Security Challenges for Businesses undergoing Digital Transformation

Harrison Stewart
Univeril Technology
Germany
stewart@harrisonstewart.net

JDIM
Journal of Digital Information Management

ABSTRACT: *This research has undertaken a systematic review of digital transformation security. Four sections make up the research project: To begin, a topic modelling important journals on information systems is carried out to better grasp the field's issues. Secondly, a case study is conducted in an organization to find out their security concerns related to digital transformation. Third, a survey is conducted in this paper, followed by a pilot test, interviews and data analysis (Kumar et al., 2019; Walsham, 2006). Fourth, the results of the topic modelling, case study and data collection are compared, and the challenges, debates and gaps in the academic literature will be discussed (Alhogail et al.,2015; Alhogail et al., 2014; Allam, Flowerday, & Flowerday, 2014; Arbanas & Hrustek, 2019). Based on the findings, a system is constructed, and the evaluation technique is applied to enable easy use of the system. The results will be validated through an observational approach (Baskerville, 1999), user participation and a feedback technique. Based on the analysis, a future study is proposed for security research in digital transformation. This study aims to identify and analyze elements that represent typical barriers to digital innovation in organizations.*

Subject Categories and Descriptors: [C.1.2 Multiple Data Stream Architectures]; Cellular architecture [H.5 INFORMATION INTERFACES AND PRESENTATION]; Hypertext navigation and maps

General Terms: Digital Transformation, Topic Modelling, Digital Security

Keywords: Digital Strategy Security, Digital Strategy, Digital Transformation, IS/IT Strategy Security

Received: 18 October 2021, Revised 3 February 2021, Accepted 20 February 2021

Review Metrics: Review Scale: 0/6, Review Score: 4.35. Inter-reviewer Consistency: 78.2%

DOI: 10.6025/jdim/2022/20/2/46-66

1. Introduction

Digitalization has impacted research on IS/IT strategy development. Several studies on IS/IT strategies have been conducted in the literature, providing various solutions, insights and frameworks that are relevant and useful for practitioners and academics (Arbanas & Hrustek, 2019). Considering the digital age and the high number of cybercrime incidents, several studies have urged organizations to incorporate security into their digital strategy (Lundgren & Möller, 2017). Confidentiality, integrity and non-repudiation are all fundamental elements in digital transformation security. The term "integrity" refers to the assurance that communication or transaction has not been tampered with. Non-repudiation establishes the existence of a communication or transaction and assures that its contents cannot be challenged after it has been transmitted (Lundgren & Möller, 2017; Collet, 2020; Karpunina et al., 2019; Stewart & Jürjens, 2018). The digital strategy encompasses both the technical and human activities within an organization and describes how the lifecycle of an organization's digital strategy practices should be managed. Academics and practitioners have long been concerned about the security of digital strategies, and a survey conducted by the digital association found that cyberattacks cost over US $103 billion in 2018/2019, rising to 10.5 trillion US$ by 2025 (Sausalito, highlighting

the impact of cybersecurity on businesses as a whole. This shows that companies must recognize and address digital security as a strategic, not just an IT issue. In the past, risk management in traditional IS/IT strategy was based on the cost structure and higher value, which is different from today's IS/IT strategy, where cybersecurity has become a strategic investment in information and communication technology (ICT) and a prerequisite for a company's long-term sustainability. As a result, there remains a disconnect between risk management efforts and developing key cybersecurity capabilities.

Therefore, a critical assessment of the current state of the art regarding academic initiatives and practitioner perspectives is required. Over the years, a substantial body of academic research has been built on digital innovation, and some research has addressed the security of digitization and the information it contains (Duc and Chirumamilla, 2019; Ande et al., 2020). Research on malware, phishing, password attacks, and social engineering attacks on information systems has evolved over the decades (EderNeuhauser et al., 2018; Bullée & Junger, 2020; Hu & Wang, 2018; Hadnagy, 2018). Several organizations are attacked daily, knowingly or unknowingly (Hu & Wang, 2018; Burda et al., 2020). The attackers' goal is to spy on, modify, delete and gain unauthorized access to data, resulting in significant financial and reputational damage (Sausalito, 2020; Oliveira et al., 2017; Stewart & Jürjens, 2017).

In 2021, there was a staggering 105 per cent increase in ransomware cyberattacks worldwide. These attacks aim to harm individuals or businesses by rendering their computer systems inoperable until they pay a ransom (Thorwat, 2018; Arbanas & Hrustek, 2019). According to the Cyber Threat Report 2022, released Thursday by cybersecurity firm SonicWall, ransomware attacks increased 1,885 per cent globally in 2021, with the healthcare industry seeing a 755 per cent increase. In North America, the number of ransomware attacks increased by 104 per cent, slightly below the global average of 105 per cent. Although academic studies on security, in general, have been done, the focus has tended to concentrate on security policy, phishing security, and computer security which have all been studied in different ways.

