loafing, social threats and the misuse of misuse of information employees, negligence (D'Arcy et al., 2009). In this study, sanction severity is defined as a control behaviour aimed at mitigating information security threats in the supply chain, following the framework development stage discussed in Chapter 3.

Previous studies have consistently found that sanction severity has a positive impact on attitudes towards reducing information security threats in various organizations, encompassing compliance, non-compliance, policy violation, and non-violation of information security measures (Merhi and Ahluwalia, 2019). In line with these findings, the current study's statistical results demonstrate that individuals' attitudes towards reducing information security threats in the supply chain are influenced by sanction severity, supporting H1a. There is a positive relationship between these two factors, indicating that when sanctions such as punishment, jail terms, or suspensions are applied, employees' attitudes are influenced to reduce information security threats in the supply chain. This finding is consistent with Safa et al. (2019), who showed that individuals' attitudes towards preventing information security misbehaviour in organizations are influenced by perceived sanction certainty and severity, and with Cheng et al., (2013), who confirmed that sanction severity significantly impacts employees' intentions to violate the Information System Security Policy (ISSP). Furthermore, if employees believe they will face severe penalties for committing crimes or abusing the system, they are less likely to engage in such behaviour. Therefore, sanction severity has a positive relationship with attitude ($\beta = 0.144$, $t = 2.589$, $p \leq 0.010$). One possible explanation for this result could be that employees weigh the high risks and low benefits associated with misconduct, which influences their decision to prevent information security threats. The impact of sanction severity on information security

threats in the supply chain is fully mediated by attitudes, as experimentally demonstrated, which aligns with the findings of (Merhi and Ahluwalia, 2019). This study provides empirical evidence and a theoretical explanation for the direct influence of sanction severity on information security threats in the supply chain, as suggested by D'Arcy and Herath (2011). These authors hypothesized that this would be the case, as sanction severity has been shown to influence attitudes towards various information security behaviours and ISP compliance (Bulgurcu et al., 2010; Workman et al., 2008). Surprisingly, in contrast to the findings of this study, the investigation by D'arcy et al. (2009) on workplace internet abuse found that attitudes did not influence the relationship between sanction severity and intentions to engage in information security behaviours related to workplace internet misuse.

6.3.2 Sanction severity and subjective norms

H1b: There is positive relationship between sanction severity and subjective norms in reducing information security threats in the SC.

According to the literature, individuals adjust their behaviour based on observing what actions are penalized and what actions are not. Regulatory mechanisms, such as deterrent policies, have a significant influence on the general behaviour of most individuals, leading to the formation of subjective norms (Merhi and Ahluwalia, 2019). Based on this understanding, it was hypothesized that there is a positive relationship between sanction severity and subjective norms in mitigating information security threats in the supply chain (INTSC). From an information security perspective, subjective norms play a role in determining individuals' behaviour (Safa and Von Solms, 2016; Herath and Rao,2009). Siponen et al. (2012) discussed that employee compliance with information security policies is influenced by the reactions received from peers, as well as the prevention and reduction of threats in the supply chain. They emphasized that if the penalties affect an individual's reputation among their peers, they are more likely to comply with organizational norms. In the context of this study, subjective norms were measured using five indicators that mainly reflected employees' intentions to mitigate threats in the supply chain due to the fear of a jail term penalty for engaging in undesirable behaviour. These indicators aimed to discourage individuals from engaging in non-compliant acts due to the influence of their supervisors, colleagues, and friends. The reliability and validity of this measure were confirmed through model evaluation, and SEM analysis provided evidence supporting H1b, which suggests a positive relationship between sanction severity and subjective norms in INTSC.

The analysis demonstrated that sanction severity has a positive impact on subjective norms ($\beta = 0.347$, $t = 3.687$, $p \leq 0.000$). The findings of this research revealed that supervisors, friends, and managers possess the power and authority to influence subordinates' well-being and job security. As a result, employees develop a sense of fear and discipline, leading them to act within the established parameters of the supply chain. This finding aligns with the research of Safa et al. (2019), which demonstrates that sanction severity and subjective norms influence individuals' efforts to prevent insider threats.

Similarly, Cheng et al. (2013) found that sanction severity and the expectations of immediate supervisors and co-workers have a significant influence on reducing violation intentions. Ifinedo (2014) conducted a more comprehensive study on the knowing-doing gap and found that subjective norms have the greatest impact on ethical behaviour. In a similar context, Humaidi and Balakrishnan (2017) discovered that sanction severity and subjective norms have a positive impact, and non-violators believe in the enforcement of penalties and are influenced by their social circles. Literature from various disciplines has consistently shown that norms directly and positively influence individuals' intentions towards certain behaviours. However, no study to date has specifically examined the impact of sanction severity and subjective norms on the supply chain. The data collected in this study supported the hypothesis, thus contributing to the existing literature on this topic.

6.3.3 Sanction severity and self-efficacy

H1c: There is a positive relationship between sanction severity and self-efficacy in reducing information security threats in the SC.

H1d: There is a positive relationship between sanction severity and information security threats in the SC

The literature review revealed that the skills required for committing information security threats are distinct from traditional crimes, and individuals engaging in such behaviour may perceive themselves as competent (Workman et al., 2008). Based on this understanding, it was hypothesized that there is a positive relationship between sanction severity and self-efficacy in information security threats in the supply chain (H1c). From an information security perspective, it was argued that employees with high levels of self-efficacy would perceive a lower likelihood of being sanctioned. In this study, self-efficacy was measured using seven items that primarily assessed employees' skills and competency in mitigating and securing information in the supply chain, considering the potential sanctions. The reliability and validity of this measure were confirmed through model evaluation. However, the SEM analysis provided evidence contradicting H1c, as an insignificant relationship was found between sanction severity and self-efficacy ($\beta = 0.034$, $t = 0.483$, $p > 0.05$). Therefore, hypothesis H1c was rejected. This finding contradicts previous research in the information security literature. For example, Cheng et al. (2013) found empirical support for the positive relationship between sanction severity and self-efficacy in digital piracy behaviour. Cuganesan et al., (2018) also discovered that sanctions and self-efficacy have a positive influence on reducing employees' intentions to commit crimes. Similar results were reported in the study by Kumar (2019), suggesting that sanction severity and self-efficacy have a significant impact on individuals' decisions regarding preventive measures to discourage deviant behaviour.

Hence, the findings of this research contradict the results of existing literature on information security in the supply chain. The culture of the people in the Nigeria could be a plausible explanation for this

finding. Moral values hold significance in their cultural context, and personal matters do not interfere with their professional responsibilities in the workplace. Nevertheless, data analysis indicated that sanction severity remains an important factor in reducing information security threats in the supply chain, particularly when considering constructs directly associated with information security threats in the supply chain. During the model modification stage in Chapter 5, an additional link was established between sanction severity and information security threats in the supply chain. The relationship was found to be significant, indicating a strong positive association between sanction severity and information security threats ($\beta = 0.131$, $t = 3.687$, $p \leq 0.000$). Thus, sanction severity does impact information security threats in the supply chain, suggesting that it serves as a deterrent for employees engaging in information security misconduct in the supply chain.

6.4 Social Bond Theory (SBT)

Social Bond Theory (SBT) was utilised as the theoretical foundation for this study. SBT has gained attention from experts across various disciplines as one of the most intriguing social theories. The literature review in Chapters 2 and 3 demonstrates that SBT has been effectively employed in numerous studies to examine its influence on the risk of threats within organizations. Hirschi (1969) proposed SBT, which focuses on individuals' relationships with their peers and peer groups. The theory emphasizes four fundamental factors: attachment to the organization, commitment to organizational objectives, involvement in specific tasks, and personal norms (Safa et al., 2018). Among these factors, commitment was chosen due to its attribute of dedicating time and effort to achieving career success rather than engaging in behaviours that could jeopardize one's professional trajectory. Therefore, a committed employee is more likely to support the reduction of information security threats in the supply chain. SBT highlights the activities individuals engage in while at work, suggesting that stronger social bonds are associated with decreased criminal behaviour. When social ties are broken or weakened, deviant behaviour becomes more prominent. These findings motivated the researcher to incorporate SBT into this study. The subsequent sections discuss the results of this study concerning the factors of commitment, attitude, self-efficacy, subjective norms, and information security threats in the supply chain.

6.4.1 Commitment and attitudes

H2a: There is a positive relationship exists between commitment and attitudes toward information security threats in the SC.

Commitment can be demonstrated through efforts, dedication, and support for protecting an organization's data. Committed individuals value personal achievement and reputation (Cheng et al., 2013). The literature review indicates that individuals have a responsibility to invest time and effort into safeguarding an organization's information assets (Cheng et al., 2013). In the context of this study, commitment is viewed as a factor that reduces information security threats in the supply chain. Previous

studies have consistently shown the positive impact of commitment and attitude on various types of information security (Safa et al., 2018; Cuganesan et al., 2018; Cheng et al., 2013). Consequently, it was hypothesized that commitment has a positive relationship with attitude towards information security threats in the supply chain (H2b). To measure commitment, five items directly adapted from Ifinedo (2012) were used. These items assess the extent to which employees invest their time and energy in mitigating and securing the company's information assets. The reliability of the measurement model for the construct was validated in Chapter 5, demonstrating its validity and reliability, thus retaining all five items in the model.

Furthermore, the structural equation modeling (SEM) analysis yielded supporting evidence for H2a, revealing a positive correlation between commitment and attitude ($\beta = 0.137$, $t = 2.647$, $p \leq 0.008$), thus confirming the hypothesis. These findings indicate that individuals who dedicate their time and effort to the organization are more likely to refrain from engaging in misconduct or inappropriate behavior. They are also more inclined to allocate additional time and effort toward mitigating information security threats in the supply chain. Previous studies have also reported similar findings regarding the relationship between commitment and attitude (Safa et al., 2018; Ifinedo, 2014; Cheng et al., 2013). Cheng (2013) assessed commitment based on individuals' desire, time, and effort invested in achieving success within the organization, and found a positive impact on attitude. Ifinedo (2014) similarly discovered that employees who strongly believe in their organization's values and goals, including those related to issues of information security and privacy, develop and maintain positive attitudes regarding the importance of such rules and guidelines. Furthermore, Safa et al. (2016), drawing from the social bond theory, examined factors influencing employee behavior in information security to mitigate risks, and their empirical evidence supported a positive association between commitment and attitude, aligning with the findings of Safa et al. (2016).

6.4.2 Commitment and subjective norms

H2b: There is a positive relationship between commitment and subjective norms in reducing information security threats in the SC.

As in Chapter 3, Section 3.5.1, Feng et al., (2015) found that commitment to information security offers operational assurance and lower risk events because it entails dedication and evident attachment to goals and services. According to Ifinedo (2014), those employees who have a comparable level of commitment as their colleagues are less likely to participate in counterproductive behaviour if their colleagues and peers do not engage in such behaviour. According to the current literature (Safa et al.,2016; Cheng et al., 2013), commitment is an important factor in information security in the supply chain setting because it needs a stable relationship, a willingness for making sacrifice and confidence stability of the relationship. As Chapter 3, section 3.5.1 mentioned, the fact that commitment and subjective norms have a positive relationship in reducing information security threats in the supply

chain has not been widely discovered yet, it was essential to find out through empirical studies how commitment and subjective norms are related to each other in the supply chain. Therefore, hypothesis H3b was created on how commitment and subjective norms are associated in reducing threats in the supply chain.

Chapter 5, section (5.15) on path coefficient analysis ($\beta = 0.012$, $t=2.242$, $P > 0.05$) found that H3b commitment and subjective norm are rejected because they are not related. Therefore, one might suggest that there is a conflicting result between the findings of this study and the results from prior studies in the field of information security in the supply chain. Feng et al., (2019) found that commitment deals with the willingness to implement and monitor decisions in the supply chain. Further, Safa et al. (2016) discovered that subjective norms positively affect the conscious care behaviour of employees' intention. A similar result was also reported in a study by Ifinedo (2014). Even though this study evidence failed to support H2b, a commitment was seen as a crucial factor in mitigating information security threats in the supply chain. Specifically, further analysis revealed that the construct had a positive relationship with attitude ($\beta=0.137$, $t = 2.647$, $p \leq 0.008$) and self-efficacy ($\beta = 0.168$, $t= 2.381$, $p \leq 0.001$).

6.4.3 Commitment and self-efficacy

H3c: There is a positive relationship between commitments and self-efficacy in information security threats in the SC.

H3d: There is a positive relationship between commitments and information security threats in the SC.

As discussed in Chapter 3, Section 3.5.1, Skotnes (2015) found that commitment to information security provides operational assurance and reduces the occurrence of risky events due to the dedication and attachment to goals and services. According to Ifinedo (2014), employees who exhibit a similar level of commitment to their colleagues are less likely to engage in counterproductive behaviour if their peers do not engage in such behaviour. The current literature (Feng, 2019; Wang, Li and Rao 2017; Hu et al.,2012) also emphasizes the significance of commitment in information security within the supply chain, highlighting the importance of stable relationships, willingness to make sacrifices, and confidence in relationship stability. Although the positive relationship between commitment and subjective norms in reducing information security threats in the supply chain has not been extensively explored, it was deemed important to investigate the relationship through empirical studies. Therefore, hypothesis H3b was formulated to examine the association between commitment and subjective norms in mitigating threats in the supply chain.

However, the path coefficient analysis in Chapter 5, section (5.15) revealed that H3b, which posited a relationship between commitment and subjective norms, was rejected as there was no significant relationship ($\beta = 0.012$, $t = 2.242$, $p > 0.05$). This finding presents a conflicting result compared to prior

studies in the field of information security in the supply chain. For instance, Villena et al., (2018) found that commitment involves the willingness to implement and monitor decisions in the supply chain. Additionally, Safa et al. (2016) discovered that subjective norms positively influence employees' intention to engage in conscientious care behaviour. Similar results were reported by Ifinedo (2014). Although this study's evidence did not support H3b, commitment was still considered a crucial factor in mitigating information security threats in the supply chain. Further analysis revealed that commitment had a positive relationship with attitude ($\beta = 0.137$, $t = 2.647$, $p \leq 0.008$) and self-efficacy ($\beta = 0.168$, $t = 2.381$, $p \leq 0.001$)

6.5 Theory of Planned Behaviour (TPB)

The TPB, which is an extension of the theory of reasoned action proposed by Ajzen and Fishbein (1985), provides an explanation for an individual's intention to engage in a specific behaviour. Attitude refers to an individual's evaluation of something, indicating their level of liking or disliking towards it. This evaluation can range from strong positive or negative feelings to neutral or ambivalent sentiments (Safa et al., 2018). According to the TPB, an individual's attitude towards a behaviour, their subjective norms, and their perception of behavioural control collectively contribute to predicting their intention to engage in that behaviour. These predictors account for a significant portion of the variability in actual behaviour (Bulgurcu et al., 2010). Scholars have successfully applied this theory to investigate people's intentions and behaviours in various contexts.

In line with the TPB, this study also utilized the theory to examine employee behaviour and their preferences towards certain aspects. Three factors, namely attitude, subjective norms, and self-efficacy, were hypothesized to have a positive influence on information security in the supply chain (H3a, H3b, and H3c). The subsequent sections will discuss the results and implications of these hypotheses.

6.5.1 Attitude and information security threats in the supply chain

H3a: There is a positive relationship between attitudes and information security threats in the SC.

Based on previous research in the context of information security in the supply chain, attitude was defined by various distinct characteristics, including evaluative reactions, feelings, and appraisals of objects, people, activities, events, and ideas. These evaluations can range from highly positive to strongly negative. The analysis of the measurement model confirmed the reliability and validity of all the items pertaining to the attitude construct. However, when testing the hypotheses, it was discovered that attitude did not have a direct relationship with information security threats in the supply chain ($\beta = 0.194$, $t = 0.154$, $p > 0.05$), leading to the rejection of H2a. This finding contradicts the outcomes of several prior studies that observed a positive association between attitudes and information security (Ifinedo, 2012; Kathryn et al., 2014; Safa et al., 2019; Passfaro, 2020).

Passfaro (2020) highlighted the multi-layered nature of the attitude construct and its distinct role in knowledge-seeking behaviour related to information security. Similarly, Safa et al. (2019) found that attitudes positively influence employees' intentions to engage in information security misconduct. Ifinedo (2012) also reported a similar result. Although this study failed to provide evidence supporting H2a, attitude is still considered a crucial element in the context of information security threats in the supply chain. In particular, further analysis revealed that the attitude construct had an indirect positive relationship with top management support ($\beta = 0.193$, $t = 3.349$, $p \leq 0.001$), commitment ($\beta = 0.137$, $t = 2.647$, $p \leq 0.008$), and monitoring/evaluation ($\beta = 0.172$, $t = 2.938$, $p \leq 0.003$). Table 5.4 presents the interaction between attitude and the five independent variables. The results in the table demonstrate that all five factors (top management support, monitoring/evaluation, commitment, reward, and sanction severity) influence attitude, with top management support exerting the most significant influence. This implies that while attitude alone may not directly affect information security threats in the supply chain, all five constructs can be utilized to shape employee attitudes towards these threats.

6.5.2 Subjective Norms and information security threats in the supply chain

H3b: There is positive relationship between subjective norms and information security threats in the SC.

The analysis conducted in this study revealed a positive relationship between subjective norms and information security threats in the supply chain ($\beta = -0.114$, $t = 1.845$, $p \leq 0.036$). This indicates that subjective norms play a role in influencing the reduction of threats in the supply chain related to information security. One possible explanation for this finding is the impact of information security policies or instructions from supervisors and colleagues, which employees are obligated to follow in the supply chain. These policies and instructions create a mandatory condition for staff to adhere to proper practices in order to protect the organization's information assets. This finding is consistent with the results of Cheng et al., (2013) and is supported by the findings of another researcher, Tondel et al. (2014).

Additional support for the findings of this study can be found in the literature. Vance et al., (2012) discovered that subjective norms significantly influenced the perceived usefulness in the supply chain. Similarly, Kumar (2019) found that subjective norms played an important role in influencing young adults' intentions in the e-waste recycling supply chain. Ifinedo (2012) further confirmed the findings of this hypothesis in their research. They demonstrated that subjective norms, representing social influences, were the most powerful and significant determinant of an employee's intention to adhere to information security policy recommendations related to USB usage. Their study suggested that emphasizing the social desirability of complying with information security policies, rather than focusing solely on the risks of non-compliance, could lead to improved intentions and behaviours related to security.

6.5.3 Self-efficacy and information security threats in the SC

H3c: There is positive relationship between self-efficacy and information security threat in the SC.

This study proposed self-efficacy as a factor that could influence employees' perceptions. However, the findings indicate that self-efficacy does not have a significant impact on the reduction of threats in the supply chain ($\beta = 0.007$, $t = 1.193$, $p > 0.05$). This finding contradicts many studies in the literature that suggest self-efficacy can improve behaviour (Zinn, 2013; Padayachee, 2012). For instance, Safa et al. (2015) found that self-efficacy reduces the risk of information threats, particularly in the context of human behaviour as a vulnerability. Zinn (2013) also discovered that self-efficacy can enhance companies' environmental behaviour. The result of this research is also contrary to the findings of Padayachee (2012), who reported that information security self-efficacy influences employees' efforts to protect their information and their intentions to reinforce information security practices.

The results presented in Table 5.4 indicate that monitoring/evaluation, sanction severity, and reward have an impact on employee attitudes, with monitoring/evaluation and sanction severity exerting a particularly significant influence. This suggests that employee competence, skills, and expertise alone are not sufficient to secure information assets. They need to be complemented by effective monitoring and evaluation mechanisms, as well as appropriate sanction severity, to shape employee attitudes towards information security. These five significant constructs, as depicted in Figure 3.1, collectively contribute to ensuring the protection of information assets.

6.6 Top management support and attitude

H1a: There is positive relationship between top management support and attitude in information security threats in the SC.

The review of existing literature indicates that the support of top management is crucial for effective supply chain management (SCM) and information security. When top management shows support for information security in the supply chain, it communicates its importance to the rest of the organization. This support can also empower employees to change their approach to information security. Several studies (Snyman 2021; Flores and Ekstedt, 2016; Skotnes and Engen 2015) have highlighted the significance of top management support in influencing information security attitudes and behaviours. Similarly, the beliefs and attitudes of individuals regarding information security are influenced by the norms prevalent in their environment, including the expectations and behaviours of their colleagues and top managers (Da Veiga and Martins, 2015; Warkentin et al., 2011; Guo et al., 2011). Based on these observations, it was hypothesized that there is a positive relationship between top management support and attitudes towards information security threats in the supply chain (H1a).

Furthermore, from the perspective of information security in the supply chain, the attitude of top management has an impact on employees' behaviour and attitudes (Cuganesan et al., 2018). In this particular study, the construct of top management support was measured using six indicators that mainly reflected the threats to information security in the supply chain. The evaluation of the model demonstrated that this measure was reliable and valid. Additionally, the analysis using structural equation modelling (SEM) provided evidence supporting the positive relationship between top management support and attitudes ($\beta = 0.193$, $t = 3.349$, $p \leq 0.001$), as hypothesized (H1a). These results suggest that when top management demonstrates support, it contributes to reducing information security threats in the supply chain. These findings align with previous studies that have also reported a positive association between top management support and attitudes towards information security (Cuganesan et al., 2018; Flores and Ekstedt, 2016; Hu et al., 2012). For instance, Cuganesan et al. (2018) measured top management support by assessing their level of interest, words, and actions towards the information assets of their organization and found a positive effect on attitudes towards information security. Shee Flores and Ekstedt, (2016) similarly concluded that top management support has a positive relationship with attitudes in the supply chain.

The results of this hypothesis emphasize the significance of top management support and attitude in mitigating information security threats in the supply chain. The statistical analysis conducted in this research clearly demonstrates that when top management demonstrates a high level of interest in securing the information within the supply chain of an organization, it significantly reduces information security threats. When the top management team is aware of the potential risks and vulnerabilities associated with information security threats in the supply chain, their attitudes serve as a motivating factor for employees to exert necessary efforts to enhance information security.

In this study, the role of top management support emerged as a crucial element in promoting employee information security behavior through their exemplary attitude. However, it's worth noting that Hu et al. (2012) did not find any evidence of a significant correlation between senior management participation in information security initiatives and employee attitudes. In the current study, 33.5% of the respondents held managerial positions, indicating that these individuals likely had the authority to make strategic decisions. This suggests that top managers have a significant impact on protecting information assets and ensuring the security of shared information.

6.6.1 Top management support and subjective norms

H4b: There is a positive relationship between top management support and subjective norms in information security threats in the SC.

In a recent publication, William et al. (2019) proposed that personal beliefs can influence individual behaviour, especially when there is a potential for gaining approval from others. They argued that the influence of influential individuals can play a persuasive role in determining whether individuals engage in specific behaviours. The actions and behaviours of top managers within an organization can facilitate the implementation of organizational initiatives. However, the findings of the study indicate that there is no significant relationship between top management support and subjective norms (β=0.049, t=0.880, $p > 0.05$). This means that there is an insignificant association between top management and subjective norms. The positive example set by top managers does not effectively encourage employees to behave in a similar manner, and consequently, it cannot be relied upon to mitigate information security threats in the supply chain.

These results are consistent with the findings of Hu et al. (2012), who also observed that top management support and subjective norms do not influence employee information security behaviour. Similarly, a recent study by Flores and Ekstedt (2016) failed to identify a significant correlation between these two constructs. These findings suggest that the support provided by top management does not have a significant impact on employee information security behaviour. Given the imminent nature of information security threats within the supply chain, it appears that the interaction between stakeholders, including both senior and junior staff, is an ineffective tool for mitigating these threats. Therefore, top management has the ability to shape the values, norms, and shared beliefs within their organization regarding information security threats in the supply chain.

6.6.2 Top management support and Self-efficacy

H4c: There is a positive relationship between top management support and self-efficacy information security threats in the SC.

H4d: There is positive relationship between top management support information security threats in the SC.

Managers and their organizations frequently face dynamic and changing circumstances. The constantly turbulent environment not only challenges managers' knowledge and abilities but also tests their general beliefs in their own effectiveness, which provides the psychological capacity to cope with various demands. Top management support, as discussed in Chapter 3, is instrumental in fostering employees' competency and influencing their efforts to reduce threats in the supply chain. The analysis of the measurement model confirmed the reliability and validity of the construct's items. However, during hypothesis testing, it was discovered that top management support has a direct relationship with self-efficacy ($\beta = 0.237$, $t = 4.114$, $p \leq 0.004$), leading to the acceptance of H1c. This finding demonstrates that top management support also positively affects employees' self-efficacy, which in turn shapes their behavior. This outcome aligns with several previous studies that have reported a positive association between these two constructs (e.g., Cuganesan et al., 2018; Hu et al., 2012). Cuganesan et al. (2018)

identified this as a key factor influencing behavior perception in the information security (InfoSec) environment. Similarly, Hu et al. (2012) found that top management support and self-efficacy have a relationship in information security initiatives and employee compliance behavior. Top management emerges as a crucial element in ensuring information security within the supply chain. Further analysis revealed that the construct also has a direct relationship with information security threats in the supply chain ($\beta = 0.244$, $t = 4.247$, $p \leq 0.020$). This suggests that the more support top management provides to employees within an organization, the lower the vulnerability to information security threats in the supply chain will be.

6.7 Reward and Attitudes

H5a: There is positive relationship between rewards and attitudes in information security threat in the SC.

As highlighted in Chapter 2, Section 2, there are various factors that can be implemented to mitigate threats in information security within the supply chain. Scholars such as (Canova and Manganelli et al.2020; Cuganesan et al.,2018; Siponen et al.,2014; Goo et al.,2014; Bulgurcu et al.,2010) emphasize the importance of rewards as a key factor in influencing employee attitudes and compliance with information security policies. Siponen et al., (2014) assert that rewards can effectively motivate performance and interest. Canova and Manganelli et al., (2020) specifically defines rewards as what employees receive at work, encompassing monetary remuneration, social approval, esteem, job security, and career opportunities, within the framework of a social exchange process. While rewards can provide strong incentives that elicit desired responses, it is essential to note that when there are no substantial changes in outcomes, employees may not comply with the required measures. Therefore, as mentioned in Chapter 2, rewards play a crucial role in mitigating information security threats in the supply chain. Safa et al. (2016) discusses how rewards serve as extrinsic motivation, discouraging individuals from engaging in harmful activities or committing crimes. Rewards within the context of information security in the supply chain are an important principle.

According to Caputo (2020), research indicates that pay-for-performance incentives vary in their level of instrumentality. This suggests that workers are aware of the long-term consequences of attempting to work in a particular manner, particularly when there is a significant situational influence. Employees require motivations that encourage them to contribute to reducing information security threats within the supply chain. Rewards and attitudes play vital roles in creating a conducive environment for employees to effectively address information security threats within the supply chain.

In Chapter 3, Section 3.10.2, the question regarding the relationship between rewards and attitudes in relation to information security threats within the supply chain was explored further. This inquiry aimed to uncover how these factors are interconnected and influence one another within the context of information security threats in the supply chain.

The findings of this study ($\beta = 0.196$, $t = 2.268$, $p \leq 0.024$) establish a significant positive relationship between rewards and attitudes in mitigating information security threats within the supply chain. The results highlight that increased employee motivation, driven by rewards, tends to lead to a reduction in threats. Notably, the level of personal motivation derived from rewards demonstrates greater significance in shaping employee attitudes toward mitigating information security threats in the supply chain (Chapter 5). This could be attributed to the fact that rewards, coupled with employee motivations, encourage active engagement in the project, even if overall satisfaction with the organization is relatively lower. However, it is worth noting that the variable of self-efficacy did not show a significant relationship with rewards, as indicated in Chapter 5.

The data analysis for this hypothesis underscores the crucial role of rewards and attitudes in addressing information security threats within the supply chain. These findings align with existing academic literature and offer more detailed insights into the significance of rewards in relation to other factors, such as subjective norms and information security threats within the supply chain (Chapter 5).

The findings of this study ($\beta = 0.196$, $t = 2.268$, $p \leq 0.024$) establish a significant positive relationship between rewards and attitudes in mitigating information security threats within the supply chain. The results highlight that increased employee motivation, driven by rewards, tends to lead to a reduction in threats. Notably, the level of personal motivation derived from rewards demonstrates greater significance in shaping employee attitudes toward mitigating information security threats in the supply chain (Chapter 5). This could be attributed to the fact that rewards, coupled with employee motivations, encourage active engagement in the project, even if overall satisfaction with the organization is relatively lower. However, it is worth noting that the variable of self-efficacy did not show a significant relationship with rewards, as indicated in Chapter 5.

The data analysis for this hypothesis underscores the crucial role of rewards and attitudes in addressing information security threats within the supply chain. These findings align with existing academic literature and offer more detailed insights into the significance of rewards in relation to other factors, such as subjective norms and information security threats within the supply chain (Chapter 5).

6.7.1 Reward and subjective norms

H5b: There is positive relationship between reward and subjective norms in information security threat in the SC.

Chapter 2, Section 2.10.3 highlighted the findings of Raza et al. (2018), emphasizing the importance of basing the sharing of rewards and promotions on individual efforts rather than political influence. Raza et al. (2018) argued that motivated employees are more likely to go the extra mile to ensure the security

of their information alongside their colleagues. Current academic literature (Cuganesan, 2018; Ashenden,2018; Boss et al.,2015) consistently identifies rewards and subjective norms as crucial factors in information security within the supply chain. These factors contribute to the formation of intentions to act responsibly and enable cooperation and coordination to safeguard firms' information assets. As mentioned in Chapter 3, Section 3, the relationship between reward and subjective norms in the context of information security within the supply chain has not been extensively explored. Therefore, it was imperative to empirically investigate how these factors interrelate regarding information security threats within the supply chain. Hence, H4b was formulated to describe the influence of the interaction between reward and subjective norms of employees on information security threats in the supply chain.

In Chapter 5, Section 5.15, the analysis revealed a positive relationship between reward and subjective norms ($\beta = -0.229$, $t = 2.774$, $p \leq 0.0012$). The data analysis of this research indicates that rewarding employees within an organization is a significant factor in reducing information security threats. Rewards for information security behaviour serve as motivation for employees and communicate to others that such behaviour is endorsed by the organization. Consequently, this positively influences employees' information security behaviour, effectively mitigating information security threats in the supply chain (ISTSC). These findings are particularly significant due to the limited research available on the relationship between reward and subjective norms. The research contributes to reducing information security threats within the supply chain based on these findings. Additionally, the findings underscore the importance of organizational rewards in enhancing employee motivation to deviate from delinquent behaviour and contribute to information security in the supply chain, thereby making a valuable contribution to the body of knowledge.

6.7.2 Reward and Self-efficacy

H5c: There is a positive relationship between reward and self-efficacy in information security threats in the SC.

H5d: There is a positive relationship between reward and information security threats in the SC.

As stated in hypothesis H4c, self-efficacy is also associated with rewards. However, the existing literature presents conflicting findings regarding the relationship between reward and self-efficacy. Some studies suggest that the effect of self-efficacy on performance varies depending on the underlying reward structures in different studies. Bandura (1991) suggests that behaviours leading to dissatisfaction are likely to have unrewarding positive valence and are likely to decrease, while behaviours leading to satisfaction have positive valence and are rewarding. Booth et al., (2008) explain that self-efficacy has a positive influence under high rewards and a negative influence under low rewards.

The data analysis conducted for this hypothesis indicates that reward and self-efficacy do not have a significant relationship with each other ($\beta = 0.027$, $t = 0.227$, $p > 0.05$). This finding aligns with previous studies that have identified rewards and self-efficacy as separate constructs in workplace settings (Cuganesan et al., 2018).

While rewards do play a role in mitigating threats in the supply chain, they are not the most influential factor in reducing information security threats. The analysis in Chapter 5, Section 5.15 reveals a positive relationship between reward and information security threats in the supply chain ($\beta = 0.946$, $t = 0.533$, $p \leq 0.000$). This suggests that motivating employees, providing benefits, and giving awards can help reduce threats in the supply chain. This finding is consistent with the study conducted by Hu et al. (2012), who found a positive relationship between reward and perceived compliance with information security policies among staff in universities. Their findings also align with the current study, as they also concluded that reward does not directly impact self-efficacy.

Additional support for the results of this study can be found in the research conducted by Bulgurcu et al. (2010), who identified reward as a crucial influencing factor for compliance behaviour in information security within organizations. Similarly, Tepe and Tepe (2015) found that reward played an important role in encouraging security compliance within the information security supply chain. Their study proposed a positive influence of self-efficacy (expectancy) under high rewards (challenging tasks) and a negative influence of self-efficacy under low rewards (no challenging tasks). They argue that behaviours leading to dissatisfaction are likely to have unrewarding positive valence and are likely to decrease, while behaviours leading to satisfaction have positive valence and are rewarding.

6.8 Monitoring/Evaluation and attitude

H6a: There is a positive relationship between monitoring/evaluation and attitudes in information security threats in the SC.

Several studies (Cuganesan et al., 2018; Akhyari et al., 2018;) discussed in Chapter 2 emphasize the crucial significance of monitoring and evaluation (M&E) in organizations for ensuring compliance and preventing negligence. M&E acts to assess and control deviant activities, relying on employees' competence and abilities to effectively mitigate information security threats. Noteworthy, (Da Veiga and Martins 2015; Cuganesan et al.,2018; Cox 2012) highlight M&E as a key factor in fostering successful information security self-efficacy. However, implementing M&E incurs additional costs related to inspecting material, information, and financial flows in supply chains, as mentioned in Chapter 2, Section 2.10.5.

To examine the influence of M&E on self-efficacy, this aspect was integrated into the hypothesis in Chapter 3. The data analysis conducted in this research confirms the vital role of M&E in enhancing self-efficacy in reducing threats in the supply chain. Almost all variables demonstrate significant relationships with M&E, as indicated by the path coefficients presented in Chapter 5, Table 5.15.

The measurement model evaluation in Chapter 5 establishes the reliability and validity of all indicators. Supporting evidence for H6c was found during hypothesis testing, revealing a positive relationship between monitoring and self-efficacy ($\beta = 0.236$, $t = 4.052$, $p \leq 0.000$). These findings suggest that employees who believe in their ability to handle security incidents and have high expectations of reducing information security threats are more likely to engage in such behaviour. Therefore, a high level of monitoring and evaluation in the context of information security threats in the supply chain leads to an improvement in employees' self-efficacy.

Furthermore, the direct relationship between monitoring/evaluation and information security threats in the supply chain was significant ($\beta = 0.226$, $t = 3.702$, $p \leq 0.020$), providing support for H6d. The findings indicate that employees' awareness of monitoring/evaluation practices enhances the mitigation of information security threats in the supply chain. In this study, it was observed that when employees are being monitored, they are less inclined to explore and exploit technology, reducing the likelihood of causing disruptive events in the supply chain. The existing literature offers limited insights into this finding, and this study contributes to the few existing studies (e.g., Feng et al.,2019; Chen and Zahedi 2016; D'Arcy et al., 2009).

Consequently, the results of the data analysis in this hypothesis enrich the current academic literature by providing a more comprehensive understanding of the importance of monitoring/evaluation in relation to information security threats in the supply chain. It also highlights the different levels of relationships between monitoring/evaluation and other variables in the data analysis. Thus, this study

adds depth to the current academic literature and sheds light on the significance of monitoring/evaluation in contributing to the understanding of information security threats in the supply chain.

As discussed in Chapter 3, Monitoring/Evaluation (M&E) is considered an essential component of project design, implementation, and completion, as highlighted by Chaplowe (2008). Haque and Khan (2014) emphasize that M&E involves the ongoing assessment of program, policy, and project performance, including cost, deliverables, and timelines, to ensure that implementation aligns with the planned objectives. In the context of information security threats in the supply chain, monitoring and evaluation of employee performance are likely to influence attitudes, subjective norms, and self-efficacy. This study recognizes M&E as a signal of security importance, which positively influences attitudes and contributes to the reduction of information security threats in the supply chain.

Extensive literature review reveals the significance of monitoring and evaluation specifically in the realm of information security in the supply chain, supported by studies such as (Chen et al., 2015; Boss et al.,2015; Crossler et al.,2013). Empirical studies have consistently demonstrated the positive influence of M&E on attitudes in various information security contexts. To measure these constructs, seven items were adapted from previous studies (Cuganesan et al., 2018; Speire et al., 2011). During the measurement model test, it was found that all items were reliable, except for one item, M/E 6, which had a low factor loading (0.031) and was subsequently removed from the model. This issue with the indicator's reliability has also been observed in previous studies. The literature strongly supports the connection between monitoring/evaluation and attitudes in the context of information security in the supply chain, as indicated by (Cuganesan et al. 2018; Da Veiga and Martins 2015; Vance et al.,2012). Consequently, the hypothesis was formulated that this construct is positively associated with attitudes toward reducing information security threats in the supply chain (H6a).

The analysis results demonstrate a significant and positive relationship between monitoring and evaluation (M&E) and attitude ($\beta = 0.172$, $t = 2.938$, $p \leq 0.003$), providing support for hypothesis H6a. This finding suggests that when employees are subject to monitoring and evaluation, their behaviour is more likely to change, leading to a reduction in information security threats. It highlights the importance of organizations implementing M&E practices to effectively mitigate information security threats in their supply chain. This finding aligns with the recommendations put forth by Parush et al., (2017). Emphasising the significance of M&E in raising awareness and implementing countermeasures.

6.8.1 Monitoring/Evaluation and subjective norms

H6b: There is a positive relationship between monitoring/evaluation and subjective norms in information security threats in the SC.

Chapter 2 thoroughly examined various studies (Rajivan et al., 2019; Da Veiga and Martins, 2015; Chen et al., 2015; Lim et al.2009; Merchant and Van Der Stede, 2007) to investigate the role of monitoring and evaluation (M&E) in ensuring information security in the supply chain. These studies collectively indicate that M&E plays a crucial role in ensuring compliance with established frameworks and information security standards, providing necessary checks and balances. In the context of this research, employees' perception of being monitored was found to be positively associated with perceiving the actions taken by authorities or colleagues as beneficial ($\beta = 0.455$, $t = 7.259$, $p \leq 0.000$). This supports hypothesis H6b, indicating a direct influence of monitoring and evaluation on subjective norms. Thus, emphasizing the significance of reducing information security threats in the supply chain through M&E leads employees to adopt the behaviours and perspectives of others.

These findings align with the research conducted by Merchant and Van Der Stede (2007), who demonstrated that control mechanisms like monitoring and evaluation signal positive outcomes to be achieved and negative outcomes to be avoided by employees. Dang-Pham (2016) also supports this view, suggesting that monitoring and evaluating employees are likely to influence subjective norms in the workplace. Chen et al. (2014) further supports these findings by highlighting the positive impact of security monitoring on employees' perceptions and assumptions regarding security. D'Arcy, Herath and Shoss (2014) found a significant influence of M&E on performance, particularly in the public sector. Ahmad et al. (2018) indicates that organizations promoting security behaviour extend the scope of monitoring beyond security policy to demonstrate the benefits derived from such measures.

6.8.2 Monitoring/Evaluation and Self-efficacy

H6c: There is positive relationship between monitoring/evaluation and self-efficacy in reducing information security threats in the SC.

H6d: There is positive relationship between monitoring/evaluation in information security threats in the SC.

As discussed in Chapter 2, several studies emphasize the critical importance of monitoring and evaluation (M&E) in organizations for ensuring compliance and preventing negligence (Cuganesan et al., 2018; Flores et al.2014). M&E serves as a mechanism to assess and control deviant activities, relying on employees' competence and abilities to effectively reduce information security threats. Notably, (Kalu and Quinn 2020; Cuganesan et al.,2018; De Meulemeester, 2013) highlight M&E as a key factor in fostering successful information security self-efficacy. Implementing M&E incurs additional costs associated with inspecting material, information, and financial flows within supply chains, as discussed in Chapter 2, Section 2.10.5. Consequently, this research incorporates the influence of M&E on self-efficacy into the hypothesis in Chapter 3.

The data analysis conducted in this research confirms the vital role of M&E in enhancing self-efficacy related to the reduction of threats in the supply chain. Nearly all variables demonstrate significant relationships with M&E, as supported by the path coefficients presented in Chapter 5, table 5.15. The measurement model evaluation in Chapter 5 validates the reliability and validity of all indicators. Hypothesis H6c is supported, revealing a positive relationship between monitoring and self-efficacy ($\beta = 0.236$, $t = 4.052$, $p \leq 0.000$). The findings suggest that employees who believe in their capability to handle security incidents and have high expectations for reducing information security threats are more likely to engage in corresponding behaviour. Thus, a high level of monitoring/evaluation in information security threats within the supply chain leads to an improvement in employees' self-efficacy.

Furthermore, the direct relationship between monitoring/evaluation and information security threats in the supply chain is significant ($\beta = 0.226$, $t = 3.702$, $p \leq 0.020$), supporting hypothesis H6d. This indicates that employees' awareness of monitoring/evaluation practices enhances the mitigation of information security threats in the supply chain. In this study context, the results show that when employees are being monitored, they are less likely to engage in exploratory and exploitative behaviour with technology, reducing the likelihood of causing disruptive events in the supply chain. The existing literature provides limited insight into this finding, and this study adds to the existing research conducted by (Kalu and Quinn,2020; and D'Arcy et al. 2009).

In summary, the data analysis results for this hypothesis enrich the current academic literature and provide a more comprehensive overview of the importance of monitoring/evaluation in contributing to information security threats in the supply chain. It also reveals the varying levels of relationships between monitoring/evaluation and other variables in the data analysis**.**

6.9 Summary

This chapter has discussed the research findings in relation to the research questions and provided support for the findings from the literature. As identified during the literature review (Chapter 2), the thesis emphasised the factors: of attitude, subjective norms and self-efficacy derived from TPB from the literature towards mitigating information security threats in the supply chain. The extent of the impact of the drivers and associated factors was established by analysis of the predictive relevance of the indirect variables, explanations power of the direct variables and the significance of the identified relationships. The study confirmed that top management had a positive impact on these three drivers and information security threats in the supply chain. Contrary to expectation, attitude and self-efficacy were found to have no direct influence on information security threats in the supply chain except for subjective norms. Still, they are considered important for information security threats in the SC as the constructs had an indirect relationship with information security threats in the SC. Consistent with prior studies, one SBT factor (commitment) was found to have relationship with attitude and self-efficacy but has no relationship with subjective norms and information security threats in the supply chain.

Similarly, reward and sanction severity were also found to have direct relationship with information security threats in the SC and indirect relationship with attitude, subjective norms and no significant relationship with self-efficacy. Nonetheless, it was concluded that the constructs are still an important element in information security threats in the SC. The data analysis revealed that monitoring/evaluation had a positive relationship with all the four factors (information security threats in the supply chain, attitude, subjective norms, self-efficacy).

Table 6.1: Table of mediating factors in relation to independent factors

Interaction between Attitude and Independent Variables		
Independent Variable	**Dependent Variable**	**Supported?**
Top management support	Attitude	Supported
Commitment	Attitude	Supported
Sanction Severity	Attitude	Supported
Reward	Attitude	Supported
Monitoring/Evaluation	Attitude	Supported

Table 6.2: Interaction between subjective norms and independent variables

Interaction between Subjective norms and Independent Variables		
Independent Variable	**Dependent Variable**	**Supported?**
Top management support	Subjective norms	Not Supported
Commitment	Subjective norms	Not supported
Sanction Severity	Subjective norms	Supported
Reward	Subjective norms	Supported
Monitoring/Evaluation	Subjective norms	Supported

Table 6.3: Interaction between Self-efficacy and Independent Variables

Interaction between Self-efficacy and Independent Variables		
Independent Variable	**Dependent Variable**	**Supported?**
Top management support	Self-efficacy	Supported
Commitment	Self-efficacy	Supported
Sanction Severity	Self-efficacy	Not Supported
Reward	Self-efficacy	Not Supported
Monitoring/Evaluation	Self-efficacy	Supported

Table 6.4: Significant Variables

Mitigation Approach Degree of Significance	
Variable	**P-Value**
Monitoring/Evaluation and Self-efficacy	0.000 ***
Monitoring/Evaluation and Subjective norms	0.000 ***
Reward	0.000 ***
Sanction severity and Subjective norms	0.000 ***
Top management support and Attitude	0.001 ***
Commitment and Self-efficacy	0.001 ***
Monitoring/Evaluation and Attitude	0.003 **
Top management support and Self-efficacy	0.004 **
Commitment and Attitude	0.008 **
Sanction severity and Attitude	0.010 *
Reward and Subjective norms	0.012 *
Top management support	0.020 *
Monitoring/Evaluation	0.020 *
Reward and Attitude	0.024 *
Subjective norms	0.036 *
Sanction severity	0.040 *
*** Significant at $p \leq 0.001$; ** Significant at or $p \leq 0.01$; and * Significant at $p \leq 0.05$	

Table 6.5: Practical Application of Mitigation Approaches Deduce from the research.

Mitigation approaches derived from the research	Significance	Application in Practice
Monitoring/Evaluation and Self-efficacy	Very strong evidence	Regular monitoring and evaluation in an organisation will cause employees to effectively use their skills and competence in reducing ISTSC.
Monitoring/Evaluation and Subjective norms	Very strong evidence	Regular monitoring and evaluation will make employees act as expected by their manager and colleagues regarding mitigation of ISTSC.
Reward	Very strong evidence	Awards, pay rise, promotion etc stimulate a positive information security behaviour toward the supply chain, thereby lowering ISTSC.
Sanction severity and Subjective norms	Very strong evidence	The severity of sanctions put in place can deter information security misconduct and act as expected by managers and colleagues in securing the organisation information system.
Top Management Support and Attitude	Very strong evidence	Top management level of interest and target regarding ISTSC will determine employee attitude towards securing the organisation's supply chain information.
Commitment and Self-efficacy	Very strong evidence	The willingness, effort and energy workers' channels towards INSTSC will determine how effective they will apply their expertise/skills in protecting the organisation's supply chain information.
Monitoring/Evaluation and Attitude	Strong evidence	Awareness of active monitoring and evaluation of company information will influence employee attitudes towards protecting the supply chain information of the company.
Top management support and Self- efficacy	Strong evidence	Senior management interests and goals for ISTSC will affect how the worker will utilise their expertise and competence in securing the company supply chain.
Commitment and Attitude	Strong evidence	The energy and effort employees are willing to invest will directly influence their attitude towards securing the company supply chain information.
Sanction severity and Attitude	Moderate evidence	Sanction severity impacts employee attitude in helping to secure the information asset of the company.
Reward and Subjective norms	Moderate evidence	Incentives, pay rises and a reward system a company put in place will motivate workers to live up to management expectations which will in turn reduce ISTSC of the company.
Top management support	Moderate evidence	Top management interest and involvement in information security have a direct influence on information security threats in the supply chain of the company.
Monitoring/Evaluation	Moderate evidence	Active monitoring and evaluation of information systems effective approach to mitigate information security threats in the supply chain.
Reward and Attitude	Moderate evidence	Promotion, awards and person mentioned will foster a positive information security attitude in securing the supply chain information.
Subjective norms	Moderate evidence	Workplace norms and practices impact has a significant influence on employee behaviour and ISTSC.
Sanction	Moderate evidence	Sanction severity directly influences ISTSC and can be used to discourage workers from engaging in information security misconduct and by so doing securing the supply chain information.

6.10 Evaluation of the Model

The creation of the model (Figure 3.1) depicting the factors influencing the mitigation of information security threats in the supply chain at the employee level is a significant outcome of this thesis. The model encapsulates all the findings derived from the hypothesis testing conducted during the research. These hypotheses and the resulting model were formulated based on insights from existing academic literature and complemented by qualitative research, which further supported the quantitative analysis.

The model encompasses a comprehensive set of factors that were studied in this thesis but have not been examined in combination before. This theoretical contribution fills a gap in the existing literature by integrating and exploring the interplay of these factors. The literature review revealed that information security plays a critical role in ensuring the resilience of the supply chain. As discussed in Chapter 2, while work processes may vary across different forms of supply chains, the author of this thesis believes that the research findings on information security threats can have implications for studies conducted at various levels within an organization.

.

Chapter 7: Conclusion and limitation

7.1 Introduction

The previous chapter discussed the research questions, and they have been answered. The objectives of the current chapter are to summarise the main findings of this research, highlight the study's contribution, discuss the limitations and identify potential areas for future research, and provide some recommendations for improving information security in the supply chain. The chapter begins with a summary of the findings, followed by a discussion of the main contributions of this study. The third sections discuss the theoretical contribution and the limitations of the research, which will then be concluded with some directions for future research.

7.2 Research Summary

The position of information security in Nigeria has been analysed through quantitative data. The results showed that industries in Nigeria acknowledge the importance of information security in their supply chains. They are making efforts at each level to secure information assets internally as well as externally with their partners. The top management team of each company emphasises the importance of securing information with the employee and their supply chain partners

The overarching research question is intended to find out how information security threats in supply chain can be mitigated. Similar to the previous studies carried out in developed countries, information security in supply chains in Nigeria are prevented and reduce by a range of factors of informal and formal categories. However, when compared, some factors had more significance in Nigeria such as top management support and monitoring/evaluation, whereas some had very little significance, such as commitment. The findings reveal that developing countries still rely on Sanction and reward to reduce information security threats in their supply chain.

The first sub research question was aimed at discovering how the factors identified as employee's perception (attitude, subjective norms and self-efficacy) influence the reduction of threats in the supply chain. Amongst previous studies, some considered information security as one-dimensional while others considered it as multi-dimensional. In previous studies, the impacts of top management, commitment and monitoring/evaluating have not been examined in information security in supply chain context. Moreover, the impacts of sanction severity and rewards contradicted with the previous studies.

While attitude, subjective norms and self-efficacy were affected by different factors, monitoring/evaluation affected both. In addition, attitude was affected by top management, monitoring/ evaluation, commitment and sanction severity. Subjective norms were affected by monitoring/evaluation, sanction severity and reward, whereas self-efficacy was affected by

monitoring/evaluation, top management and commitment. This showed that the precursors of attitude, subjective norms and self-efficacy are different mainly due to the fact they affect employees at different levels. According to the results, monitoring/evaluation had the strongest positive impact on attitude, subjective norms and self-efficacy. Furthermore, top management support, commitment, sanction severity and reward exerted a mild positive effect. The research model explained 27% of the variation in attitude, 83% of the variation in subjective norms and 64% of variation in self-efficacy.

The second sub research question aimed to find out influential factors for mitigating information security threats in the supply chain. Among these factors, some factors had not been examined before in supply chain context, while some had been examined frequently because of their importance and some factors needed further examination to confirm their impact on information security in supply chain. Hypotheses were developed to investigate the relationship between factors and information security threats in the supply chain in the context of Nigeria. The findings revealed that information security threats in supply chain in Nigeria are reduced with the support of top management support, subjective norms, reward, sanction, monitoring/evaluation, commitment, attitude and self-efficacy. From the study, 1) Information security in the supply chain (not studied before) has been improved to have an impact on supply chain information security; 2) top management support, monitoring/evaluation, sanction and reward (frequently studied) were found to be important factors reducing information security threats in the supply chain in the context of Nigeria; and 3) attitude, subjective norms, self-efficacy and commitment (needed further examination) received further reports as factors reducing information security threats in the supply chain.

The qualitative analysis supported the quantitative findings. However, there were a few additional factors identified through interviews which failed to achieve statistical significance in the quantitative analysis. Commitment and top management support, in this study, did not find a direct relationship with subjective norms. More so, reward and sanction severity did not have direct relationship with self-efficacy. Yet, the constructs were still found to be an important factor in information security threats in supply chain because they have a positive and indirect relationship with information security threats in the supply chain via attitude and self-efficacy. More so, reward and sanction severity did not have direct relationship with self-efficacy. Although, they have a positive and indirect relationship with information security threats in the supply chain via attitudes. Interestingly, sanction did not have direct relationship with information security threats in the supply chain. While the quantitative results also showed that these factors influenced information security in the supply chain, they failed to achieve statistical significance level chosen by this study. In quantitative analysis (PLS-SEM), some of the items intended to measure these factors had to be deleted due to factor loadings. The likely reason for this is the improper phrasing of the items in the survey instrument.

7.3 Contribution of the Research

This study makes multiple contributions to both academic literature and practitioners in the field. Firstly, it identifies a comprehensive list of general and specific threats that impact the supply chain. Additionally, it proposes a model to investigate and mitigate information security threats within the supply chain. Despite the potential benefits of increased rewards for securing information among supply chain participants, the study highlights the failure of data security measures as required.

According to Hair et al. (2017), the inclusion of more independent variables in a model improves its predictive power and enables the development of more effective strategies. While existing literature has identified various factors influencing information security threats in the supply chain, no single study has comprehensively explored these factors. This study conducts a systematic literature review (SLR) to identify a comprehensive list of threats in the supply chain and delves deeper into the human factors associated with them.

Moreover, the study categorizes the identified factors into two sections. Although this categorization could not be empirically verified, it contributes to the literature as there is limited research on human factors in supply chain management. The study further contributes to the literature by examining the cause-and-effect relationship between information security threats and their impacts on supply chains. It presents a model that establishes the precursor-effect relationship of information security threats and tests it across different contexts, incorporating various causes (threats) and effects (General Deterrence Theory, Social Bond Theory, Theory of Planned behaviour, top management support, rewards, monitoring/evaluation). The study confirms that information security threats have a detrimental effect on a firm's supply chain performance. Therefore, it is crucial to enhance information security measures among supply chain participants. This underscores the importance of identifying and addressing potential factors to mitigate information security risks in the supply chain.

Moreover, supply chain companies in Nigeria and similar countries can employ this model to mitigate threats and improve the performance of their supply chains by proactively addressing information security threats both within and outside their chain. This study utilizes both quantitative and qualitative methods to gain a deeper understanding of the investigated issues and provide additional insights into the interpretation of research findings. Qualitative data collection supplements the quantitative data to enhance the accuracy of the results. While it reinforces the quantitative findings, it also uncovers supplementary results that help interpret the observed relationships and identify factors that may not have been acknowledged by the statistical analysis and its rationale.

The systematic literature review conducted in this study also highlights the geographical distribution of previous research. The majority of studies have been conducted in developed countries such as the United States, United Kingdom, Germany, Finland, Netherlands, Australia, New Zealand, Sweden, and South Korea, with the United States having the highest number of studies. Only a few studies have been

carried out in Asian countries like China and Taiwan, and there is a lack of research in developing countries like Nigeria and Ghana. Therefore, the second contribution of this study lies in its research conducted in Nigeria, providing context-specific insights that enrich supply chain management (SCM) research. Context-specific research enables the identification of best practices around the world based on their specific contextual specifications.

Meeting the Aim and Objectives of the thesis

Several objectives that were outlined in Chapter 1 and achieved as detailed in the preceding chapters helped to attain the aim of this thesis.

Table 7.1: Sections/Chapters

Objectives	Sections/Chapters
Objective 1	Chapter 2, Section 2.5, Tables 1 and 3
Objective 2	Chapter 2, Section 2.6, Table 4 and 5
Objective 3	Chapter 3 and Chapter 4
Objective 4	Chapter 5, Chapter 6, Chapter 7

- **Objective 1:** To critically review the threats that is prevalent in the information security threats in the supply chain.

  The literature study identified various information security threats predominant in the supply chain and further categorised them into technology-related and human-related threats (Chapter 2, Section 2.5, Tables 1 and 3).

- **Objective 2:** To identify and investigate human factors' influence in the mitigation of information security threats in the supply chain.

  The literature review that forms the baseline of this research explored the theoretical concept, findings and ISTSC mitigation approach recommended by previous authors (Chapter 2, Section 2.6, Tables 4 and 5).

- **Objective 3:** To develop and propose integrated human factors model for mitigating information security threats in the supply chain.

The study developed a conceptual framework underpinned by the Theory of Planned Behaviour (attitude, subjective norms and self-efficacy), Social Bond theory (commitment), General Deterrence Theory (sanction severity) and management control (top management support, reward, monitoring/evaluation) to mitigate ISTSC. Details can be seen in Chapters 3 and Chapter 4.

- **Objective 4:** To provide recommendations for business owners and managers to improve and secure their information security in supply chain.

In Chapter 5, the empirical data gathered from 450 survey questionnaires from 150 companies in 4 different industries, and 9 interviews with 5 companies in Nigeria were analysed and presented based on the justification of the research methodology (in chapter 4) and was used to test the suggested conceptual model. Testing and evaluating the conceptual model put forth in Chapter 3 was done during this process. The study results were considered in Chapter 6 and used to determine the theoretical framework. Conclusion, Contribution, Limitation and Future Research were reported in Chapter 7.

The development of a novel model to investigate and mitigate factors affecting information security threats in the supply chain made it possible to achieve the aforementioned objectives. Thus, the research has contributed to both academics and practice. The specific parts of the contribution made by this work come from various parts of this thesis: (a) from the background information given in Chapters 1, 2 and 3, (b) from the research methodology reported in Chapter 4, (c) from the planning and execution of research findings in Chapter 5, and finally (d) from the empirical analysis of the data gathered and the development of the revised model presented in Chapters 5 and 6.

- **Research Aim:** To investigate information security threats in the supply chain and propose a framework to mitigate these threats in the supply chain.

The theoretical model developed in chapters 5 and 6 provides an effective mitigation approach that can be adopted by organisations in reducing information security threats in their supply chain.

- **The overarching research question:**

How do the supply chain stakeholders mitigate information security threats in the supply chain?

Addressed adequately in the findings of this research in chapter 6.

- **Sub research questions**

  What factors influence employees' information security behaviour in the supply chain?

  Chapter 2 (Section 2.6.2) and Chapter 3.

- What factors mitigate information security threats in the supply chain?

  The question was addressed in Chapter 6.

7.4 Main Findings of this Thesis

The following summarises the key findings drawn from the research described in this thesis:

- **Finding 1:** The literature on information security threats in the supply chain is scant. While conducting a systematic literature review in this area and an empirical tested in four main business department in supply chain firms (Manufacturing, Logistic &Transport, Marketing & Distribution, and Production & Operation) from 150 companies in Nigeria, this was validated.
- **Finding 2:** The limited research available that identified and described predominant information security threats affecting the supply chain. This research presents an extensive list, description, category and impact of information security threats in the supply chain (See 2.6 and… chapter 2).
- **Finding 3:** When it comes to the influence of human factors on security supply chain information and mitigating ISTSC using the human approach, this study found limited extant literature on information security in the supply chain conducted in other fields of study. Ifinedo (2014) was concerning policy compliance, Safa et al. (2019) focused on insider threats in the organisation, Leering et al. (2022) was on non-compliant behaviour, Cuganasan et al. (2018) discussed the effect of senior managers and workplace norms on information security attitude, and Hutchinson et al., (2008) aim at user security awareness to mention but few (See Table 2.4). More so, other authors have adopted a technology approach to mitigating information security threats (Table 2.3). The human mitigation approach to information security threats in the supply chain makes the study novel.
- **Finding 4:** It was found that most of the previous studies as mentioned in Finding 3 above were conducted in developed countries like Canada, Finland, China, United States of America, Netherland as described in Table 2.5. This study is one of the pioneer research works on information security threats in the supply chain conducted in a developing country.

- **Finding 5:** The researcher found a gap in the factors affecting the security of supply chain information from the human factor perspective. By developing and testing a theoretical framework to fill this gap.

- **Developing and Testing a Framework**

  The primary objective of this study was to develop and test a theoretical framework for factors mitigating information security in the supply chain. Towards achieving this goal, this study reviewed prior related studies. As discussed in the earlier section, the literature review helped in identifying several important factors. Many of the identified factors were covered by three theories: GDT, SBT, TPB and control mechanisms. Several hypotheses were developed showing the relationships between the constructs inside the framework. The proposed framework was then tested using online questionnaires.

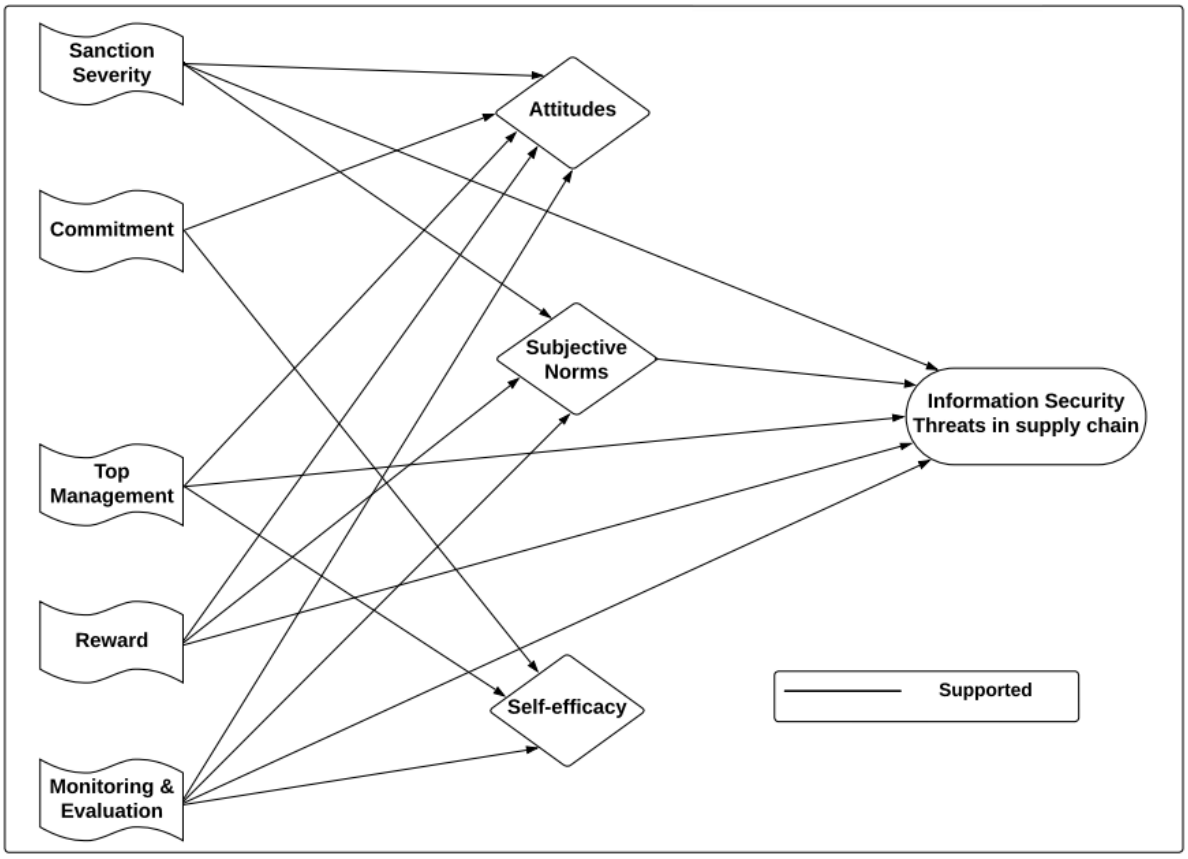


Figure 7.1: The Final Version of the Theoretical Framework

- **The Final Version of the Theoretical Framework**

As depicted in Figure 7.1, this study identifies four constructs that serve as predictors of information security threats within the supply chain. The findings indicate that top management support, rewards, sanctions, and monitoring/evaluation are positively associated with information security in the supply

chain. These results align with previous studies conducted by (Zhang and Welch 2021; Hu et al. 2012; Bulgucur et al.,2010).

In contrast to prior research conducted by Chen et al. (2013), this study did not find an indirect relationship between commitment and information security threats in the supply chain. However, commitment remains an important factor in information security as it exhibits a positive and direct relationship with attitude and self-efficacy. Moreover, in line with numerous empirical studies conducted by Leering et al. (2020), Safa et al. (2019, 2018), this study reveals that subjective norms have a direct influence on information security threats in the supply chain. Surprisingly, no direct relationship between attitude and self-efficacy was discovered, contrary to the results reported in several previous studies, such as Safa et al. (2016) and Ifinedo (2014). Nonetheless, attitude and self-efficacy are still considered crucial factors in information security, as these constructs exhibit direct relationships with other variables.

7.5 Statement of Contribution and Research Novelty

While information security literature is a prominent area of study in academia and is developing at a significant rate, evaluation and mitigation of factors affecting information security threats in the supply chain is a new area of study with little existing literature. There is, however, a dearth of literature in the domain of the human aspect in supply chain information security, as detailed in the pertinent chapters of this thesis. In light of this, this research contributes to both academics and industry.

7.5.1 Theoretical Contribution

Contribution 1: This study contributes significantly to the growing body of knowledge on the relationship between human behaviour and information security within the supply chain. It achieves this by proposing, modifying, and validating a framework aimed at mitigating information security threats in the supply chain. The framework is based on three theories: General Deterrence Theory (GDT), Social Bond Theory (SBT), and Theory of Planned behaviour (TPB), as well as the mechanisms of control such as top management support, rewards, and monitoring/evaluation. Existing literature has examined various factors rooted in general deterrence and social bond theories to explain how threats can be mitigated. The factors identified in this study discourage employees from engaging in information security misconduct within the organisation, thereby reducing threats in the supply chain. While both theories have a similar effect on attitudes (as per the TPB), GDT emphasizes individual perception and attitude, while social bond theory highlights the social ties employees have with the organization, which contribute to mitigating threats in the supply chain.

Empirical tested, to the best of the researcher knowledge, this is the study to offer a theoretical explanation and empirical support for the impact of an employee's belief to reduce information

security threats through the influence of attitude, subjective norms and self-efficacy within supply chain companies. The study showed that attitude towards reducing or perverting information security threats can be traced back to cognitive beliefs. In summary, the TPB help to design interventions and strategies that target employee belief, competency, attitude and perceptions to promote positive behaviours and discourage negatives ones.

- Previous research has examined how the severity of rewards and punishments can discourage inappropriate behaviour and encourage employees to reduce risks in the proposed model. This study stands out as one of the few that explores the impact of employee actions in reducing information security risks within the supply chain context. Consequently, the study has unveiled the significance of developing strategies to discourage potential wrongdoers and uphold a sense of social order.
- This study provides further support to the findings in the extant literature that showed that such factors as attitude, self-efficacy and subjective norms do have effect on employees' behaviour towards preventing threats. Monitoring/ evaluation is the key factors because it has a significant positive relationship on theory of planned behaviour and self-efficacy to mitigate information security threats in the supply chain. This result brings more understanding of the information security standard behaviour towards computer usage with the information standard that is attached to it and constant monitoring the activities of employees on the system. The results of the study also suggest that regular monitoring and evaluation within an organization lead to employees effectively utilising their skills and competencies to reduce information security threats in the supply chain (ISTSC)
- This research in the area of information security in supply chain opens an opportunity for development of a comprehensive integrative contingency model for assessing and reducing information security threats in supply chain.
- This study also has deepened our understanding of human behaviour in the face of information security threats. (See Chapter 3, 5 and 6)

Contribution 2: Contribution to the knowledge of Information security threats in the supply

This study has contributed immensely to extant literature through a systematic literature review on information security threats in the supply chain. The research identified an extensive list of information security threats in the supply chain and categorised these threats into technology-related and human-related information security threats. Several extant works of the literature identified and described either technology-related or human-related threats. However, this literature described both categories of threat in detail which can form a baseline for future research work in this area (See section 2.2, 2.2.1 Table 2.6.1)

Contribution 3: Novelty of testing the conceptual framework in a developing country (Nigeria).

Similar studies, conducted in other field were mostly in developed countries, like USA, Finland, Canada, Netherland, United Kingdom to mention but a few (see detail in Table 2.5). Most of the outcome of data analysis agrees with international standards presented in previous literature. Constructs like monitoring/evaluation and top management support influences information security directly and indirectly through mediating construct. While attitude and self-efficacy do not affect ISTSC directly they are observed to mediate the independent variables. This can provide the basis of testing the conceptual framework in other developing and developed countries to see how the construct interacts with the attitude and culture of the chosen community or countries.

Contribution 4: Contribution toward methodology

This study demonstrates the appropriateness of employing a mixed methods design when investigating a complex and intrusive topic. The literature suggests various forms of mixed methods research designs. In this study, qualitative research was conducted to complement the quantitative approach and aid in model verification. A paper discussing this topic has been accepted and presented at the BAM 2022 conference in Manchester, with publication yet to be published.

- **Practical Contribution**

This study's applications to practice are diverse. The findings of the study can assist managers, and business owners in identifying information-security-related threats in their supply chain and how to minimise the threats through their colleagues and employees by considering the four contributions below:

- **Contribution 1: Raising awareness of various information security threats in the supply chain.**
- This study raises the awareness level of supply chain operators about possible security threats that could affect their supply chain information and the consequence of these threats on their business. The in-depth description of each identified threat in the study makes it easier for companies to identify information security threats in their supply chain. The theoretical model created will provide organisations with a road map on effective mitigation approaches to reduce ISTSC see section 2.6).
- **Contribution 2: Raising awareness of the human perspective mitigation approach for ISTSC.**

Despite several extant works of literature employing technological approaches, information security threats in the supply chain are still on the increase. The study provides industries with insight on how to apply the human approach in mitigating supply chain information security threats. Practical application of mitigation approaches deduce from the research (Table 6.3) provides companies and managers with options on how to reduce these threats. The various interaction and degrees of influence of the independent factors on the dependent variables presented in this Table could form a baseline for an organisation's mitigation strategy. It offers company insight on a suitable line of attack in reducing ISTSC. Operators of the supply chain can utilise the outcome of this research and information on Table 6.3 to customise a mitigation method to work best for their peculiar work environment. This study suggests to organisations that Monitoring/evaluation and top management support have the most influence on employee involvement in minimising ISTSC.

In additions, this research shows that attitude on its own does not influence information security behaviour of employees. However, independent variables like top management support, monitoring and evaluation, and sanction severity when applied, influences the attitude of employees towards ISTSC. For a company to create a positive information security attitude in their workplace, the factor can be used to influence the attitude of worker and mitigate ISTSC.

- **Contribution 3: Contribution to companies in developing countries.**

  As much as the several aspect studies agree with international standards, and constructs from other similar studies. However, there are certain factors that disagree with extant literature as reported in section 6.2 For example, Attitude and information security behaviour was not supported by the research while it tested positive in a study conducted by Cuganesan et al., (2018). This could form a guideline for developing countries like Nigeria. It creates an opportunity for other researchers to test similar models in other developed countries within a supply chain context.

7.6 Research Limitation

This study had some limitations which need to be considered while interpreting the results. While efforts had been made to minimise them as much as possible, some of them could not be avoided. The limitations of this study are addressed below:

- **Sample Size**

Firstly, considering the context of Nigeria the researcher decided to collect the data by direct visitation with personnel to increase the response rate. However, during data collection, Nigeria was facing political instability, COVID-19, which caused a lockdown in the country. This created logistical difficulties, as it was not possible to visit these companies in person due to the lockdown caused by the pandemic. The distribution of questionnaire was more cumbersome as companies were closed during

this period and most management staff were working from home. Nigeria being a developing country, some of the junior staff either do not have internet at home or are not in possession of a mobile phone that can help complete the online interview. More so due to the high rate of cyber-crime in Nigeria several employees will rather complete a hard copy questionnaire due to a misconstrued belief that the online survey could pose a threat to their data if completed on their mobile device. And due to ongoing lockdown only limited paper questionnaire could be distributed. In addition, many companies refused to participate as they were busy trying to cope with the economic impact caused by COVID-19. One of the biggest challenges faced by the researcher was inability to conduct interviews for more than nine respondents from 3 organisations. Because of their busy schedules, the researcher was unable to set up appointments as a result. Two of the interviewees were hesitant to answer some questions as they consider it confidential considering their position in the company. These unanticipated events reduced the response rate, which restricted the sample size needed for various statistical studies. The quantity of interviews that could be conducted was also constrained by logistical difficulties.

- **Questionnaire design**

The quantitative questionnaire was lengthy, as evidenced by some of the responses we got from the respondents. However, it was created to deliver the best outcomes in the shortest amount of time. The ultimate length was necessary for the subsequent hypothesis testing. A few respondents claimed they found some of the questions to be perplexing, while another felt some of the questions were challenging to quantify. A key point raised by some of the respondents about knowledge, skill and expertise in securing supply chain information. They believed a section of the questionnaire placed an undue emphasis on these parameters, and as junior staff, they have no professional training that could help develop skill and expertise in securing supply chain information. These remarks can be helpful for future research, keeping in mind that the questionnaire was created as a result of the literature analysis and some empirical experiments.

- **Generalisability**

The study's sample was only collected from one developing nation, which limits the conclusions' generalisability in relation to other developed and developing countries due to unique socio-cultural behaviour towards information security in their supply chain. Another constraint of the study is the limited ability to generalize the findings to the global supply chain due to the small number of participants included in the research. The small sample size restricts the representativeness of the findings and their applicability to the larger population of the global supply chain.

Additionally, the intrusive nature of the study, particularly when conducted by a student researcher, poses a challenge in terms of participant engagement. Participants may feel reluctant to fully participate

and provide accurate information due to concerns about privacy and the potential consequences of their involvement.

7.7 Recommendation for Future Research

Recommendation 1: This study provides a foundation for future research into information security threats in the supply chain. Other studies could test this model or a similar model on other developing countries to determine the influence of the factors discussed in this study on information security threats in the supply chain. The findings of the study conducted by Cuganasan et al., (2018) and Safa et al. (2019) in the United Kingdom and Australia respectively reveal that attitude influences information security which disagrees with the finding of this study conducted in Nigeria. Further research in developing countries can be used to investigate how information security behaviour like attitude, self-efficacy and subjective norms can affect the supply chain. While some factors like (Top management support, reward, monitoring and evaluation) influences the security of supply chain information in both developed and developing countries, some other factor like attitude may not have an effect in developing countries' supply chain information security due to socio-cultural differences. As a result, it is not possible to generalise the findings of this study. The study suggests that this model be tested in various countries. So, evaluating the proposed model in numerous developing and developed nations could be a realistic area for future research. Furthermore, a comparison study could be carried out between emerging and developed countries to identify the effectiveness of the human factor mitigation approach in curbing information security threats in the supply chain as it will further enhance the findings of this study.

Recommendation 2: The data acquired from this research involves 550 distributed questionnaires and 9 interviews. Other studies could consider using a larger sample size with a special focus on increasing interviews conducted. The outcome of such data analysis can be compared with that of this study to further extend the human factor mitigation approach in supply chain information security threats. A large-scale survey will provide the chance to verify the model empirically tested by this study. Future research should aim to increase the sample size by including a more diverse range of participants from different sectors and countries within the global supply chain. Moreover, researchers should take steps to minimize the intrusive nature of the study, such as ensuring participant anonymity and confidentiality, building trust, and clearly explaining the purpose and benefits of the research to encourage participation.

Recommendation 3: Information security behaviour focused on the supply chain is in its infant stage as most previous studies are tailored to other field of study. Albrechetsen and Ho was centred on raising information security awareness in the organisation. Leering et al.; 2022, Ifinedo, 2012 discussed information security behaviour in relation to employee compliance. Cugnesan et al., (2018) study was on how senior management and workplace norms influences the information security attitude of

employees. Taking cue from this studies, future research could focus on extending this study by investigating information security behaviour of employees in the supply chain context.

References

Abawajy, J., 2014. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), pp.237-248.

Abbott, M.L. and McKinney, J., (2013) *Understanding and applying research desi-gn*. John Wiley & Sons.

Abd El-Latif, A.A., Abd-El-Atty, B., Mehmood, I., Muhammad, K., Venegas-Andraca, S.E. and Peng, J., (2021) Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities. *Information Processing & Management*, *58*(4), p.102549.

Abdullah, F.S., Abu Seman, A., Ibrahim, N., Majid, N.A., Abdul Wahab, N.M., Mustafa, M.S. and Mohd Sani, N.F., (2017) Web-based application of the internship management system. *Journal of Computing Research and Innovation (JCRINN)*, *2*(3), pp.46-51.

Abouzahra, M. and Ghasemaghaei, M., (2020) The antecedents and results of seniors' use of activity tracking wearable devices. *Health Policy and Technology*, *9*(2), pp.213-217.

Ahmad, A., Bosua, R. and Scheepers, R., (2014) Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security*, *42*, pp.27-39.

Ait Maalem Lahcen, R., Caulkins, B., Mohapatra, R., and Kumar, M.,(2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3(10), https://doi.org/10.1186/s42400-020-00050-w

Ajzen, I., (1985) *From intentions to actions: A theory of planned behavior* (pp. 11-39). Springer Berlin Heidelberg.

Ajzen, I., (1991) The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), pp.179-211.

Ajzen, I., (1999) Dual-mode processing in the pursuit of insight is no vice. *Psychological Inquiry*, *10*(2),

Akhyari, N., Ruzaini, A. A., and Rashid, A. H. (2018) Information security culture guidelines to improve employee's security behavior: A review of empirical studies. *Journal of Fundamental and Applied Sciences*, *10*(2S), 258-283.

Akinyomi, O.J., (2012) Examination of fraud in the Nigerian banking sector and its prevention. *Asian Journal of Management Research*, *3*(1), pp.182-194pp.110-112.

Aladenusi, T., (2020) COVID-19's Impact on Cybersecurity. *Deloitte Nigeria*.

Albrechetsen, E, & Hovden, J. (2010) Improving information security awareness and behavior through dialogue, participation, and collective reflection. An intervention study, Computer, and Security, Vol 29(4)

Alese, B.K., Dahunsi, F.M., Akingbola, R.A., Adewale, O.S. and Ogundele, T.J., (2014) Improving deception in honeynet: Through data manipulation. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)* (pp. 198-204). IEEE.

Aleroud, A. and Zhou, L., (2017) Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, *68*, pp.160-196.

Almeida, F., (2018) Strategies to perform a mixed methods study. *European Journal of Education Studies*.

Alanazi, S., Anbar, M., A. Ebad, S., Karuppayah, S. and Al-Ani, H.A., (2020) Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector. *Symmetry*, *12*(9), p.1544.

Al-Dhahri, S., Al-Sarti, M. and Abdul, A., (2017) Information security management system. *International Journal of Computer Applications*, *158*(7), pp.29-33.

AlHogail, A., (2015) Design and validation of information security culture framework. *Computers in human behavior*, *49*, pp.567-575.

Alhogail, A. and Mirza, A., (2014) a framework of information security culture change. *Journal of Theoretical & Applied Information Technology*, *64*(2).

Alimohamadian, S. and Abdi, F., (2014) Analyzing the effects of information technology on supply chain integration: The role of ERP success mediator. *Management Science Letters*, *4*(4), pp.799-806

Al-Izki, F. and Weir, G.R., (2016) Management attitudes toward information security in Omani public sector organisations. In *2016 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 107-112). IEEE.

Ali Vafaei-Zadeh, Thurasamy Ramayah, Haniruzila Hanifah, Sherah Kurnia, Imran Mahmud (2020) *Supply chain information integration and its impact on the operational performance of manufacturing firms in Malaysia. Information & Management.*

Alkhudhayr, F., Alfarraj, S., Aljameeli, B. and Elkhdiri, S., (2019), May. Information security: A review of information security issues and techniques. In (2019) 2nd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6).

Alshare, K.A., Lane, P.L. and Lane, M.R., (2018) Information security policy compliance: a higher education case study. *Information & Computer Security*, *26*(1), pp.91-108.

Alhassan, M.M. and Adjei-Quaye A. (2017) Information Security in a Global Age. Mediterranean Center of Social and Educational Research. 2 p. 113

Allison, P.D., 2009. Missing data. *The SAGE handbook of quantitative methods in psychology*, pp.72-89.

Allen, B., Kelly, T., Loyear, R., Poole, A., Awojulu, A., Kmetetz, A., Rakotomavo, M., Wang, Z., Xu, H., Xu, M. and Yuan, H. (2018) 'Security Risk Governance: A Critical Component to Managing Security Risk'. The Journal of Applied Business and Economics, 20 (1), 132-146

Anat Hovav, John D'Arcy (2012) *Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea*. Information & management 49(99-110)

Antonioli D., Bernieri G., Tippenhauer N., O., (2018) Taking Control: Design and Implementation of Botnets for Cyber-Physical Attacks with CPSBot

Anderson C, Baskerville R. L. Kaul M (2017) information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information, Journal of Management information system, Vol. 34 (4)

Andy Field (2018) Discovering Statistics Using IBM SPSS Statistics. Thousand Oaks, California. Sage Publication

Andrews, D., Nonnecke, B. & Preece, J. (2010) 'Electronic Survey Methodology: A Case Study in Reaching Hard-to-Involve Internet Users' International Journal of Human-Computer Interaction, 16(2), 185-210

Areej Alhogail Abdurrahman Mirza Saad Haj bakry (2015) A comprehensive human factor framework in information security in organisation. Journal of theorical applied information technology. Vol.78. No.2

Ashenden, D., (2018) In their own words: employee attitudes towards information security. *Information & Computer Security*.

Ashenden, D., (2008) Information Security management: A human challenge. *Information security technical report*, *13*(4), pp.195-201.

Ashton, M.C., Paunonen, S.V. and Lee, K., (2014) On the validity of narrow and broad personality traits: A response to. *Personality and Individual Differences*, *56*, pp.24-28.

Baihaqi, I. and Sohal, A.S., (2013) The impact of information sharing in supply chains on organisational performance: an empirical study. Production Planning & Control, 24(8-9), pp.743-758.

Badie N., Laskari A H., (2012) A New Evaluation Criteria for Effective Security Awareness in Computer Risk Management. Journal of Basic and Applied Scientific Research

Baker, W., Smith, G. and Watson, K., (2007) Information security risk in the e-supply chain. In *E-supply chain technologies and management* (pp. 142-161). IGI Global.

Bandura, A., (1977) Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, *84*(2), p.191.

Bandura, A., (1986) Fearful expectations and avoidant actions as coeffects of perceived self-inefficacy.

Bandura, A., (1986) The explanatory and predictive scope of self-efficacy theory. *Journal of social and clinical psychology*, *4*(3), pp.359-373.

Bandura, A., (1991) Social cognitive theory of self-regulation. *Organizational behavior and human decision processes*, *50*(2), pp.248-287.

Barratt, M., (2004) Understanding the meaning of collaboration in the supply chain. Supply Chain Management: an international journal, 9(1), pp.30-42.

Barratt, M. and Barratt, R. (2011), "Exploring internal and external supply chain linkages: Evidence from the field", Journal of Operations Management, Vol. 29, No. 5, pp. 514-528

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

Barton, M.A., Sutcliffe, K.M., Vogus, T.J. and DeWitt, T., (2015) Performing under uncertainty: Contextualized engagement in wildland firefighting. *Journal of Contingencies and Crisis Management*, *23*(2), pp.74-83.

Barton, K.A., Tejay, G., Lane, M. and Terrell, S., 2016. Information system security commitment: A study of external influences on senior management. *Computers & Security*, *59*, pp.9-25.

Baskerville, Richard, Frantz Rowe, and François-Charles Wolff.(2018) "Integration of information systems and cybersecurity countermeasures: an exposure to risk perspective." *ACM SIGMIS Database: the DATABASE for Advances in Information Systems 49*, no. 1 33-52.

Becker, S., Bryman, A. and Ferguson, H. eds., (2012) Understanding research for social policy and social work: themes, methods and approaches. policy press.

Bell, E., Bryman, A. and Harley, B., (2022) *Business research methods*. Oxford university press.

Bendovschi, A. (2015). Cyber-attacks: Trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31. doi:10.1016/S2212-5671(15)01077-1.

Benjamin, D.J., Berger, J.O., Johannesson, M., Nosek, B.A., Wagenmakers, E.J., Berk, R., Bollen, K.A., Brembs, B., Brown, L., Camerer, C. and Cesarini, D., (2018) Redefine statistical significance. *Nature human behaviour*, *2*(1), pp.6-10.

Benthall, S., (2017), September. Assessing software supply chain risk using public data. In *2017 IEEE 28th Annual Software Technology Conference (STC)* (pp. 1-5). IEEE.

Baskerville, R., Rowe, F., and Wolff, F. (2018) 'Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective'. ACM SIGMIS Database: The DATABASE for Advances in Information Systems 49 (1), 33-52

Bezshtanko, V. and Makarevych, O., (2016) Implementation of information security management system in organization. *Collection" Information Technology and Security"*, *4*(1), pp.33-43.

Boiko, A., &Shendryk, V. (2017). System integration and security of information systems. Procedia Computer Science 104, 35-42.

Boiko, A., Shendryk, V. and Boiko, O., (2019) Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia computer science*, *149*, pp.65-70.

Booth, J.A., Farrell, A. and Varano, S.P., (2008) Social control, serious delinquency, and risky behavior: A gendered analysis. *Crime & Delinquency*, *54*(3), pp.423-456.

Borghesi, A. and Gaudenzi, B., (2013) Risk Identification. *Risk Management*, pp.43-52.

Boss, S. R., Galletta, D. F., Benjamin L. P., Moody, G., D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors, MIS Quarterly, 39(4), 837-864.

Botetzagias, I., Dima, A.F. and Malesios, C., (2015) Extending the theory of planned behavior in the context of recycling: The role of moral norms and of demographic predictors. *Resources, conservation and recycling*, *95*, pp.58-67.

Blanchard, D., (2010) *Supply chain management best practices*. John Wiley & Sons.

Braun, V. and Clarke, V., (2019) Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health*, *11*(4), pp.589-597.

Brotby, W.K. and Hinson, G., (2013) Pragmatic security metrics: applying metametrics to information security. CRC Press.

Brown Hart. S (2015) After the data breach: Managing the crisis and mitigating the impart, Journal of business Continuity &Emergency planning. Volume 8(4)

Bryman, A., (2006) Integrating quantitative and qualitative research: how is it done? *Qualitative research*, *6*(1), pp.97-113.

Bryman, A., (2016) *Social research methods*. Oxford university press.

Bronstein, J., and Tzivian, L. (2013). Perceived self-efficacy of library and information science professionals regarding their information retrieval skills. Library & Information Science Research, 35(2), 151

Bulgurcu, B., Cavusoglu, H. and Benbasat, I., (2010) Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, pp.523-548.

Cai, S., Jun, M. and Yang, Z. (2010), "Implementing supply chain information integration in China: The role of institutional forces and trust", Journal of Operations Management, Vol. 28, No. 3, pp. 257-268

Canova, L., Bobbio, A. and Manganelli, A.M., (2020) Predicting fruit consumption: A multi-group application of the Theory of Planned Behavior. *Appetite*, *145*, p.104490.

Caputo, A., (2020) Comparing theoretical models for the understanding of health-risk behaviour: Towards an integrative model of adolescent alcohol consumption. *Europe's Journal of Psychology*, *16*(3), p.418.

Carcary, M., Renaud, K., McLaughlin, S. and O'Brien, C. (2016) 'A Framework for Information Security Governance and Management'. It Professional, 18 (2), 22-30

Cavusoglu, H., Son, J.Y. and Benbasat, I., (2015) Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information & Management*, *52*(4), pp.385-400.

Cayetano, T.A., Dogao, A., Guipoc, C. and Palaoag, T., (2018), March. Cyber-physical IT assessment tool and vulnerability assessment for semiconductor companies. In *Proceedings of the 2nd International Conference on Cryptography, Security and Privacy* (pp. 67-71).

Colwill, (2009) "Human factors in information security: The insider threat – Who can you trust these days?," Inf. Secur. Tech. Rep., vol. 14, no. 4, pp. 186–196, Nov. 2009.

Cid-Fuentes, J.Á., Szabo, C. and Falkner, K., (2018) An adaptive framework for the detection of novel botnets. *Computers & Security*, *79*, pp.148-161.

Chan, M., Woon, I. and Kankanhalli, A., (2005) Perceptions of information security in the workplace: linking information security climate to compliant behavior. *Journal of information privacy and security*, *1*(3), pp.18-41.

Chiew, K.L., Yong, K.S.C. and Tan, C.L., (2018). A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications*, *106*, pp.1-20.

Chapple, C.L., (2005) Self-control, peer relations, and delinquency. *Justice Quarterly*, *22*(1), pp.89-106.

Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behavior: a technology threat avoidance perspective. Information and Computer Security, 25(3), 330-344.

Chen.J A.N.K. Ramamurthy and Wen (2015) Impacts of Comprehensive Information Security Culture. Journal of Computer Information Systems 55(3) 11-9

Chen, J., Huang, Y., Xia, P., Zhang, Y. and Zhong, Y., (2019) Design and implementation of real-time traceability monitoring system for agricultural products supply chain under Internet of Things architecture. *Concurrency and Computation: Practice and Experience*, *31*(10), p.e4766.

Chen, J., Zhong, M., Li, J., Wang, D., Qian, T. and Tu, H., (2021) Effective deep attributed network representation learning with topology adapted smoothing. IEEE Transactions on Cybernetics, 52(7), pp.5935-5946.

Cheng, J.T., Tracy, J.L., Foulsham, T., Kingstone, A. and Henrich, J., (2013) Two ways to the top: evidence that dominance and prestige are distinct yet viable avenues to social rank and influence. *Journal of personality and social psychology*, *104*(1), p.103.

Chen, L., Zhao, X., Tang, O., Price, L., Zhang, S. and Zhu, W., (2017) Supply chain collaboration for sustainability: A literature review and future research agenda. *International Journal of Production Economics*, *194*, pp.73-87.

Chen P. Kataria, G.and Krisshnan R (2011) Correlated failures, diversification and information security risk Mis Quarterly, 35 (2) 397-393

Chen Y. H.. LinT.P and Yen, D. C. (2014) How to facilitate inter-organizational knowledge sharing: The impact of trust. Information and management,51 (5), 568-578

Chen, Y., and Zahedi, F.M. (2016) "Individuals' Internet Security Perceptions and Behaviours: Polycontextual Contrasts between the United States and China.," MIS Quarterly (40:1), pp 205-222.

Chen Y. H. LinT.P and Yen, D. C. (2014) How to facilitate inter-organizational knowledge sharing: The impact of trust. Information and management,51 (5), 568-578

Chen, Z.F. and Cheng, Y., (2020) Consumer response to fake news about brands on social media: the effects of self-efficacy, media trust, and persuasion knowledge on brand trust. *Journal of Product & Brand Management*, *29*(2), pp.188-198.

Cheng, H. K., Sims, R. R., & Teegen, H. (1997). To Purchase or to pirate software: An Empirical Study. *Journal of Management Information Systems, 13*(4), 49-60.

Cheng, L., Li, Y., Li, W., Holm, E. and Zhai, Q., 2013. Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, *39*, pp.447-459.

Chesnut, S.R. and Burley, H., (2015) Self-efficacy as a predictor of commitment to the teaching profession: A meta-analysis. *Educational research review*, *15*, pp.1-16.

Cheung, K.F., Bell, M.G. and Bhattacharjya, J., (2021) Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, p.102217.

Chileshe, N., Hosseini, M.R. and Jepson, J., (2016) Critical barriers to implementing risk assessment and management practices (RAMP) in the Iranian construction sector.

Chirasha, V., (2013) Human Resource Development, Emotional Intelligence and Social Capital for Senior Managers in the Hospitality Industry in Zimbabwe. *African Education Indices*, *5*, pp.1-9.

Choi, T.M. and Luo, S., (2019) Data quality challenges for sustainable fashion supply chain operations in emerging markets: Roles of blockchain, government sponsors and environment taxes. *Transportation Research Part E: Logistics and Transportation Review*, *131*, pp.139-152.

Chopra, S. & Meindl, P. (2003). Supply Chain Management. Strategy, Planning & Operations, Prentice Hall, Upper Saddle River, New Jersey

Christopher, M., (2016) *Logistics & supply chain management*. Pearson Education, New York, NY

Christy, A.Y., Fauzi, B.N., Kurdi, N.A., Jauhari, W.A. and Saputro, D.R.S., (2017), June. A closed-loop supply chain under retail price and quality dependent demand with remanufacturing and refurbishing. In Journal of Physics: Conference Series (Vol. 855, No. 1, p. 012009). IOP Publishing.

Colajanni, G., Daniele, P. and Sciacca, D., (2020) A projected dynamic system associated with a cybersecurity investment model with budget constraints and fixed demands. *J. Nonlinear Var. Anal*, *4*(1), pp.45-61.

Colicchia, C., Creazza, A. and Menachof, D.A., (2019) Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), pp.215-240.

Collier, Zachary A., Daniel DiMase, Steve Walters, Mark Mohammad Tehranipoor, James H. Lambert, and Igor Linkov. "Cybersecurity standards: Managing risk and creating resilience." *Computer* 47, no. 9 (2014): 70-76

Couce-Vieira, A. and Houmb, S.H., (2016) The role of the supply chain in cybersecurity incident handling for drilling rigs. In Computer Safety, Reliability, and Security, Proceedings 35 (pp. 246-255). Springer International Publishing.

Cox (2012) In formation system user security: a structured model of doing gap. Computer & Human Behaviour Vol. 28 (5)

Creswell, J.W., (2009) Research designs: Qualitative, quantitative, and mixed methods approach. Callifornia: Sage

Creswell, J.W., (2012) Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Pearson Education, Inc.

Creswell, J., Klassen, A.C., Plano Clark, V.L., Smith, K.C. and Meissner, H.I., (2012) Best practices in mixed methods for quality-of-life research. *Quality of life Research*, *21*, pp.377-380.

Creswell, J.W., (2014) A concise introduction to mixed methods research. SAGE publications.

Creswell, J.W. and Creswell, J.D., (2017) Research design: Qualitative, quantitative, and mixed methods approach. Sage publications.

Creswell, J.W. and Clark, V.L.P., (2017) *Designing and conducting mixed methods research*. Sage publications.

Cresswell, J.W. and Plano Clark, V.L., (2011) Designing and conducting mixed methods research.

Creswell, J.W. and Tashakkori, A., (2007) Differing perspectives on mixed methods research. *Journal of mixed methods research*, *1*(4), pp.303-308.

Creswell, J.W., Forman, J., Damschroder, L., Kowalski, C.P. and Krein, S.L., (2008) Qualitative research methods: key features and insights gained from use in infection prevention research. *American journal of infection control*, *36*(10), pp.764-771.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R., (2013) Future directions for behavioral information security research. *computers & security*, *32*, pp.90-101.

Cuganesan, S., Steele, C. and Hart, A., (2018) How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & information technology*, *37*(1), pp.50-65.

Cui, L., Gao, M., Dai, J. and Mou, J., (2022) Improving supply chain collaboration through operational excellence approaches: an IoT perspective. *Industrial Management & Data Systems*, *122*(3), pp.565-591.

Cui, R., Gallino, S., Moreno, A. and Zhang, D.J., (2018). The operational value of social media information. *Production and Operations Management*, *27*(10), pp.1749-1769.

Dang-Pham, D., Kautz, K., Hoang, A.P. and Pittayachawan, S., (2022) Identifying information security opinion leaders in organizations: Insights from the theory of social power bases and social network analysis. *Computers & Security*, *112*, p.102505.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employee's security compliance. Information Management and Computer Security, 22(5), 474-489.

D'arcy, J. and Herath, T., (2011) A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European journal of information systems*, *20*(6), pp.643-658.

D'Arcy, J., Herath T. Shoss M.k (2014) Understanding Employee Responses to Stressful information Security Requirement: A Coping Perspective. Journal of Management Information systems, 31(2) 285-318).

D'Arcy, J., Hovav, A. and Galletta, D., (2009) User awareness of security countermeasures and its impact on information system misuse: A deterrence approach. *Information systems research*, *20*(1), pp.79-98.

Das, T., Eldosouky, A.R. and Sengupta, S., (2020), June. Think smart, play dumb: Analyzing deception in hardware trojan detection using game theory. In *2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE.

D'Arcy, J., Herath T. Shoss M.k (2014) Understanding Employee Responses to Stressful information Security Requirement: A Coping Perspective. Journal of Management Information systems, 31(2) 285-318).

Debnath, B., Das, A., Das, S. and Das, A., (2020), February. Studies on security threats in waste mobile phone recycling supply chain in India. In *2020 IEEE Calcutta Conference (CALCON)* (pp. 431-434). IEEE.

de Barros, A.P., Ishikiriyama, C.S., Peres, R.C. and Gomes, C.F.S., (2015) Processes and benefits of the application of information technology in supply chain management: an analysis of the literature. *Procedia Computer Science*, *55*, pp.698-705.

de Haan, J., (2020), June. Specific air traffic management cybersecurity challenges: architecture and supply chain. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops* (pp. 245-249).

Denzin, N. K. and Lincoln, Y. S. (2012) Collecting and Interpreting Qualitative Materials.: Sage Publications

De Vass, T., Shee, H. and Miah, S.J., (2018) The effect of "Internet of Things" on supply chain integration and performance: An organisational capability perspective. *Australasian Journal of Information Systems*, *22*.

Dessler, G (2011) Human resource management (12th ed) Harlow, UK: Pearson Education.

De Meulemeester, A. (2013). The "Information Literacy Self-Efficacy Scale" and the Medical Curriculum at Ghent University. Communications in Computer and Information Science. Volume 397 CCIS, pp. 465-470.

Dhillon, G. and Torkzadeh, G., (2006) Value-focused assessment of information system security in organizations. *Information Systems Journal*, *16*(3), pp.293-314.

Dhillon, G., (2007) *Principles of information systems security: Texts and cases*. John Wiley & Sons Incorporated.

Dhillon, G., Tejay, G. and Hong, W. (2007) 'Identifying Governance Dimensions to Evaluate Information Systems Security in Organisations' in (ed.) 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). held at IEEE, 157b-157

Dijkstra, J.K., Cillessen, A.H., Lindenberg, S. and Veenstra, R., (2010) Basking in reflected glory and its limits: Why adolescents hang out with popular peers. *Journal of Research on Adolescence*, *20*(4), pp.942-958..

Dilley, P., (2004) Interviews and the philosophy of qualitative research.

Drost, E.A., (2011) Validity and reliability in social science research. *Education Research and perspectives*, *38*(1), pp.105-123.

Dubey, R., Gunasekaran, A., Papadopoulos, T., Childe, S. J., Shibin, ., K. T., & Wamba, S. F. (2017). Sustainable supply chain management: framework and further research directions. Journal of Cleaner Production, 142, 1119-1130.

Dupin-Bryant, P.A., (2010) Software piracy: Exploring awareness of the law as a determinant of softlifting attitude and intention. *Issues in Information Systems*, *11*(1), pp.17-22.

Dunlop, P.D. and Lee, K., (2004) Workplace deviance, organizational citizenship behavior, and business unit performance: The bad apples do spoil the whole barrel. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, *25*(1), pp.67-80.

.Dubrin A. J. (2009) Essentials of management (8th ed.) Mason, OH: South-Western

Durowoju, O., (2014) Implication of information disruption to supply chain improvement strategy decision-an entropy perspective (Doctoral dissertation, University of East Anglia).

Durowoju, O., Chan, H.K. and Wang, X., (2020) Investigation of the effect of e-platform information security breaches: a small and medium enterprise supply chain perspective. *IEEE Transactions on Engineering Management*, *69*(6), pp.3694-3709.

Du, T.C., Lai, V.S., Cheung, W. and Cui, X., (2012) Willingness to share information in a supply chain: A partnership-data-process perspective. *Information & Management*, *49*(2), pp.89-98.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K. and Kyngäs, H. (2014) 'Qualitative Content Analysis: A Focus on Trustworthiness'. Sage Open 4 (1)

Evans, N. (2003), "Information Security Guideline For NSW Government – Part 1 Information Security Risk Management", Office of Information and Communication Technology Syney, [Online], Sept 18, 2019 at https://pdfslide.net/documents/information-security-guideline-for-nsw-government-part-1.html?page=1

Evans, M., He, Y., Maglaras, L. and Janicke, H., (2019) HEART-IS: A novel technique for evaluating human error-related information security incidents. *Computers & Security*, *80*, pp.74-89.

Evans, M.G., He, Y., Yevseyeva, I. and Janicke, H., (2018) Information Security Incidents and Breaches to establish the Proportions of Human Error. In *HAISA* (pp. 191-202).

Evans, M., Maglaras, L and Janicke, H. (2016) Human behaviour as an aspect of cyber security assurance, Computer & Security. 1-22

Fagnot, I. and Paquette, S., (2012) Organizational information security: The impact of employee attitudes and social media use.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information system. Information Technology and Management archive, 6, 202-225.

Fawcett, S.E. Osterhaus, P. Magnan, G.M. Brau, J.C. and McCarter, M.W., (2007) Information sharing and supply chain performance: the role of connectivity and willingness. *Supply Chain Management: An International Journal*, *12*(5), pp.358-368.

Femi-Oyewole, F. (2015). Information security in business: Issues and solutions. A covenant university presentation. March 2015.

Feng, G., Zhu, J., Wang, N. and Liang, H.,(2019). How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond. *Journal of the Association for Information Systems*, *20*(11), p.2.

Fernández-Caramés, T.M., Blanco-Novoa, O., Froiz-Míguez, I. and Fraga-Lamas, P., (2019) Towards an autonomous industry 4.0 warehouse: A UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *Sensors*, *19*(10), p.2394.

Fidel, R., (2008) Are we there yet?: Mixed methods research in library and information science. *Library & information science research*, *30*(4), pp.265-272.

Flores, W.R. and Ekstedt, M., (2016) Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & security*, *59*, pp.26-44.

Flynn B. Huo B. & Zhao X (2010) The impact of supply chain integration on performance: A contingency and configuration approach. Journal of Operation Management, Vol 28 (1) pp 58-71

Forman, J. and Damschroder, L., 2007. Qualitative content analysis. In *Empirical methods for bioethics: A primer* (pp. 39-62). Emerald Group Publishing Limited.

Fowler, K., (2016) *Data breach preparation and response: breaches are certain, impact is not*. Syngress.

Fraile, F., Tagawa, T., Poler, R. and Ortiz, A., (2018) Trustworthy industrial IoT gateways for interoperability platforms and ecosystems. *IEEE Internet of Things Journal*, *5*(6), pp.4506-4514.

Frank, I. and Odunayo, E., (2013) Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of Cognitive Research in science, engineering and education*, *1*(1), pp.100-110.

Fricker, R.D., (2008) Sampling methods for web and e-mail surveys. The SAGE handbook of online research methods. London: SAGE Publications Ltd.

G. Dhillon, Principles of information systems security. John Wiley & Sons., 2007.

Ghadge, A., Dani, S. and Kalawsky, R., (2012) Supply chain risk management: present and future scope. *The international journal of logistics management*.

Giampietri, E., Verneau, F., Del Giudice, T., Carfora, V. and Finco, A., (2018) A Theory of Planned behaviour perspective for investigating the role of trust in consumer purchasing decision related to short food supply chains. *Food Quality and Preference*, *64*, pp.160-166.

Ganguly, K.K. and Guin, K.K., (2013) A fuzzy AHP approach for inbound supply risk assessment. *Benchmarking: An International Journal*.

Garson, G.D., (2016) Partial least squares (PLS-SEM): Regression and structural equation models. *North Carolina: Statistical Publishing Associates*.

Gerow, J.E., Galluch, P.S. and Thatcher, J.B., (2010) To slack or not to slack: Internet usage in the classroom. *JITTA: Journal of Information Technology Theory and Application*, *11*(3), p.5.

Ghadge, A., Weiß, M., Caldwell, N.D. and Wilding, R., (2020) Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), pp.223-240.

Gharib, R.K., Philpott, E. and Duan, Y., 2017. Factors affecting active participation in B2B online communities: An empirical investigation. *Information & Management*, *54*(4), pp.516-530.

Ghoroghchian, M., Adeli, O.A., Safa, M. and Pourfakharan, M.R., (2022) A Framework for Identifying LARG Supply Chain Risks. *Journal of Environmental Science and Technology*.

Gjerdrum, D. and Peter, M. (2011) The New International Standard on the Practise of Risk Management – A Comparison of ISO 31000: 2009 and the COSO ERM Framework. Risk Management 31(2), 8-13

Gunasekaran, A. and Kobu, B., 2007. Performance measures and metrics in logistics and supply chain management: a review of recent literature (1995–2004) for research and applications. International journal of production research, 45(12), pp.2819-2840.

Goo, J., Yim, M.S. and Kim, D.J., (2014) A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication*, *57*(4), pp.286-308.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: a review and synthesis. Computers and Security, 32, 242-251.

Guo, K.H. and Yuan, Y., (2012) The effects of multilevel sanctions on information security violations: A mediating model. *Information & management*, *49*(6), pp.320-326.

Gupta, N., Chen, F., Tsoutsos, N.G. and Maniatakos, M., (2017) Obfuscating additive manufacturing CAD models against counterfeiting. In *Proceedings of the 54th Annual Design Automation Conference 2017* (pp. 1-6).

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

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M., (2019) When to use and how to report the results of PLS-SEM. *European business review*, *31*(1), pp.2-24.

Hair Jr, J.F., Sarstedt, M., Ringle, C.M. and Gudergan, S.P., (2017) *Advanced issues in partial least squares structural equation modeling*. saGe publications.

Hajmohammad, S. and Vachon, S., (2014) Managing supplier sustainability risk: Strategies and predictors. In *Academy of Management Proceedings* (Vol. 2014, No. 1, p. 14266). Briarcliff Manor, NY 10510: Academy of Management.

Handfield, R., Jeong, S. and Choi, T., (2019) Emerging procurement technology: data analytics and cognitive analytics. *International Journal of Physical Distribution & Logistics Management*, *49*(10), pp.972-1002.

Handfield, R.B. and Nichols Jr, E.L., (1999) Introduction to. Supply Chain Management, Prentice Hall, Englewood Cliffs, NJ, pp.1-29.

Handfield, R., Blackhurst, J., Craighead, C.W. and Elkins, D., 2011. Introduction: a managerial framework for reducing the impact of disruptions to the supply chain. [online] http://scm. ncsu. edu/scm-articles/article/introduction-a-managerial-framework-for-reducingthe-impact-of-disruptions-(accessed 14 April 2019).

Hannah, D.R. and Robertson, K., (2015) Why and how do employees break and bend confidential information protection rules?. *Journal of management studies*, *52*(3), pp.381-413.

Hanafy H. A. and Hashem A. E (2017). The impact of information security initiative on supply chain performance. *Global Journal of Management and Business Research*

Hart, C., (2018) Doing a literature review: Releasing the research imagination.

Hasibuan, A., Arfah, M., Parinduri, L., Hernawati, T., Harahap, B., Sibuea, S.R. and Sulaiman, O.K., (2018), April. Performance analysis of supply chain management with supply chain operation reference model. In *Journal of Physics: Conference Series* (Vol. 1007, No. 1, p. 012029). IOP Publishing.

Henle, C.A. and Blanchard, A.L., 2008. The interaction of work stressors and organizational sanctions on cyberloafing. *Journal of managerial issues*, pp.383-400.

Henseler, J., Ringle, C.M. and Sarstedt, M., 2015. A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the academy of marketing science*, *43*, pp.115-135.

Herath, T. and Rao, H.R., (2009) Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*, pp.106-125.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J. and Rao, H.R., (2014) Security services as coping mechanisms: An investigation into user intention to adopt an email authentication service. *Information systems journal*, *24*(1), pp.61-84.

Hinchliffe, A., (2017) Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime. *Computer Fraud & Security*, *2017*(5), pp.5-9.

Hirschi, T. and Selvin, H.C., (1967) Delinquency Research: An Appraisal of Analytic. *Methods*.

Hirschi, T. and Stark, R., (1969) Hellfire and delinquency. *Social Problems*, *17*(2), pp.202-213.

Hoe, S.L., (2008). Issues and procedures in adopting structural equation modelling technique. *Journal of Quantitative Methods*, *3*(1), p.76.

Holdsworth, S., Sandri, O., Thomas, I., Wong, P., Chester, A. and McLaughlin, P., (2019) The assessment of graduate sustainability attributes in the workplace: Potential advantages of using the theory of planned behaviour (TPB). *Journal of Cleaner Production*, *238*, p.117929.

Hooper, D., Coughlan, J. and Mullen, M., (2008), September. Evaluating model fit: a synthesis of the structural equation modelling literature. In *7th European Conference on research methodology for business and management studies* (pp. 195-200).

Hovav, A. and D'Arcy, J., (2012) Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, *49*(2), pp.99-110.

Hsu, M.H. and Chiu, C.M., (2004) Predicting electronic service continuance with a decomposed theory of planned behaviour. *Behaviour & Information Technology*, *23*(5), pp.359-373.

Hua, J. and Bapna, S., (2013) Who can we trust?: the economic impact of insider threats. *Journal of Global Information Technology Management*, *16*(4), pp.47-67.

Hudnurkar, M., Deshpande, S., Rathod, U. and Jakhar, S., (2017) Supply chain risk classification schemes: A literature review. *Operations and Supply Chain Management: An International Journal*, *10*(4), pp.182-199.

Hu, Q., Dinev, T., Hart, P. and Cooke, D., (2012) Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), pp.615-660.

Humaidi, N. and Balakrishnan, V., (2015) Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology*, *5*(4), p.311.

Humaidi, Norshima, and Vimala Balakrishnan. "Indirect effect of management support on users' compliance behaviour towards information security policies." *Health Information Management Journal* 47, no. 1 (2018): 17-27.

Hutchins, M.J., Bhinge, R., Micali, M.K., Robinson, S.L., Sutherland, J.W. and Dornfeld, D., (2015) Framework for identifying cybersecurity risks in manufacturing. *Procedia Manufacturing*, *1*, pp.47-63.

Hutchinson, J.C., Sherman, T., Martinovic, N. and Tenenbaum, G., (2008) The effect of manipulated self-efficacy on perceived and sustained effort. *Journal of Applied Sport Psychology*, *20*(4), pp.457-472.

Ifinedo, P., (2012) Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), pp.83-95.

Ifinedo, P., (2014) Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), pp.69-79.

Iftekhar, A., Cui, X., Hassan, M. and Afzal, W., (2020) Application of blockchain and Internet of Things to ensure tamper-proof data availability for food safety. *Journal of Food Quality*, *2020*, pp.1-14.

Koskosas, K. Kakoulidis, and C. Siomos, "Information Security: Corporate Culture and Organizational Commitment," Int. J. Humanit. Soc. Sci., vol. 1, no. 3, pp. 192–198, 2011. [

Ashenden, (2009)"Information Security Management: A Human Challenge?," Inf. Secur. Tech. Rep., vol. 13, no. 4, pp. 195– 201, 2009.

Imeri, A. and Khadraoui, D., 2018, February. The security and traceability of shared information in the process of transportation of dangerous goods. In *(2018) 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* (pp. 1-5). IEEE.

Information Security Breaches Survey, "(2014) Information Security Breaches Survey," 2014

ISO/IEC 27002 (2013), Information Technology — Security Techniques — Code of Practice for Information Security Controls, 2nd ed., ISO/IEC 27002. 270.

Ivankova, N.V., Creswell, J.W. and Stick, S.L., (2006) Using mixed-methods sequential explanatory design: From theory to practice. *Field methods*, *18*(1), pp.3-20.

Jaafar, N.I. and Ajis, A., (2013) Organizational climate and individual factors effects on information security compliance behaviour. *International Journal of Business and Social Science*, *4*(10).

Jankowicz, A.D., 2013. *Business research projects*. Springer.

Javorcik, T., Kostolanyova, K. and Havlaskova, T., (2023) Microlearning in the Education of Future Teachers: Monitoring and Evaluating Students' Activity in a Microlearning Course. Electronic Journal of e-Learning, 21(1), pp.13-25.

Jegede, A.E., (2014) Cyber fraud, global trade and youth crime burden: Nigerian experience. *Afro Asian Journal of Social Sciences*, *5*(4).

Johnson, D., Deterding, S., Kuhn, K.A., Staneva, A., Stoyanov, S. and Hides, L., (2016) Gamification for health and wellbeing: A systematic review of the literature. *Internet interventions*, *6*, pp.89-106.

Johnson, R.B., Onwuegbuzie, A.J. and Turner, L.A., (2007) Toward a definition of mixed methods research. *Journal of mixed methods research*, *1*(2), pp.112-133.

Johnston, A.C., Warkentin, M. and Siponen, M., (2015) An enhanced fear appeal rhetorical framework. *MIS quarterly*, *39*(1), pp.113-134.

Johnston, A.C. and Warkentin, M., (2010) Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, pp.549-566.

Jones, R.A. and Horowitz, B., (2012) A system-aware cyber security architecture. *Systems Engineering*, *15*(2), pp.225-240.

J. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," Comput. Secur., vol. 29, no. 4, pp. 476–486, Jun. 2010

Kaljahi, M. A., Payandeh, A., & GhaznaviGhoushchi, M. B. (2015). TSSL: Improving SSL/TLS protocol by trust model. Security and Communication Networks, 8(9), 1659-1671.

Kalu, S.R., Menon, S.E. and Quinn, C.R., (2020) The relationship between externalizing behavior and school and familial attachments among girls from diverse backgrounds. *Children and Youth Services Review*, *116*, p.105170.

Kampanakis, P., (2014) Security automation and threat information-sharing options. *IEEE Security & Privacy*, *12*(5), pp.42-51.

Kamal Dahbur, Maysoon R. Isleem, Sara Ismail (2012) A Study of Information Security Issues and Measures in Jordan. International management review

Kaspersky Lab (2017). Employees are one of the biggest cyberthreats to businesses in North America. Business Wire (English), Kaspersky Lab, Moscow.

Karlsson, F., Kolkowska, E. and Prenkert, F., (2016) Inter-organisational information security: A systematic literature review. *Information & Computer Security*, *24*(5), pp.418-451.

Karlsson, F., Karlsson, M. and Åström, J., (2017) Measuring employees' compliance–the importance of value pluralism. *Information & Computer Security*.

Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, Cata Jerram (2014) Journal of Computer and Security, Vol 42 (165-176)

Kembro, J., Selviaridis, K. and Näslund, D., (2014) Theoretical perspectives on information sharing in supply chains: a systematic literature review and conceptual framework. *Supply chain management: An international journal*.

Kennedy, S. E. (2016). The pathway to security-mitigating user negligence. Information and Computer Security, 24(3), 255-264.

Kenny, S., (2017) Strengthening the network security supply chain. *Computer Fraud & Security*, *2017*(12), pp.11-14.

Kevin A. Barton, Guivirender Tejay, Michael Lane, Steve Terrell (2016) *Information system security commitment: A study of external influence on senior management*. Computers & Security 59 (9-25).

Keshnee Padayachee (2013) A conceptual Opportunity-based framework to mitigate the insider threat. IEEE explores

Kim, H.W. and Kankanhalli, A., (2009) Investigating user resistance to information systems implementation: A status quo bias perspective. *MIS quarterly*, pp.567-582.

Kim, K.C. and Im, I., (2014) Issues of cyber supply chain security in Korea. *Technovation*, *34*(7), pp.387-388.

Kivunja, C. and Kuyini, A.B., (2017) Understanding and applying research paradigms in educational contexts. *International Journal of higher education*, *6*(5), pp.26-41.

Khan O, Christopher M and Creazza A (2012), "Aligning Product Design with the Supply Chain: A Case Study Supply Chain Management: An International Journal, Vol. 17, No. 3, pp. 323-336

Kline, P., (2014) *An easy guide to factor analysis*. Routledge Koh, K., Ruighaver, A.B., Maynard, S.B. and Ahmad, A., (2005) Security governance: Its impact on security culture.

Knapp, K.J., Marshall, T.E., Kelly Rainer, R. and Nelson Ford, F., (2006) Information security: management's effect on culture and policy. *Information Management & Computer Security*, *14*(1), pp.24-36.

Koohang, A., Anderson, J., Nord, J.H. and Paliszkiewicz, J., (2020) Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*.Kshetri, N., (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications policy*, *41*(10), pp.1027-1038.

Kraemer, S. and Carayon, P., (2007) Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, *38*(2), pp.143-154.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security, 27*(5/6), 224- 231.

Kun, A.I., (2020) Qualitative methods in HRM research: they can offer more than an escape route from statistics…. *Metszetek-Társadalomtudományi folyóirat*, *9*(1), pp.91-96.

Kuvaas, B., Buch, R., Gagne, M., Dysvik, A. and Forest, J., (2016) Do you get what you pay for? Sales incentives and implications for motivation and changes in turnover intention and work effort. *Motivation and Emotion*, *40*, pp.667-680.

Kuypers, M.A., Heon, G., Martin, P., Smith, J., Ward, K. and Paté-Cornell, E., (2014) Cyber security: the Risk of Supply Chain Vulnerabilities in an Enterprise Firewall. In *Proceedings of the probabilistic safety assessment and management, PSAM 12*.

Kumar, A., 2019. Exploring young adults'e-waste recycling behaviour using an extended theory of planned behaviour model: A cross-cultural study. *Resources, Conservation and Recycling*, *141*, pp.378-389.

Kumar Mangla S. and Luthra, S., (2018) Evaluating challenges to Industry 4.0 initiatives for supply chain sustainability in emerging economies.

Kunnathur, A. S., & Vaithianathan, S. (2008). Information security issues in global supply chain. *Proceedings at the IMR Conference 2008*.

Kwon, J., Ulmer, J. R., & Wang, T. (2012). The association between top management involvement and compensation and information security breaches. Journal of Information Systems. Vol 27 (1).

Kyriazos, T.A., 2018. Applied psychometrics: sample size and sample power considerations in factor analysis (EFA, CFA) and SEM in general. *Psychology*, *9*(08), p.2207.

La Barbera, F. and Ajzen, I., (2020) Control interactions in the theory of planned behavior: Rethinking the role of subjective norm. *Europe's Journal of Psychology*, *16*(3), p.401.

Lambert, D.M. and Enz, M.G., (2017) Issues in supply chain management: Progress and potential. *Industrial Marketing Management*, *62*, pp.1-16.

Lanzini, P. and Thøgersen, J., (2014) Behavioural spillover in the environmental domain: An intervention study. *Journal of Environmental Psychology*, *40*, pp.381-390.

Lauren, N., Fielding, K.S., Smith, L. and Louis, W.R., (2016) You did, so you can and you will: Self-efficacy as a mediator of spillover from easy to more difficult pro-environmental behaviour. *Journal of environmental psychology*, *48*, pp.191-199.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and H. Breitner, M., (2014) Information security awareness and behavior: a theory-based literature review. *Management Research Review*, *37*(12), pp.1049-1092.

Lee, Y. and Larsen, K.R., (2009) Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), pp.177-187.

Leech, N.L. and Onwuegbuzie, A.J., (2009) A typology of mixed methods research designs. *Quality & quantity*, *43*, pp.265-275.

Leering, A., van de Wijngaert, L. and Nikou, S., 2022. More honour'd in the breach: predicting non-compliant behaviour through individual, situational and habitual factors. *Behaviour & Information Technology*, *41*(3), pp.519-534.

Lehoux, N., D'Amours, S. and Langevin, A., (2014) Inter-firm collaborations and supply chain coordination: review of key elements and case study. Production Planning & Control, 25(10), pp.858-872.

Leonard, M., Graham, S. and Bonacum, D., (2004) The human factor: the critical importance of effective teamwork and communication in providing safe care. *BMJ Quality & Safety*, *13*(suppl 1), pp.i85-i90.

Liezel Cilliers (2020) Wearable devices in healthcare: Privacy and information security issues. Health Information Management Journal 49 (2-3).

Li, Y. and Xu, L., (2021) Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *International Journal of Production Research*, *59*(4), pp.1216-1238.

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. Proceedings of the 7th Australian Information Security Management Conference.

Little, R.J. and Rubin, D.B., 2019. *Statistical analysis with missing data* (Vol. 793). John Wiley & Sons.

Long, H., (2014) An empirical review of research methodologies and methods in creativity studies (2003–2012). *Creativity Research Journal*, *26*(4), pp.427-438.

Long, K.L., Chao, L.L., Kazama, Y., An, A., Hu, K.Y., Peretz, L., Muller, D.C., Roan, V.D., Misra, R., Toth, C.E. and Breton, J.M., (2021) Regional gray matter oligodendrocyte-and myelin-related measures are associated with differential susceptibility to stress-induced behavior in rats and humans. *Translational psychiatry*, *11*(1), p.631.

Lumley, T., Diehr, P., Emerson, S. and Chen, L., 2002. The importance of the normality assumption in large public health data sets. *Annual review of public health*, *23*(1), pp.151-169.

Lysne, O., Hole, K.J., Otterstad, C., Ytrehus, Ø., Aarseth, R. and Tellnes, J., (2016) Vendor malware: detection limits and mitigation. *Computer*, *49*(8), pp.62-69.

Ma, C., Xia, Y., Yang, Q. and Zhao, Y., (2019) The contribution of macrophages to systemic lupus erythematosus. *Clinical Immunology*, *207*, pp.1-9.

Magnusson, E. and Marecek, J. (2015) Doing Interview-Based Qualitative Research: A Learner's Guide.: Cambridge University Press

Mahieu, R., van Eck, N. J., van Putten, D., & van den Hoven, J. (2018). From dignity to security protocols: A scientometric analysis of digital ethics. Ethics and Information Technology, 20,175-187.

Mahmoud Moussa (2015) Monitoring Employee Behaviour Through the use of technology and issues of the employee. Privacy in America. SAGE

Mamonov, S., and Benbunan-Fich, R. (2018) "The Impact of Information Security Threat Awareness on Privacy-Protective Behaviours," Computers in Human Behaviour (83), pp 3244.

Ma, Q., Johnston, A.C. and Pearson, J.M., (2008) Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*, *16*(3), pp.251

Malterud, K., Siersma, V. D. and Guassora, A. D. (2016) 'Sample Size in Qualitative Interview Studies: Guided by Information Power'. Qualitative health research, 26 (13), 1753-1760

Marucheck A, Greiss N, Mena C and Cai L (2011) Product Safety and Security in the Global Supply Chain: Issues, Challenges, and Research Opportunities", Journal of Operations Management, Vol. 29, pp. 707-720

Maskey, R., Fei, J. and Nguyen, H.O., (2020) Critical factors affecting information sharing in supply chains. *Production Planning & Control*, *31*(7), pp.557-574.

Maskey, R., Fei, and Nguyen, H.O., (2017) Exploratory factor analysis-antecedents of information sharing in supply chains. In *IAME2017* (Vol. 2017, pp. 1-25).

Masvosvere, D.J.E. and Venter, H.S., (2016) Using a standard approach to the design of next generation e-Supply Chain Digital Forensic Readiness systems. *SAIEE Africa Research Journal*, *107*(2), pp.104-120.

May, T. and Perry, B., (2022) *Social research: Issues, methods and process*. McGraw-Hill Education (UK).

McFadden, F.E. and Arnold, R.D., (2010), November. Supply chain risk mitigation for IT electronics. In *2010 IEEE International Conference on Technologies for Homeland Security (HST)* (pp. 49-55). IEEE.

Mentzer, J.T., Min, S. and Zacharia, Z.G., (2000) The nature of interfirm partnering in supply chain management. Journal of retailing, 76(4), pp.549-568.

Merhi, M.I. and Ahluwalia, P., (2019) Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior*, *92*, pp.37-46.

Mertens, D.M., (2019) Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods. Sage publications.

Mesch, G.S., (2009) Social bonds and Internet pornographic exposure among adolescents. *Journal of Adolescence*, *32*(3), pp.601-618.

Metawa, N., Hassan, M.K., Metawa, S. and Safa, M.F., (2019) Impact of behavioral factors on investors' financial decisions: case of the Egyptian stock market. *International Journal of Islamic and Middle Eastern Finance and Management*, *12*(1), pp.30-55.

Metalidou E.C. Marinagi, P Trivellas, N. Eberhagen, C Skourlas and G. Giannakopoulos (2014) The Human Factor of information security: unintentional Damage perspectives. Procedia-Social and Behaviour Science 147:424-428

Mileski, J., Clott, C. and Galvao, C.B., (2018) Cyberattacks on ships: a wicked problem approach. *Maritime Business Review*.

Mishra, P., Pandey, C.M., Singh, U., Gupta, A., Sahu, C. and Keshri, A., 2019. Descriptive statistics and normality tests for statistical data. *Annals of cardiac anaesthesia*, *22*(1), p.67.

Modi, S.B., Wiles, M.A. and Mishra, S., (2015) Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management*, *35*, pp.21-39.

Moeller, J.D., Culler, E.D., Hamilton, M.D., Aronson, K.R. and Perkins, D.F., (2015) The effects of military-connected parental absence on the behavioural and academic functioning of children: A literature review. *Journal of Children's Services*.

Mohammed, I., Nauman, A., Paul, P., Ganesan, S., Chen, K.H., Jalil, S.M.S., Jaouni, S.H., Kawas, H., Khan, W.A., Vattoth, A.L. and Al-Hashimi, Y.A., (2022) The efficacy and effectiveness of the COVID-19 vaccines in reducing infection, severity, hospitalization, and mortality: A systematic review. *Human vaccines & immunotherapeutics*, *18*(1), p.2027160.

Moher, D. Liberati A, Tetzlaff J, Altman DG, PRISMA Group (2009) Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Annals of internal medicine* 151(4), pp 264-269

Moletsane, T. and Tsibolane, P., (2020), March. Mobile information security awareness among students in higher education: An exploratory study. In *2020 conference on information communications technology and society (ICTAS)* (pp. 1-6). IEEE.

Molina-Azorín, J.F Fàbregues, S., (2017) Addressing quality in mixed methods research: A review and recommendations for a future agenda. *Quality & Quantity*, *51*, pp.2847-2863.

Mondal, S., Wijewardena, K.P., Karuppuswami, S., Kriti, N., Kumar, D. and Chahal, P., (2019) Blockchain inspired RFID-based information architecture for food supply chain. *IEEE Internet of Things Journal*, *6*(3), pp.5803-5813.

Moody, G.D., Siponen, M. and Pahnila, S., (2018) Toward a unified model of information security policy compliance. *MIS quarterly*, *42*(1).

Mouna Jouinia,, Latifa Ben Arfa Rabaia, Anis Ben Aissab (2014) *Classification of security threats in information systems*. Procedia Computer Science 32

Moussa, M., 2015. Monitoring employee behavior through the use of technology and issues of employee privacy in America. *Sage Open*, *5*(2), p.2158244015580168.

Mustafa Kamal, M. and Irani, Z., (2014) Analysing supply chain integration through a systematic literature review: a normative perspective. *Supply Chain Management: An International Journal*, *19*(5/6), pp.523-557.

Mustafa, M., Alshare, M., Bhargava, D., Neware, R., Singh, B. and Ngulube, P., (2022) Perceived security risk based on moderating factors for blockchain technology applications in cloud storage to achieve secure healthcare systems. *Computational and mathematical methods in medicine*, *2022*.

Mwagwabi, F., McGill, T., and Dixon, M. 2018. "Short-Term and Long-Term Effects of Fear Appeals in Improving Compliance with Password Guidelines," Communications of the Association for Information Systems (41:1), pp Article 7 (147-182).

Nader Sohrabi Safa, Carsten Maple, Steve Furnell, Muhammad Ajimal Azad, Charith Perera, Mohammad Dabbagh, Mehdi Sookhak (2019) *Deterrence and prevention-based model to mitigate information security insiders' threats in organizations*. Future Generation Computer Systems.

Nader Sohrabi Safa, Mehdi Sookkak, Rossauw Von Solms, Steven Furnell, Norjihan Abdul Ghani, Tutut Herawan (2015) *Information security conscious care behaviour formation in organizations.* Computers & Security.

Nagurney, A., Daniele, P. and Shukla, S., (2017) A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints. *Annals of operations research*, *248*, pp.405-427.

Ndanusa, H.S. and Daniel, C.O., (2019) Effect of Supplier Development on Operational Performance of Manufacturing Firms in Nigeria.

Nel, F. and Drevin, L. (2019) Key elements of an information security culture in organisations. Information & Computer Security, 27(2), pp 146-164.

Nitzl, C., (2016) The use of partial least squares structural equation modelling (PLS-SEM) in management accounting research: Directions for future theory development. *Journal of Accounting Literature*.

Njilla, L.L., (2020), April. A zero-sum game theoretic approach for mitigating counterfeit integrated circuits in supply chain. In *Disruptive Technologies in Information Sciences IV* (Vol. 11419, pp. 46-53). SPIE.

Noble, H. and Heale, R., 2019. Triangulation in research, with examples. *Evidence-based nursing*, *22*(3), pp.67-68.

Nørfeldt, L., Bøtker, J., Edinger, M., Genina, N. and Rantanen, J., (2019) Cryptopharmaceuticals: increasing the safety of medication by a blockchain of pharmaceutical products. *Journal of pharmaceutical sciences*, *108*(9), pp.2838-2841.

Nunnally, J. C. (1978). Psychometric Theory, McGraw-Hill, New York.

Oforji, J.C., Udensi, E.J. and Ibegbu, K.C., (2017) Cybersecurity challenges in Nigeria: The way forward. *SosPoly Journal of Science and Agriculture*, *2*, pp.1-5.

Olasanmi, O.O., (2019) Online shopping and customers' satisfaction in Lagos State, Nigeria. *American Journal of Industrial and Business Management*, *9*(06), p.1446.

Okdinawati, Liane, Togar M. Simatupang, and Yos Sunitiyoso. (2015)"Modelling collaborative transportation management: Current state and opportunities for future research." Journal of Operations and Supply Chain Management (JOSCM) 8, no. 2 : 96-119.

Okolo, N.B., (2016) Evaluating Factors of Security Policy on Information Security Effectiveness in Developing Nations: A Case of Nigeria. Northcentral University.

Ologbo, A.C., Oluwatosin, O.S. and Okyere-Kwakye, E., (2012) Strategic management theories and the linkage with firm competitive advantage from the human resource-based view. *International Journal of Research in Management & Technology*, *2*(4), pp.366-376.

Olasanmi, O. O. (2019) 'Online Shopping and Customers' Satisfaction in Lagos State, Nigeria'. American Journal of Industrial and Business Management, 9 (06), 1446

Onwuegbuzie, A.J. and Leech, N.L., (2004) Enhancing the interpretation of "significant" findings: The role of mixed methods research. *The qualitative report*, *9*(4), pp.770-792.

Onwuegbuzie, A.J., Johnson, R.B. and Collins, K.M., (2009) Call for mixed analysis: A philosophical framework for combining qualitative and quantitative approaches. *International journal of multiple research approaches*, *3*(2), pp.114-139

Oke A and Gopalakrishan M (2009) Managing Disruptions in Supply Chains: A Case Study of a Retail Supply Chain, International Journal of Production Economics, Vol. 118, pp. 168-174.

Osho, O. and Onoja, A.D., (2015) National cyber security policy and strategy of Nigeria: a qualitative analysis. *International Journal of Cyber Criminology*, *9*(1), p.120.

Ouyang, Y. and Li, X., (2010) The bullwhip effect in supply chain networks. *European Journal of Operational Research*, *201*(3), pp.799-810.

Padayachee K. (2013) A conceptual opportunity-based framework to mitigate the insider threat. Paper presented at the information Security for south African 14-16

Pahnila, S., Siponen, M. and Mahmood, A., (2007) Which factors explain employees' adherence to information security policies? An empirical study.

Pallant, J., (2020) SPSS survival manual: A step by step guide to data analysis using IBM SPSS. McGraw-hill education (UK).

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A, & Zwaan, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & Security, 42, 165-176.

Parush A, Parush D, Ilan R (2017). Human factors in healthcare: a field guide to continuous improvement. Morgan & Claypool.

Passafaro, P., (2020) Attitudes and tourists' sustainable behavior: An overview of the literature and discussion of some theoretical and methodological issues. *Journal of Travel Research*, *59*(4), pp.579-601.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., and Calic, D. (2015). "Factors that Influence Information Security Behaviours: An Australian Web-Based Study," in: Proceedings of the International Conference on Human Aspects of Information Security, Privacy, and Trust. Cham: Springer, pp. 231-241.

Paul, J., Lim, W.M. O'Cass, Andy Wei Hao and Stefeno Bresciani (2021) "Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). International Journal of Consumer Studies, 45(4), 01-016.

Payne, A.A., (2008) A multilevel analysis of the relationships among communal school organization, student bonding, and delinquency. *Journal of Research in Crime and Delinquency*, *45*(4), pp.429-455.

Peguero, A.A., Popp, A.M., Latimore, T.L., Shekarkhar, Z. and Koo, D.J., (2011) Social control theory and school misbehavior: Examining the role of race and ethnicity. *Youth violence and juvenile justice*, *9*(3), pp.259-275.

Peng, D.X. and Lai, F.,(2012) Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of operations management*, *30*(6), pp.467-480.

Peng, J., Li, M., Wang, Z. and Lin, Y., 2021. Transformational leadership and employees' reactions to organizational change: evidence from a meta-analysis. *The Journal of applied behavioral science*, *57*(3), pp.369-397.

Peterson, M., (2014) Identification of Behavioral Factors within Organizations that Can Improve Information Systems Security Compliance.

Pereira, T., Barreto, L. and Amaral, A., (2017) Network and information security challenges within Industry 4.0 paradigm. *Procedia manufacturing*, *13*, pp.1253-1260.

Pfleeger, S.L. and Caputo, D.D., (2012) Leveraging behavioral science to mitigate cyber security risk. *Computers & security*, *31*(4), pp.597-611.

Pfleeger, C.P., Pfleeger, S.L. (2007), Security in Computing, 4th Ed, Prentice Hall, New Jersey.

Pham, H., Brennan, L. and Richardson, J., (2017), June. Review of behavioural theories in security compliance and research challenge. In *Informing Science and Information Technology Education Conference, Vietnam* (pp. 65-76). Santa Rosa, CA: Informing Science Institute.

PN, S., (2021) The impact of information security initiatives on supply chain robustness and performance: an empirical study. *Information & Computer Security*, *29*(2), pp.365-391.

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

Polatidis, N., Pimenidis, E., Pavlidis, M. and Mouratidis, H., (2017) Recommender systems meeting security: From product recommendation to cyber-attack prediction. In *Engineering Applications of Neural Networks: 18th International Conference, EANN 2017, Athens, Greece, August 25–27, 2017, Proceedings* (pp. 508-519). Springer International Publishing.

Ponemon Institute LLC (2017). Exposing cybersecurity cracks: A global perspective. Ponemon Institute LLC.

Posey, C., Roberts, T.L. and Lowry, P.B., (2015) The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), pp.179-214.

Pratt, M.G., Rockmann, K.W. and Kaufmann, J.B., (2006) Constructing professional identity: The role of work and identity learning cycles in the customization of identity among medical residents. *Academy of management journal*, *49*(2), pp.235-262.

PricewaterhouseCoopers (2017). The global state of information security survey. Retrieved from www.pwc.com/us/en/cybersecurity/information-security-survey.html

(Price Waterhouse Coopers PWC, "Managing insider threats," 2014.

Princely Ifinedo (2012*) Understanding information system security policy Compliance*: *An integration of theory of planned behaviour protection motivation theory*. Journal of Computer and Science

Preuveneers, D., Joosen, W. and Ilie-Zudor, E., (2017) Trustworthy data-driven networked production for customer-centric plants. *Industrial Management & Data Systems*.

Puhakainen, P. and Siponen, M., (2010) Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, pp.757-778.

Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*," Decis. Sci., vol. 43, no. 4, pp. 615–660, 2012.

Quey Jen Yeh and Arthur Jung -Ting Chang (2007) *Threat and measures for information system security: A cross-industry stud*. Journal of information and management.

Rajivan, P., Moriano, P., Kelley, T., and Camp, L.J. (2017) "Factors in an End User Security Expertise Instrument," Information & Computer Security (25:2), pp 190-205.

Ralston, P., Richey, R.G. and J. Grawe, S., (2017) The past and future of supply chain collaboration: a literature synthesis and call for research. The International Journal of Logistics Management, 28(2), pp.508-530.

Ramesh, T., (2014), Security and trust-new challenges to computing today in cyberspace. In *2014 Seventh International Conference on Contemporary Computing (IC3)* (pp. 1-6). IEEE.

Rasoolimanesh, S.M. and Ali, F., (2018) Partial least squares-structural equation modeling in hospitality and tourism. *Journal of Hospitality and Tourism Technology*, *9*(3), pp.238-248.

Raweewan, M. and Ferrell Jr, W.G., (2018) Information sharing in supply chain collaboration. Computers & Industrial Engineering, 126, pp.269-281.

Rayna, T., & Striukova, L. (xxxx). Privacy or piracy, why choose? Two solutions to the issues of digital rights management and the protection of personal information. International Journal of Intellectual Property Management, X(Y), 000-000.

Reyes, P.M. and Jaska, P., (2007) Is RFID right for your organization or application?. *Management Research News*, *30*(8), pp.570-580.

Rhee, H.S., Kim, C. and Ryu, Y.U., (2009) Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & security*, *28*(8), pp.816-826.

Rigdon, E.E., 2016. Choosing PLS path modeling as analytical method in European management research: A realist perspective. *European Management Journal*, *34*(6), pp.598-605.

Ringle, C.M., Sarstedt, M., Mitchell, R. and Gudergan, S.P., (2020) Partial least squares structural equation modeling in HRM research. *The International Journal of Human Resource Management*, *31*(12), pp.1617-1643.

Rocco, T.S.R.T.S., Bliss, L.A.B.L.A., Gallagher, S.G.S., Pérez, A.P.A. and Prado, P., (2003) Taking the next step: Mixed methods taking the next step: Mixed methods research in organizational systems research in organizational systems. *Information technology, learning, and performance journal*, *21*(1), p.19.

Rocha Flores, W., Antonsen, E., and Ekstedt, M. (2014) "Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture," Computers & Security (43), pp 90-110.

Rönkkö, M., McIntosh, C.N. and Antonakis, J., 2015. On the adoption of partial least squares in psychological research: Caveat emptor. *Personality and Individual Differences*, *87*, pp.76-84.

Rooney, J. and Cuganesan, S., (2015) Leadership, governance and the mitigation of risk: a case study. *Managerial Auditing Journal*.

Rue, R., Pfleeger, S.L. and Ortiz, D., (2007), June. A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. In WEIS.

Rushton, A., Croucher, P. and Baker, P., (2022) The handbook of logistics and distribution management: Understanding the supply chain. Kogan Page Publishers.

Safa, N.S. and Von Solms, R., (2016) An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, pp.442-451.

Safa, N.S., Maple, C., Watson, T. and Von Solms, R., (2018) Motivation and opportunity-based model to reduce information security insider threats in organisations. *Journal of information security and applications*, *40*, pp.247-257.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T., (2015) Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, pp.65-78.

Safa, N.S., Von Solms, R. and Furnell, S., (2016) Information security policy compliance model in organizations. *computers & security*, *56*, pp.70-82.

Sai Suraj, B.V., Sharma, S.K. and Routroy, S., 2016. Positioning of Inventory in Supply Chain Using Simulation Modeling. *IUP Journal of Supply Chain Management*, *13*(2).

Sahin, F. and Robinson, E.P., (2002) Flow coordination and information sharing in supply chains: review, implications, and directions for future research. Decision sciences, 33(4), pp.505-536

Sahin, M.D. and Öztürk, G., (2019) Mixed Method Research: Theoretical Foundations, Designs and Its Use in Educational Research. *International Journal of Contemporary Educational Research*, *6*(2), pp.301-310.

Sarstedt, M., Hair, J.F., Ringle, C.M., Thiele, K.O. and Gudergan, S.P., (2016) Estimation issues with PLS and CBSEM: Where the bias lies!. *Journal of business research*, *69*(10), pp.3998-4010.

Saunders, B., Kitzinger, J. and Kitzinger, C., (2015) Anonymising interview data: Challenges and compromise in practice. *Qualitative research*, *15*(5), pp.616-632.

Saunders, C.S Pearlson, K.E.,. and Galletta, D.F., (2016) *Managing and using information systems: A strategic approach*. John Wiley & Sons.

Saunders, M., Lewis, P. and Thornhill, A., (2009) *Research methods for business students*. Pearson education.

Saunders, Pearlson, K.E., C.S. and Galletta, D.F., (2019) *Managing and using information systems: A strategic approach*. John Wiley & Sons.

Sarka, K.R. (2010) Assessing insider threats to information security using technical, behavioural and organisational measures. *Information security technical reports,* 15(3), pp.112-133

Schorsch, T., Wallenburg, C.M. and Wieland, A.,(2017) The human factor in SCM: Introducing a meta-theory of behavioral supply chain management. *International Journal of Physical Distribution & Logistics Management*, *47*(4), pp.238-262.

Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. South African Computer Journal, 31, 46-52.

Seazzu, A. and Burd, S., (2011) Social engineering: The neglected human factor for information security management. *Information Resources Management Journal (IRMJ)*, *24*(3), pp.1-8.

Sekaran, U. and Bougie, R., (2016) Research methods for business: A skill building approach. john wiley & sons.

Selvi, A.F., 2019. Qualitative content analysis. In *The Routledge handbook of research methods in applied linguistics* (pp. 440-452). Routledge.

Skotnes, R. O (2015) "Management commitment and awareness creation – ICT safety and security in electric power supply network companies", Information & Computer Security, Vol. 23 Issue: 3, pp.302-316, https://doi.org/10.1108/ICS-02-2014-0017

Sharma, S.K. and Vasant, B.S., (2015) Developing a framework for analyzing global supply chain security. *IUP Journal of Supply Chain Management*, *12*(3), p.7.

Shropshire, J., Warkentin, M. and Sharma, S., (2015) Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *computers & security*, *49*, pp.177-191.

Simon, J. and Omar, A., (2020) Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*(1), pp.161-171.

Sindhuja, K. and Devi, S.P., (2014) A symmetric key encryption technique using genetic algorithm. International journal of computer science and information technologies, 5(1), pp.414-416.

Sindhuja. PN (2021) The impact of information security initiatives on supply chain robustness and performance: an empirical study. *Information & Computer Security*, *29*(2), 365-391.

Singh, B., 2010, December. Network security and management. In (2010) IEEE International Conference on Computational Intelligence and Computing Research (pp. 1-6). IEEE.

Siponen, M., Mahmood, M.A. and Pahnila, S., (2014) Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), pp.217-224.

Siponen m, Vance A (2010). Neutralization: new insights into the problem of employee systems security policy violations MIS Q 34 (3) 487 – 502

Skotnes, R.Ø. and Engen, O.A., (2015) Attitudes toward risk regulation–Prescriptive or functional regulation. *Safety Science*, *77*, pp.10-18.

Smith, H.J., Dinev, T. and Xu, H., (2011) Information privacy research: an interdisciplinary review. *MIS quarterly*, pp.989-1015.

Snyman, D.P. and Kruger, H., (2021) Collective information security behaviour: a technology-driven framework. *Information & Computer Security*, *29*(4), pp.589-603.

Snyman, D. and Kruger, H., (2017) The application of behavioural thresholds to analyse collective behaviour in information security. *Information & Computer Security*.

Sodhi, M.S., Son, B.G. and Tang, C.S., (2012) Researchers' perspectives on supply chain risk management. *Production and operations management*, *21*(1), pp.1-13.

Son, J.Y., (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, *48*(7), pp.296-302.

Son, J.Y. and Rhee, H.S., 2007. Out of fear or desire: Why do Employees follow information systems security policies?. *AMCIS 2007 Proceedings*, p.268.

Soomro, Z.A., Shah, M.H. and Ahmed, J., (2016) Information security management needs more holistic approach: A literature review. *International journal of information management*, *36*(2), pp.215-225.

Sosik, J.J., Kahai, S.S. and Piovoso, M.J., (2009) Silver bullet or voodoo statistics? A primer for using the partial least squares data analytic technique in group and organization research. *Group & Organization Management*, *34*(1), pp.5-36.

Spanos, G. and Angelis, L., (2016) The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, pp.216-229.

Spears, J.L. and Barki, H., (2010) User participation in information systems security risk management. *MIS quarterly*, pp.503-522.

Stake, R.E., (2008). Qualitative case studies

Stallings, W. (2007) Network Security Essentials: Applications and Satandards, 3rd Ed, Prentice Hall, New Jersey

Straub Jr, D.W. and Collins, R.W., (1990) Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *Mis Quarterly*, pp.143-156.

Štemberger, M.I., Manfreda, A. and Kovačič, A., (2011) Achieving top management support with business knowledge and role of IT/IS personnel. *International Journal of Information Management*, *31*(5), pp.428-436.

Stevens, M., MacDuffie, J.P. and Helper, S., (2015) Reorienting and recalibrating inter-organizational relationships: Strategies for achieving optimal trust. *Organization Studies*, *36*(9), pp.1237-1264.

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance, 6(2), 1-4. doi:10.17645/pag.v6i2.1569.

Sun, J.C., Yu, S., Lin, S.S.J., and Tseng, S. (2016) "The Mediating Effect of Anti- phishing Self-efficacy Between College Students' Internet Self-efficacy and Anti-phishing Behaviours and Gender Difference," Computers in Human Behaviours (59), pp 249-257

Suresh Cuganesan, Cara Steeleb and Alison Hart (2018) *How senior management and workplace norms influence information security attitudes and self-efficacy. Journal of Behaviour &* Information Technology, VOL. 37, NO. 1, 50–65

Susanto, H., Almunawar, M.N. and Tuan, Y.C., (2011) Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), pp.23-29.

Sutduean, J., Singsa, A., Sriyakul, T. and Jermsittiparsert, K., (2019) Supply chain integration, enterprise resource planning, and organizational performance: The enterprise resource planning implementation approach. *Journal of Computational and Theoretical Nanoscience*, *16*(7), pp.2975-2981.

Tabachnick, B.G., Fidell, L.S. and Ullman, J.B., 2013. *Using multivariate statistics* (Vol. 6, pp. 497-516). Boston, MA: pearson.

Tamjidyamcholo, A., Baba, M.S.B., Tamjid, H. and Gholipour, R., (2013) Information security–Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education*, *68*, pp.223-232.

Tam, K.P., (2013) Concepts and measures related to connection to nature: Similarities and differences. *Journal of environmental psychology*, *34*, pp.64-78.

Tang, O. and Musa, S.N., (2011) Identifying risk issues and research advancements in supply chain risk management. *International journal of production economics*, *133*(1), pp.25-34.

Teddlie, C. and Tashakkori, A. (2009) Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences. Thousand Oaks, CA, SAGE Publications

Tashakkori, A. and Teddlie, C., (2003) Issues and dilemmas in teaching research methods courses in social and behavioural sciences: US perspective. *International journal of social research methodology*, *6*(1), pp.61-77.

Teddlie, C. and Yu, F., (2007) Mixed methods sampling: A typology with examples. *Journal of mixed methods research*, *1*(1), pp.77-100.

Tepe, R., & Tepe, C. (2015). Development and psychometric evaluation of an information literacy self-efficacy survey and an information literacy knowledge test. Journal of Chiropractic Education, 29(1), 11-15.

Thomas, S.P., Thomas, R.W., Manrodt, K.B. and Rutner, S.M., (2013) An experimental test of negotiation strategy effects on knowledge sharing intentions in buyer–supplier relationships. Journal of Supply Chain Management, 49(2), pp.96-113.

Tipton, H.F. and Krause, M., (2007) *Information security management handbook*. CRC press.

Trang, S. and Brendel, B., (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, *21*, pp.1265-1284.

Tsai, F.M., Bui, T.D., Tseng, M.L., Ali, M.H., Lim, M.K. and Chiu, A.S., (2021) Sustainable supply chain management trends in world regions: A data-driven analysis. *Resources, Conservation and Recycling*, *167*, p.105421.

Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J. and Cotten, S.R., (2016) Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, pp.138-150.

Tsohou, A., Karyda, M. and Kokolakis, S., (2015) Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & security*, *52*, pp.128-141.

Tuptuk, N. and Hailes, S., (2018) Security of smart manufacturing systems. *Journal of manufacturing systems*, *47*, pp.93-106.

Tu, Z. (2016) Information security management: A critical success factors analysis. [online] Doctoral thesis, McMaster University, Ontario

Queirós, A., Faria, D. and Almeida, F., (2017) Strengths and limitations of qualitative and quantitative research methods. *European journal of education studies*.

Uchenna Daniel Ani, Hongmei he, Ashutosh Tiwari, (2018) Human Factor Security; Evaluating the Cybersecurity Capacicity of the Industrial Workforce. Journal of systems and information Technology. Vol 33 (4) 360-376

Uffen, J. and Breitner, M.H., (2013) Management of technical security measures: An empirical examination of personality traits and behavioral intentions. *International Journal of Social and Organizational Dynamics in IT (IJSODIT)*, *3*(1), pp.14-31.

Urciuoli, L. Mannisto, T. Hintsa, J. and Khan, T. (2013). Supply chain cyber security-potential threats. Information & Security: An International Journals, 29(1).

Vance, A., Brinton A. B., Brock K. C., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: insights from electroencephalography (EEG). Journal of the Association for Information Systems, 15(10), 679-722.

Vance, A., Siponen, M. and Pahnila, S., (2012) Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), pp.190-198.

Venkatesh, V., Brown, S.A. and Bala, H., (2013) Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS quarterly*, pp.21-54.

Villena, V.H., Lu, G., Gomez-Mejia, L.R. and Revilla, E., 2018. Is top management team-supply chain manager interaction the missing link? An analysis of risk-bearing antecedents for supply chain managers. *International Journal of Operations & Production Management*, *38*(8), pp.1640-1663.

Von Solms, R. and Van Niekerk, J., (2013) From information security to cyber security.C*omputers & Security*, *38*, pp.97-102.

Wada, F. and Odulaja, G.O., (2012) Electronic banking and cyber crime in Nigeria-a theoretical policy perspective on causation. *Afr J Comp ICTs*, *5*(1), pp.69-82.

Warkentin, M., & Willison, R. (2009). Behavioral and Policy Issues in Information Systems Security: The Insider Threat. European Journal of Information Systems, 18(2), 101-105.

Warkentin, M., Bapna, R. and Sugumaran, V., (2000) The role of mass customization in enhancing supply chain relationships in B2C e-commerce markets. *J. Electron. Commer. Res.*, *1*(2), pp.45-52.

Wang, C.S. and Chen, C.Y., (2014) Developing supply chain strategies model for Taiwanese manufacturing companies. Journal of American Academy of Business, 19(2), pp.217-226.

Wang, H., Tsui, A.S. and Xin, K.R., (2011) CEO leadership behaviors, organizational performance, and employees' attitudes. *The leadership quarterly*, *22*(1), pp.92-105.

Wang, J., Muddada, R.R., Wang, H., Ding, J., Lin, Y., Liu, C. and Zhang, W., (2014) Toward a resilient holistic supply chain network system: Concept, review and future direction. *IEEE Systems Journal*, *10*(2), pp.410-421.

Wang, V., Nnaji, H. and Jung, J. (2020) 'Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability'. International Journal of Law, Crime and Justice, 62, 100415

Wang, P., D'Cruze, H., & Wood, D. (2019). Economic costs and impacts of business data breaches. Issues in Information Systems, 20(2), 162-171.

Wang, V., Nnaji, H. and Jung, J., (2020) Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, p.100415.

Wiengarten, Frank, Paul Humphreys, Guangming Cao, Brian Fynes, and Alan McKittrick. "Collaborative supply chain practices and performance: exploring the key role of information quality." Supply Chain Management: An International Journal 15, no. 6 (2010): 463-473

Williams, A.S., Maharaj, M.S. and Ojo, A.I., (2019) Employee behavioural factors and information security standard compliance in Nigeria banks. *International Journal of Computing and Digital Systems*, *8*(04), pp.387-396.

Willison, R. and Warkentin, M., (2013) Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, pp.1-20.

Whitman, M.E. and Mattord, H.J., (2012) Roadmap to information security: For IT and InfoSec managers. Cengage Learning.

Workman, M., Bommer, W.H. and Straub, D., (2008) Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behaviour*, *24*(6), pp.2799-2816.

Wu I L., Chuang, C- H, & (2014) Information sharing and collaborative behaviours in enabling supply chain performance: A social exchange perspective. International Journal of Production Economics 148122-132

Wu, F., Zhang, H., Wang, W., Jia, J., & Yuan, S. (2015). A new method to analyze the security of protocol implementations based on ideal trace. *Hindawi Security and Communication Networks*, DOI: https://doi.org/10.1155/2017/7042835

Xiao, Y. and Maria Watson (2019) Guidance on conducting a systematic literature review. *Journal of planning education and research*, 39(1), pp 93-112

Yang, T.-M. & Maxwell, T. A. (2011), "Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors", Government Information Quarterly, Vol. 28, No. 2, pp. 164-175.

Yeboah-Ofori, A., Islam, S. and Brimicombe, A., (2019), Detecting cyber supply chain attacks on cyber physical systems using bayesian belief network. In *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)* (pp. 37-42). IEEE.

Ye, Yuxiao, Mohammed Ali Suleiman, and Baofeng Huo. (2022) "Impact of just-in-time (JIT) on supply chain disruption risk: the moderating role of supply chain centralization." *Industrial Management & Data Systems* ahead-of-print

Yigitbasioglu, O.M., (2010) Information sharing with key suppliers: a transaction cost theory perspective. *International Journal of Physical Distribution & Logistics Management*.

Young, R.F. and Windsor, J., 2010. Empirical evaluation of information security planning and integration. *Communications of the Association for Information Systems*, *26*(1), p.13.

Yinka, A. M. (2011) Data and Information Security in a Security in a Global Age. Mediterranean Center of Social and Education Research, 2, p. 113

Yoon, C., Hwang, J.W. and Kim, R., (2012) Exploring factors that influence students' behaviors in information security. *Journal of information systems education*, *23*(4), pp.407-416.

Zhang, D., Dadkhah, P. and Ekwall, D., 2011. How robustness and resilience support security business against antagonistic threats in transport network. *Journal of transportation security*, *4*, pp.201-219.

Zhang, X. and Wang, H. (2011) Empirical research on associations among information technology, supply chain robustness and supply chain performance", International Journal of Business and Management, Vol. 6 No. 2, pp. 231-235.

Zhao, X., Xue, L. and Whinston A.B. (2013) Managing Interdependent Information Security Risks: Cyber insurance, Managed Security Security Services and Risk Pooling Arrangement.' *Journal of Management Information Systems*, 30(1), 123-152.

Zikmund, W.G., D'alessandro, S., Winzar, H., Lowe, B. and Babin, B., (2014) *Marketing research*. Sydney: Cengage Learning.

Zinn, S.E. (2013). The information literacy self-efficacy of disadvantaged teachers in South Africa. Communications in Computer and Information Science, Vol. 397 CCIS, pp. 212-218.

Appendix A: Participant information sheet

PARTICIPANT INFORMATION SHEET

PROJECT TITLE: Evaluating information security threats in the supply chain.

You are being invited to take part in research on Information security threats in the supply chain. Christiana Akintoye at Coventry University is leading this research. Before you decide to take part it is important you understand why the research is being conducted and what it will involve. Please take the time to read the following information carefully

1. Information about the project /Purpose of the project

The purpose of the research is to critically explore information security threats in the supply chain address issue of threats. More specifically, this research focused on employees, supply chain partners and customers attitudes towards mitigating information security threats in the supply chain.

2. What are the benefits of taking part?

The research will aid in greatly reducing the rate of information security threats in manufacturing sector of supply chain on the condition that full implementation of its provision is ensured. It will also greatly enhance process of information management. Minimized the risk of information security in the organization. Going forward, it will enhance the securing of information asset of different industries, fields and disciplines. Companies within the process industry will also have opportunity to incorporate a more holistic model into their management system and upon successful implementation, stand a great chance of increasing their operational reputations with regards to information security.

3. Data protection & confidentiality

All information provided to me **will be confidential** and used solely for purpose of this study. The data will be collected and stored in accordance with Data Protection Act 1998 and will be disposed in a secure manner. The information will be used in a way that will not allow you to be identified individually and the public or any

Appendix B: Survey questionnaire

Please, indicate your gender

- Male
- Female

Please, indicate your age range

- Less than 20
- 21-30
- 31-40
- 41-50
- 51-60
- 61 and above

Educational background

- Secondary School Certificate
- N.C.E
- Diploma or equivalent
- Bachelor's degree or equivalent
- Master's degree or equivalent
- Ph.D.

Position

- Junior Staff
- Senior Staff
- Management

Business sector:

- Manufacturing

Business sector:

- Manufacturing
- Logistics and transport
- Marketing and distribution
- Production and operation

Work experience

- 1 to 2 years
- 3 to 5 years
- Above 5 years

Number of employee

- 1 to 10
- 11 to 30
- 31 to 50
- 50 and above

Company Age

- Less than 10
- 10 - 20 years
- Above 20 years

Information Sharing Platform (ISP)

- Blog
- Email
- Twitter
- Instagram
- other company ISP

Click to write the question text

	Strongly agree	Agree	Neutral	Strongly disagree	Disagree
Threat to the information security of my company supply chain is severe	○	○	○	○	○
Threats to the information security of my company supply chain are harmless	○	○	○	○	○
My company involve our supply chain partners in identification and mitigation of potential supply chain threat	○	○	○	○	○
My company has processes in place to reduce information security threats in our supply chain	○	○	○	○	○
Active monitoring of information assets by my company reduces information security threats in the supply chain	○	○	○	○	○
My company has the technical and administrative controls to detect information security threats	○	○	○	○	○
My company involve our customers in identification and mitigation of supply chain threats	○	○	○	○	○

To what extent do you agree/disagree with the following statements?

	Strongly agree	Agree	Neutral	Strongly disagree	Disagree
Top management in my company is interested in information security threats in the supply chain	○	○	○	○	○
Evident support for information security goals by top management is clear	○	○	○	○	○
Top management considers information security in the supply chain an important organizational priority	○	○	○	○	○
Top management decision on supply chain information security is relevant to supply chain partners	○	○	○	○	○
Top management collaborate with supply chain partners to reduce information security threats	○	○	○	○	○
Top management's words and actions demonstrate that information management is a priority	○	○	○	○	○

To what extent do you agree/disagree with the following statements.

	Strongly agree	Agree	Neither agree nor disagree	Strongly disagree	Disagree
I am committed to safeguard organizational information asset	○	○	○	○	○
I invest my energy and effort to ensure my company information security threats are reduced.	○	○	○	○	○
I am committed to my company's concern about information security threats in the supply chain.	○	○	○	○	○
I am committed to avoiding any actions that jeopardize my company's information security	○	○	○	○	○
Employees of my company have a responsible disposition towards proper information security practices	○	○	○	○	○
Supply chain partners of my firm willingly spend time and effort to reduce information security threats	○	○	○	○	○

To what extent do you agree/disagree with the following statements?

	Strongly agree	Agree	Neutral	Strongly disagree	Disagree
My pay raises and/or promotions depend on whether I manage the supply chain information the way the company requires and /or expects me to	○	○	○	○	○
I will receive person mention if I manage supply chain information the way my company requires and/or expects me to	○	○	○	○	○
I will be given awards for managing supply chain information the way my company supply chain requires and/or expects me to do	○	○	○	○	○

To what extent do you agree/disagree with the following statements?

	Strongly agree	Agree	Neutral	Strongly disagree	Disagree
I will be punished if I manage my company supply chain information inappropriately	○	○	○	○	○
I will incur penalties if I fail to operate within stated information security parameters of the company	○	○	○	○	○
I think punishment will be severe if I sell or transfer supply chain information outside	○	○	○	○	○
There will be consequences if I violate the confidentiality of my company's supply chain information	○	○	○	○	○
My firm has defined consequences for supply chain partners who fail to comply with supply chain security procedures	○	○	○	○	○
I prefer not to disclose my company information asset to individuals or third-party companies (suppliers) due to the punishment or penalties that may follow	○	○	○	○	○

To what extent do you agree/disagree with the following statements?

	Strongly Agree	Agree	Neutral	Strongly Disagree	Disagree
My company uses security audits to determine if relationships should be maintained with supply chain partners	○	○	○	○	○
When it comes to information security in the supply chain, my company actively monitors the conduct of workers	○	○	○	○	○
The evaluation of information security behaviour of employees is a regular activity in my company	○	○	○	○	○
There are many information security tasks, activities and behaviours that are not monitored in my company's supply chain	○	○	○	○	○
The evaluation of information systems provides my company's supply chain partners with valid information they need to respond to information security threats	○	○	○	○	○
The monitoring of our information systems provides our supply chain partners with timely information they need to respond to information security threats	○	○	○	○	○
My company regularly monitors employee computing activities to see how well employees follow information management policies and procedures.	○	○	○	○	○
My firm uses security audits to determine if relationships should be maintained with customers	○	○	○	○	○

To what extent do you agree/disagree with the following statements?

	Strongly agree	Agree	Neutral	Strongly disagree	Disagree
My company expectations concerning the security of information influences the way my colleagues think I should handle my company information asset	○	○	○	○	○
Line managers believes that we should protect information assets of my company's supply chain	○	○	○	○	○
I am well in line with the expected processes preferred by my supervisors in security of information in this organisation	○	○	○	○	○
My friends in my office encourage me to have safe information security actions	○	○	○	○	○
My colleagues think that we should behave safely to protect the organizational security features	○	○	○	○	○

To what extent do you agree/disagree to the following statements?

	Strongly agree	Agree	Neutral	Strongly disagree	disagree
Safe information security actions expressed by the employees serve to preserve information assets in my company	○	○	○	○	○
Appropriate information security actions adopted by the employees help in mitigates the risk of information security threats in my company's supply chain	○	○	○	○	○
To me, securing information the way my company requires me to is valuable	○	○	○	○	○
Safe information security behaviour decreases information security threats in my company's supply chain	○	○	○	○	○

To what extent do you agree/disagree with the following statements?

	Strongly agree	Agree	Neutral	Strongly disagree	disagree
For me, securing supply chain information the way my company requires and expect me to is difficult	○	○	○	○	○
I have the expertise to protect my company business and private data	○	○	○	○	○
I have the necessary skills to secure information the way my company requires and expect me to	○	○	○	○	○
My company exchanges information with our trading partners electronically	○	○	○	○	○
I have the necessary knowledge to secure the supply chain information the way my company requires and expects me to do	○	○	○	○	○
My company's supply chain partners can provide actionable information needed to respond to information security threats	○	○	○	○	○
My company can ensure the security of information of supply chain partners in the supply chain	○	○	○	○	○

	Strongly agree	Agree	Neutral	Strongly disagree	Disagree
Threat to the information security of my company supply chain is severe	○	○	○	○	○
Threats to the information security of my company supply chain are harmless	○	○	○	○	○
My company involve our supply chain partners in identification and mitigation of potential supply chain threat	○	○	○	○	○
My company has processes in place to reduce information security threats in our supply chain	○	○	○	○	○
Active monitoring of information assets by my company reduces information security threats in the supply chain	○	○	○	○	○
My company has the technical and administrative controls to detect information security threats	○	○	○	○	○
My company involve our customers in identification and mitigation of supply chain threats	○	○	○	○	○

Appendix C: Semi-Structured Interview

Evaluating information security threats in the supply chain

Introduction (interviewer)

- On the research objectives
- Structure of the interview

Code Number: (P1,P2,P3,P4,P5,P6,P7,P8 and P9**)**

Date of the interview:

The total length of the interview: 30 minutes

Part A – **Demographic Questionnaire**

- Demographic
- Work details
- Experience
- What is your main business and how long have you been doing it?
- What is your position in the company and how long have you been in this position?
- How many employees do you have?

Part B: **Questionnaire**

Q1) Information security threats in the supply chain

- Now I would like to capture your view about information security threats in the supply chain. What does information security mean to you? How is it controlled in your company?
- Would you say that the information security problem in the supply chain of your company is severe or harmless? If yes, can you explain how, please?
- Do your company involve your supply chain partners in the identification and mitigation of potential supply chain threats?

Q2) Top management support

- In what ways does top management support information security?
- Do they consider it a priority in the organisation?
- What has top management done to express the importance of Information security?
- What has top management done to help mitigate information security threats in the supply chain?
- How did top management show their support to employees on information security?

Q3) Commitment

- How committed are you to safeguarding the organisational information asset?
- How committed are employees in this organization to safeguarding the organisational information asset?
- How has your level of commitment affected your attitude towards information security threats in the supply chain (organisation)
- Tell me some actions you have taken at work to meet a and c.

The first section included questions regarding the respondents 'background and the company's background. The second section had questions regarding the respondents' supply chain

Q4) Reward

- Do you receive a pay raise/promotion when you manage the supply chain the way the company require**?**
- Do you think the elimination of benefits, awards and people mentioned by companies can influence employees' attitudes towards information security? Why do you think so?

Q5) Sanctions

- What sorts of sanctions do you expect from the organisation? Would you continue to comply?
- What is your perception of the negative outcomes if you do not mitigate the organisation's information security threats in the supply chain?
- Would punishment or demotion deter you from information security misconduct? Why?
- Will the implementation of sanctions (punishment, demotion, suspension from duty) influence employee attitude toward reducing information security?

Q6) Monitoring/Evaluation

- How does your organisation monitor information security issues in the supply chain?
- How does your manager evaluate the information security behaviour of the employee?
- Does regular monitoring of information security behaviour by your organisation influence employee attitude? How?
- Does the regular evaluation of information security by your organisation prevent employee information security misconduct? How?

Q7) Attitudes

- How much value do you place on information security in your organization?
- Do you support the protection and safeguarding of information in your organization?

Q8) Subjective norms

- Do you agree with the overarching policies on information security?

Do top management, and your line manager's expectations influence your information security behaviour at work? Why?

Appendix D: List of companies

S/N	Companies	Specialization
1	KAM Industries (Nigeria) Limited	Spring and Wire product manufacturing, Metalworking machinery, Manufacturing foundries, Nails, steel or cut.
2	Dangote Cement PLC	Cement manufacturing, Automotive, Salt &Seasonings, Fertilizer, Tomatoes Paste, Sugar, Petrochemicals, Real Estate, Mining, Polysacks, Rice, and Energy.
3	Nigeria Bottling Company Limited	Producing and delivering quality soft drinks in Nigeria
4	Friesland Wamco Nigeria limited	Provide better nutrition for Nigeria (Milk and dairy)
5	Lafarge Africa Plc	Building for people and planet
6	Bua cement Plc	Manufacturing Of Cement
7	Ardova Plc	Operates in the downstream sector of Oil and gas, operating in aircraft refuelling
8	International Breweries PLC	Producer of Trophy, Hero, Castle lite, Eagle, Budweiser, beer.
9	Seven-Up Bottling Co. PLC	Manufacturing, producing and distributing loves beverages.
10	Guinness Nigeria	
11	Honeywell Flour Mills	Producing of wheatmeal, noodles, superfine flour, macaroni, composite
12	Eterna plc	Manufacturing and sales of lubricating and petrochemicals, importation and bulk/retail sale of petroleum products including PMS, AGO, Base Oils, bitumen, and export of lubricants/fuel.
13	Stallion Nigeria Limited	Manufacturing of food, plastic, auto assemble, steel and fish integration
14	Greenlife Pharmaceuticals limited	Manufacturing of anti- malarias, anti-infectives, anti-inflammatories, anti-helminthics, anti-hypentensive, laxatives and multivitamins
15	Elephant Group ltd	Produce rice, fertilizer, maize soya beans, sesame seed cassava, cocoa, crude oil,
16	Purechem Industries private limited	Manufactures cement and building product
17	Avon Crowncaps and containers Nigeria ltd	Produce food cans, aerosol cans, paints cans, pails, crowncaps, ropp closures, speciality containers
18	Vitafoam Nigeria Plc	Manufactures foam products
19	Afprints Nigeria Plc	Production of Apparel &Textile
20	Dansa food ltd	Production natural Fruit Juice, cotton, tomatoes paste, processed gum arabic
21	West Africa Seasoning Company	Manufactures Umami seasoning called Ajinomoto

22	Beta Glass	Manufacturing of Glass container, machinery, Equipment, and Supplies Merchant Wholesalers, Nonmetallic Mineral
23	Unique Pharmaceuticals limited	Pharmaceutical and medicine, manufacturing Chemical manufacturing, manufacturing of medicines, capsuled, ampule
24	Premier feed mills company limited	Manufactures of feeds
25	Cadbury Nigeria Plc	Manufacturing of Beverages, Biscuits and cookies, chocolate, gum and candy, meals
26	Kabelmetal Nigeria Plc	Manufacturing of advance cable
27	Pz Cussons Nigeria plc	Manufacturing of baby products
28	Golden Sugar company limited	Manufacturing of sugar and confectionery, food
29	Mandilas enterprises limited	
30	Chemstar paints industry Nigeria	Manufacturing of building paint, marine paints, wood finishes and automotive paint
31	Reliance chemical products	Manufacturing of chemical product, and preparation, allied product merchant
32	Somzel Agro enterprise	Produce tomato puree
33	Flour Mill	Produce flour
34	7up Bottling Company	Producing and distribution of beverages
35	GlaxoSmithKline	Manufacture vaccines and specialty medicines to prevent and treat disease
36	Lafarge Cement	Offer a wide variety of bulk and packed cementitious materials
37	Chi Farms	Processing of commercial broilers and breeding operations
38	Fan Milk	Manufacture and reltail of ice cream and frozen dairy products
39	Consolidated Breweries plc	Produces and markets alcoholic beverages
40	Nestle Nigeria	Manufacturing, marketing, and distribution of food products, including purified water throughout the country
41	Eleganza	Manufacturer of Plastics
42	Coca-Cola	Produce and Distribution of beverages
43	P&G	Manufacture of personal care and hygiene products
44	British American Tobacco	Manufacture and distribution cigarettes, tobacco and other nicotine products
45	May &Baker	Manufacture and distribute pharmaceutical products, such as vaccines, antibiotics, and sera
46	UAC	Manufacturing, services, logistics and warehousing, agricultural and real estate

47	Unilever Nigeria Plc	Manufacture and market consumer products primarily in the home, personal care and foods categories
48	Nigeria Breweries	The brewing, marketing, and selling of lager, stout, non-alcoholic malt drinks and soft drinks
49	Orange Drugs	Pharmaceuticals, Personal Care, Food and Beverage
50	Dansa	Manufacture and distribute a wide range of juices, nectars, soda, and water products
51	McNichols Consolidated Plc	Proccess food
52	Livestock Feeds Plc	Manufacturer and distributor of food
53	Nigerian National Petroleum Company Ltd	Oil corporation in Nigeria
54	Inlaks Power Solutions Limited	
55	Golden Guinea Breweries	Brewing, packaging, marketing, and distribution of lager beer, malta, and stout primarily in Nigeria
56	Swiss Pharma Nigeria Ltd	Manufactures, markets, and distributes pharmaceutical products
57	Flour Mills of Nigeria	They operate in four major sectors of Food, Su, Agro-allied, Port Operations and Logistics, Packaging and Real Estate
58	Nigerian Eagle Flour Mills Ltd	Manufacture and market Flour and allied products like Semolina and Bran.
59	Nestle Nigeria Plc	Manufacture, marketing, and distribution of food products, including purified water throughout the country
60	Nigerian Breweries Plc	Brewing, marketing, and selling of lager, stout, non-alcoholic malt drinks and soft drinks
61	Elsewedy Electric Nigerian Ltd	Manufactures and sells integrated energy products and services in seven energy segments
62	Vallourrec Nigeria Ltd	manufacturing and sales of tubes and connections suitable for oil and gas well equipment and machinery.
63	Frieslandcampina Wamco Ltd	keeps milk affordable in Nigeria, ensuring access to quality dairy, fortified with the required nutrients; educating consumers on how to make healthier choices and live an active lifestyle
64	Dangote Sugar Refinery	Refining and marketing of sugar
65	Ardova Plc	produces and distributes a wide range of high-quality lubricants brands to satisfy various automotive and industrial lubrication needs
66	Neimeth International Pharmaceuticals Plc	manufactures and markets a range of Pfizer pharmaceutical and animal health products in Nigeria

67	Bua Foods Plc	processes, manufactures, and distributes food produce such as a flour and pasta, sugar, refined oil, and rice.
68	Mamunda Industries Nigeria Ltd	Pop Cola Beverages, Sacks and Mats, Foods, Tanneries/Leather, and Power plant.
69	Chrisokeson International Ltd	Manufactures packaging bags and sacks
70	Dangote Agro Sacks Ltd	Manufactures packaging bags and sacks
71	Quaternary International Company Ltd	Environmental and laboratory services company
72	Crown Flour Mills Ltd	Wheat milling
73	Meyer Plc	Manufactures and markets paints.
74	Olam Nigeria Ltd	Operates the largest integrated animal feed, poultry breeding farm and day-old-chick facility in nigeria.
75	Innoson Vehicle Manufacturing Co. Ltd	Automobile manufacturer
76	DAG Industries Ltd (BAJAJ)	Authorized distributor and marketer of bajaj two-wheelers across nigeria
77	Hyundai Heavy Industries Company Ltd	Provides services through its subsidiaries in the heavy industry and energy sectors
78	The Nigerian Printing and Minting Plc	Manufacturing superior security documents and developing security solutions.
79	Viva Metal and Plastics Industries Ltd	Manufacturers and exporters of plastics and various polypropylene products.
80	JMG Ltd	Wholesale distribution of electrical apparatus and equipment wiring supplies.
81	Dangote Group	A Nigeria multinational industrial conglomerate,
82	TACNA Services	Helps companies manufacture in low cost low and cheap labour
83	DUFIL Prima Foods	Produces and distributes noodles.
84	Nexans Nigeria	Provides customers with advanced cable technologies for power and data transmission
85	United Africa Company of Nigeria	Manufacturing, services, logistics and warehousing, agricultural and real estate
86	BAGCO	A provider of total packaging solutions
87	Cejex Designs Ltd	Creating kitchens, bedroom sets, wall units and bathroom cabinetry for local clients and projects around the world
88	Comvicong Nigeria Company	Manufacturing polythene nylon and printing consumables in nigeria for industrial purposes and domestic uses

89	Daily – Need Industries	Manufacturer of pharmaceutical, food and personal care products
90	Eversharpmaster Idumota	Manufactures cutting discs for stones/wheels, metal grinding wheels, fibre discs and diamond blades for cutting materials.
91	Geotextile &Gabions Ltd	Improve soil strength at a lower cost than conventional soil nailing
92	Gmicord Industrial Group	Fabrication, cathodic/galvanic protection by film galvanizing technology and industrial inspection services
93	International Merchants Ltd	Leading manufacturer of customized furniture in Nigeria.
94	Jacob Wines Ltd	Wine manufacturer and a pioneer in pineapple wine technology in Africa
95	Jotna Nigeria Ltd	Manufacturing beverages &related packaging in Africa
96	Tranos	Nigeria's first indigenous manufacturers of high-quality electrical distribution systems for low and medium voltage apparatuses
97	Wichtech Industries Ltd	Supplier of quality roofing and plumbing systems
98	Zeenab Foods Ltd Lagos	Food processing and production company
99	Alumaco Plc	Manufactures a wide range of aluminum products for use in home, offices and infrastructure
100	Annuri International Ltd Factory	Design and produce timeless, durable and beautiful leather and textile soft goods such as diplomatic leather, royal leather, standard leather and presidential leather products
101	Association of Cottage Industries of Nigeria	solicit support to improve and promote Nigerian Made Products for home consumption and export
102	Clay Industry Nigeria Ltd	Manufacturer of clay bricks for partition walls, sun breakers, decking floor, load bearing walls and finishing
103	Kalek Fibre Company Nigeria Ltd	Fibre Glass Hair Wash Basin with marble effect of various colours and design.
104	NADMACO Ltd	Manufacture tablet drugs, capsules and liquid formulations.
105	Neat Zenith Ng Ltd	Tissue manufacturing, serviette, kitchen towels
106	Padson Industries Ltd	Assemblage and manufacturing
107	Reddi2wear	A leading manufacturer and suppliers of top-quality home textiles, decorative pillows, curtains, table mats etc.
108	TMC DÉCOR Company	Space control systems' design and production
109	Chi Ltd	An interior decoration, manufacturing
110	Boulos Enterprises	Distributor and trading company of motorcycles, power bikes, Cargo tricycles, Suzuki Super Carry Trucks and outboard motors in Nigeria.
111	Dignified Mobile Toilets	Reducing the public toilets deficit and improving sanitation

112	Eunisell	Supplying key products and solutions to a wide base of customers operating in Africa.
113	Promasidor Nigeria	The leading provider of high-quality food products across various regions in Africa
114	Ruff 'n' Tumble	Specializes in the manufacturing and retail of apparel, footwear and accessories for children from ages 0-16.
115	Vitafoam Nigeria Plc	Manufacturer of flexible, reconstituted and rigid foam products
116	Wemy Industries	Manufacturing and distribution of hygiene products
117	Engee Pet Manufacturing Company Nigeria Ltd	Manufacturer of the highest quality food-grade PET resin in West Africa
118	Legacy Sugar Company Nigeria Ltd	Producing sugar and ethanol
119	Geeta Plastic Products Ltd	Produces superior quality plastics, alongside providing customers with assistance and expertise on innovative designs, moulds, and labelling
120	Beloxxi Industries Ltd	Nigerian biscuit manufacturer
121	Nigerian Bag Manufacturing Company Ltd	Manufactures a wide range of woven polypropylene bags
122	May and Baker Plc	Manufacturers and distributes pharmaceutical products, such as vaccines, antibiotics, and sera.
123	Polystyrene Industries Ltd	Produce all types of moulded products
124	Sacvin Nigeria Limited	Provides plastic solutions for industrial and household use
125	Newpal Nig Ltd	Engineering services
126	Forza Nigeria Ltd	Providing fluid power, transfer and control services to clients across the energy and marine industry
127	Delta Shoes and Plastics Nigeria Ltd	Produce shoes and Plastics
128	Paptec Industries Limited	Pulp and Paper family, Printing, Packaging, Publishing and Chemical Suppliers
129	Dehero company	Produce all types of moulded products
130	Geokov Company Ltd	Manufacturing of cartons, Carton branding, perforated cartons and Corrugated cartons
131	Nadis Trading Company Nigeria	Manage existing power purchase agreements and new procurement of power in the electricity industry transition process.
132	Industrial Cartons Limited	Manufacturing of cartons, Carton branding, perforated cartons and Corrugated cartons

133	Deltaplast Company Nigeria Ltd	A complete service to the water, sewage, ducting and the construction industry
134	Horse Power Pharmaceutical Co. Ltd	Specializes on Pharmaceutical Products, Hospital Equipment and Laboratory Reagents
135	Cometstar Manufacturing Company Ltd.	Manufacturer of conduit, surface wiring cable, earthing copper conductor cables, PVC insulated, sheathed, non-armoured copper cables, PVC conduit boxes, pattress boxes and lattice copper earth plate
136	The Bosch Manufacturing Ltd	A sales, marketing and service office
137	Shemoma Nigeria Ltd Factory	Manufacturing construction products
138	Nunoka Nigeria Limited	A complete service to the water, sewage, ducting and the construction industry
139	O K Jazz Metal Company Ltd	Aluminium manufacturing
140	Klat Pharmaceutical Company Nigeria Ltd	Produce and supply antioxidant and immune-boosting supplement Vitamin E, capsules and zinc
141	Shekwo Agro Chemicals Nigeria Ltd	Produce and supply antioxidant and immune-boosting supplement Vitamin E, capsules and zinc
142	Marshal Paints and Chemical Industries Ltd Nigeria	Manufactures and supply exterior/interior floating materials, textured coating, emulsion and other types of industrial paints and chemicals.
143	Amswift Nigeria Ltd	Aluminium manufacturing
144	Girako Nigeria Enterprise	sales, marketing and service office
145	Fidson Healthcare Plc	Manufacturing and distribution of pharmaceutical products
146	Nemaco Global Resources Ltd	Manufacturers of UPVC, PVC Pipes, Conduit Pipes and Borehole Casin Pipes
147	Bennie Agro Ltd	A machine Design and Fabrication Company Leading in technological innovations
148	Diemco Nigeria Ltd	Information, business information, directors/partners and contact details.
149	Eajtech Energy Company Ltd	Sale and installment all types of solar panels, inverter, batteries and others
150	Harafoams and Chemicals Ltd	Manufacturing of mattress and flexible foam, furniture, beds and bedding products

CONSENT FORM

Evaluating information security threats in the Supply chain: Human Factor

You are invited to take part in the above research project for the purpose of collecting data on Information security threats in the supply chain.

Before you decide to take part, you must **read the accompanying Participant Information Sheet and Privacy Notice**

Researcher: Christiana Akintoye

Department: Strategy and Applied Management

Contact details: (*akintoyc@uni.coventry.ac.uk*)

Supervisor name: Dr. Muhammad Kamal

Supervisor contact details: Coventry University

This form is to confirm that you understand what the purposes of the research project are, what will be involved and that you agree to take part. If you are happy to participate, please initial each box to indicate your agreement, sign and date the form, and return to the researcher.

Please do not hesitate to ask questions if anything is unclear or if you would like more information about any aspect of this research. It is important that you feel able to take the necessary time to decide whether or not you wish to take part.

Appendix E: Participant consent form

1	**I confirm that I have read and understood the Participant Information Sheet for the above research project and have had the opportunity to ask questions.**	
2	**I understand that all the information I provide will be held securely and treated confidentially. I understand who access to any personal data will have provided and what will happened to the data at the end of the research project.**	
3	**I understand my participation is voluntary and that I am free to withdraw my participation and data, without giving a reason, by contacting the lead at any time until the date specified in the Participant Information Sheet.**	
4	**I understand the results of this research will be used in academic papers and other formal research outputs.**	
5	**I am happy for the interview to be audio/video recorded.**	
6	**I agree to take part in the above research project.**	

_____ _____ _____

Name of Participant **Signature** **Date**

_____ _____ _____

Name of Researcher **Signature** **Date**

Participant Information Sheet Evaluating information security threats in the supply chain: Human factor

You are being invited to take part in research on Information security threats in the supply chain. Christiana Akintoye at Coventry University is leading this research. Before you decide to take part it is

important you understand why the research is being conducted and what it will involve. Please take the time to read the following information carefully.

What is the purpose of this research?

The purpose of the research is to critically explore information security threats in the supply chain address issue of threats. More specifically, this research focussed on employees, supply chain partners and customers attitudes towards mitigating information security threats in the supply chain.

The research was granted ethical approval by Coventry University's Research Ethics Committee P106106

Do you have to take part?

No – it is entirely up to you. If you do decide to take part, please keep this Information Sheet and complete the Consent Form to show that you understand your rights in relation to the research, and that you are happy to participate. Please note down your participant number and provide this to the lead researcher if you wish to withdraw from the research at a later date. You are free to withdraw your information from the research at any time until the data is destroyed on 13/10/22 or until the data is fully anonymised in our records on 13/10/22. You do not need to provide a reason for withdrawing. A decision to withdraw, or not to take part, will not affect you in any way.

What will happen if I decide to take part?

You will have the opportunity to ask any question you may have about the survey. The questionnaire/interview will take place via telephone which will be convenient for you. It should take around 15 to 20 minutes and we would like to audio/record your responses.

Why have you been invited to take part?

You have been invited to participate in this research because you knowledge and experience

What are the benefits and potential risks and benefits in taking part?

By taking part, you will be helping Christiana Akintoye and Coventry University to better understand information security threats in the supply chain and there are no significant risks associated with participation.

What information is being collected in the research?

This survey will include questions about the following themes:

- Information security threats in the supply chain
- Top management support

- Commitment
- Sanction
- Attitude
- Subjective Norms
- Self-efficacy
- Rewards

Lawful basis of processing. Under the UK General Data Protection Regulation (UK GDPR) 2016 we must have a lawful basis to process your personal data and for the purpose of this research, our lawful basis is that of your consent. Although we do obtain your consent, this is not for data protection purposes.

What will happen to the results of the research?

The results of this research may be summarised in published articles, reports and presentations. Quotes or key findings will always be made anonymous in any formal outputs unless we have your prior and explicit written permission to attribute them to you by name.

Who will have access to the information?

Your data will only be accessed by the researcher.

Where will the information be stored and how long will it be kept for?

Your data will be processed in accordance with the UK General Data Protection Regulation 2016 (UK GDPR) and the Data Protection Act 2018 (DPA). All information collected about you will be kept strictly confidential. Unless they are fully anonymised in our records, your data will be referred to by a unique participant number rather than by name. If you consent to being audio recorded, all recordings will be destroyed once they have been transcribed.

All electronic data will be stored. All paper records will be stored in a locked filing cabinet in Coventry University. Your consent information will be kept separately from your responses. The researcher will take responsibility for data destruction and all collected data will be destroyed on or before 13/10/22

What will happen next?

If you would like to take part, please contact the lead researcher. You will be asked to complete a consent form before taking part.

Researchers contact details:

Christiana Akintoye, akintoyc@uni.coventry.ac.uk
[SUPERVISOR NAME AND CONTACT DETAILS]

Dr. Muhammad Kamal, Coventry University

Who do I contact if I have any questions or concerns about this research?

If you have any questions, or concerns about this research, please contact the researcher, or their supervisor. If you still have concerns and wish to make a complaint, please contact the University's Research Ethics and Integrity Manager by e-mailing ethics.uni@coventry.ac.uk. Please provide information about the research project, specify the name of the researcher and detail the nature of your complaint.

Thank you for taking time to read this information sheet and for considering participating in this research.

Appendix F: Pilot Results

In this report, concerns about information security threats in supply chain companies were analysed and

The reliability test, case summaries for missing values, outliers, demographic distribution, R Squares and casual relationships were the primary focuses of the report.

Reliability Analysis

Variables	No. of Items	Alpha Coefficients
Information security	6	0.700
Top Management	4	0.812
Commitment	4	0.816
Reducing Reward	4	0.715
Sanction	5	0.841
Monitoring/Evaluation	6	0.752
Attitude	4	0.882
Subjective Norms	4	0.832
Self-Efficacy	4	0.860

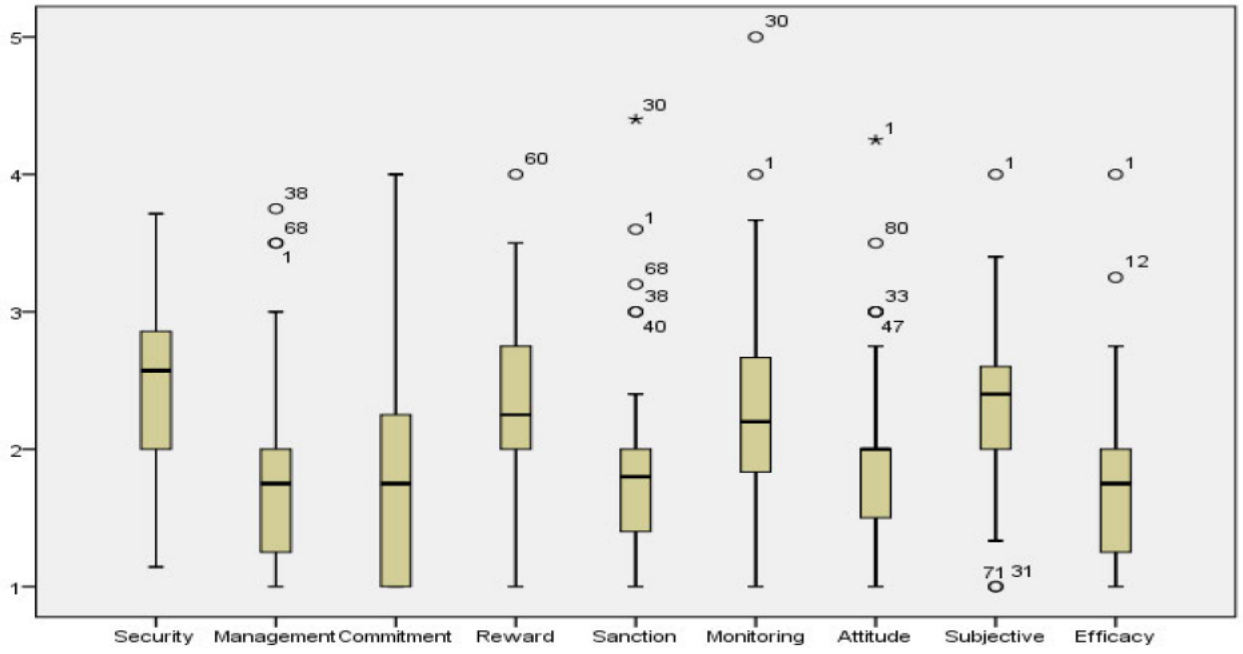
According to Field (2018), one way to confirm that the measurement is kept to a minimum is to determine properties of the measure that give confidence that it is doing its job appropriately. This is one method that can be used to confirm that the measurement is kept to a minimum. The first property is called validity, and it refers to whether or not an instrument measures what it is intended to measure. Reliability can be defined as the extent to which a given instruction can be interpreted in the same manner in a variety of contexts. There are many methods available to choose from when conducting a reliability test. Among these are things like maintaining internal consistency.

The Cronbach alpha coefficients for the pilot study are detailed in Table 1, which can be found above. The distributions from the alpha demonstrate that based on the Nunally (1978) benchmark of 0.70, instruments for information security threats and subjective norms appear to be below expected standards; as a result, they require further modifications and a re-assessment of opinions.

Distribution for missing values

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Security	73	91.3%	7	8.8%	80	100.0%
Management	73	91.3%	7	8.8%	80	100.0%
Commitment	73	91.3%	7	8.8%	80	100.0%
Reward	73	91.3%	7	8.8%	80	100.0%
Sanction	73	91.3%	7	8.8%	80	100.0%
Monitoring	73	91.3%	7	8.8%	80	100.0%
Attitude	73	91.3%	7	8.8%	80	100.0%
Subjective	73	91.3%	7	8.8%	80	100.0%
Efficacy	73	91.3%	7	8.8%	80	100.0%

The summary for missing values for cases can be found in the aforementioned Table 2, which notes that each variable has a total of seven cases with incidences of missing values, which has an effect of approximately nine percent on the statistical power and accuracy of the representation. On the other hand, this is less than a 10% bias effect.



Demographic Distributions

Demographic distribution for gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	73	91.3	93.6	93.6
	Female	5	6.3	6.4	100.0
	Total	78	97.5	100.0	
Missing	System	2	2.5		
Total		80	100.0		

Based on the distribution presented above, it is evident that the majority of the participants of the study are male, with a frequency of 73 (91%) whereas the females account for 5 (6%). The result demonstrates that the male gender is the most dominant in the company.

Demographic distribution for age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	21-30	9	11.3	11.5	11.5
	31-40	25	31.3	32.1	43.6
	41-50	41	51.3	52.6	96.2
	51-60	3	3.8	3.8	100.0
	Total	78	97.5	100.0	
Missing	System	2	2.5		
Total		80	100.0		

Table 4 above demonstrates the distribution for the age of respondents. The evidence reveals the highest distribution to be at the 41 – 50 years bracket which accounts for a frequency of 41 and a 51% of the total population.

Demographic distribution for educational background

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	School Certificate	1	1.3	1.3	1.3
	N.C.E	2	2.5	2.6	3.8
	Diploma or equivalent	7	8.8	9.0	12.8
	Bachelor's degree or equivalent	39	48.8	50.0	62.8
	Master's degree or equivalent	28	35.0	35.9	98.7
	Ph.D. or equivalent	1	1.3	1.3	100.0
	Total	78	97.5	100.0	
Missing	System	2	2.5		
Total		80	100.0		

Presented in Table 5 is the distribution for the educational background of the study, where the bachelor's degree is noted to be the qualification with the highest frequency at 39 (49%), demonstrating that the majority of the participants have acquired first-degree certifications.

Demographic distribution for position of respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Junior Staff	21	26.3	27.3	27.3
	Senior Staff	30	37.5	39.0	66.2
	Management	26	32.5	33.8	100.0
	Total	77	96.3	100.0	
Missing	System	3	3.8		
Total		80	100.0		

Presented in table 6 above is the distribution for the position of respondents with most of the staff noted to have a position of senior roles within their organisations with a frequency of 30 (37.5%) suggesting a higher level of participation from the management staff of the organisation.

Demographic distribution for business sector

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Manufacturing	29	36.3	37.7	37.7
	Logistics and transport	8	10.0	10.4	48.1
	Marketing and distribution	11	13.8	14.3	62.3
	Production and operation	29	36.3	37.7	100.0
	Total	77	96.3	100.0	
Missing	System	3	3.8		
Total		80	100.0		

Table 7 above demonstrates the distribution for the business sector where the manufacturing as well as production/operations are observed to have the highest level of frequency at 29 (36.3%). Both categories as such can be said to dominant in the population.

Demographic distribution for work experience

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 to 2 years	9	11.3	11.5	11.5
	3 to 5 years	10	12.5	12.8	24.4
	Above 5 years	59	73.8	75.6	100.0
	Total	78	97.5	100.0	
Missing	System	2	2.5		
Total		80	100.0		

Table 8 above demonstrates the distribution for work experience and shows that most respondents have work experiences ranging above 5 years in their respective organisations with a frequency of 59 (74%). The distribution demonstrates evidence of substantiality in the work experience of respondents.

Demographic distribution for number of employees

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1 to 10	23	28.8	29.5	29.5
	11 to 30	9	11.3	11.5	41.0
	31 to 50	6	7.5	7.7	48.7
	50 and above	40	50.0	51.3	100.0
	Total	78	97.5	100.0	
Missing	System	2	2.5		
Total		80	100.0		

Presented in Table 9 is the distribution of the number of employees in the company of interest. The result shows that the category for organisations with 50 and above workforce has the highest frequency at 40 (50%), revealing this category as the most dominant in the study.

The next section explains the process of phase 2 after the piloting test.