This study is crucial for achieving a balance between establishing sufficient controls and the ever-changing nature of cyber-attacks. Thus, the study is guided by the following research questions;

RQ1; What are the current gaps in past literature on IS/IT strategy that contribute to the biggest challenges for companies in digital transformation regarding security?

RQ2; What elements are most effective and successful in contributing to the security of a company's digital transformation.

A topic selection criterion must be undertaken based on the selected research topics to establish definitive proof and prevent bias. Once the primary research phase is completed, this paper adopts Pan and Tomlison's research guidelines (2016). The references on the main search phase's selected articles are extensively checked, and if the paper fulfils relevant criteria, it will be included in the synthesis. Furthermore, a financial company is used as a case study for analyzing the concept of security in digital strategy to provide conceptual clarity. According to Stewart (2022), the basic definition of information security states that information systems security is about maintaining the integrity of the logical and formal components of information systems. Consequently, information security is protecting data, processes and information. Similar concepts of information systems and security can also be found in other literature (Samonas & Coss 2014, Luse et al. 2013). All subsequent literature evaluations in IS security research have been limited to specific streams of study (e.g., compliance) within the field rather than broad assessments of the field's trajectory.

The paper begins with an introduction in Section 1, then explores the characteristics of organizational IS security in Section 2, and finally provides an overview of different IS security theories in Section 3. Section 4 of this paper discusses the case study of a financial institution on the security challenges of digital transformation. In contrast, Section 5 discusses the research methodology before presenting the results in Section 6. Section 7 discusses the findings and Section 8 concludes with an analysis of the common elements impacting IS security. In conclusion, the scope of this research is confined to the security of digitization (Baskerville, 1993; Siponen, 2005).

2. Literature Review

There are numerous studies on factors affecting information systems security (Alhogail et al.,2015; Alhogail et al., 2014; Allam, Flowerday, & Flowerday, 2014; Arbanas & Hrustek, 2019). Al-Omari et al. (2012) focus on user compliance with ICT regulations to investigate the factors that influence the security of information systems. Al-Hogail (2015) examines security culture to maintain an organization's information systems. Stewart (2022) proposes a framework that addresses the development and implementation of information security policies (ISPs), while Alhogail, Mirza & Bakry (2015) proposed a framework that addresses only the human aspects of IS protection.

Dillion (2021) conducts a systematic review of the literature on information systems security by performing topic modelling of the primary information systems journals to understand the debate in the field; performs a Delphi study with senior information security executives of major companies in the US to identify the security issues they consider important, and compares the results of the topic modelling and the Delphi study; and discusses the significant controversies, gaps and paradoxes found in the scientific literature. Dillion then addresses the lack of

synergy between academic research and practical concerns and proposes a future research agenda in three broad themes: IS security design, attacks; vulnerabilities; compliance and behaviour.

Baskerville (1993) published the first literature review on IS security as a model made up of three eras that are linear in time and advance. Each of these eras has its own set of tactics, goals, means, obstacles, and philosophical assumptions that distinguish them from one another. The first generation, which originated in the early 1970s with the purpose of mapping constrained solutions to an information issue, is referred to by Baskerville as checklist techniques. This era's security was achieved by the use of checklists and risk assessments and was mainly based on product supplier documentation. The third era of Baskerville builds on logical transformation methods and consists of a highly abstracted design that describes the problem and solution space. Structured analytical data modelling and entity-relationship diagrams are common development methods and tools for this generation, while logical control designs and data flow diagrams are common security tools. Baskerville (1993) suggests three specific security risks based on his overview:

1. Baskerville claims that IS security management uses a mechanical approach to complexity partitioning.

2. There is a focus on the bare minimum of controls required to meet protection standards.

3. There is a dualism of growth.

According to Baskerville, security is treated as an add-on to the overall architecture of information systems. Instead, he believes that information systems architecture should incorporate all aspects of security from the outset. Siponen (2005) asserts in a review that, while researchers have established various new methodologies, old approaches like checklists, standards, maturity criteria, risk management, and formal procedures continue to dominate research. Security is still treated as an outcast by system designers due to competing priorities between security goals and information use (Stewart, 2021; Stewart, 2022); White and Dhillon (2005) define duality in secure systems development as the process by which "an information system and its security are designed, built, and implemented separately in an organisational environment, allowing for the possibility of conflict between a system's functionality and its security" (Albrechtsen 2007). Such dualism is defined by Spagnoletti and Resca (2008) as 'drift,' which happens when the technological system deviates from the initial plan. As initially conceived by Baskerville, evidence of development dualism predominates, as evidenced by various research (Paananen et al., 2020).

Future IS security research should include social and organizational elements, according to Dhillon and Backhouse (2001). The human and behavioural components are subsumed under the social and organizational variables (Stewart & Jürjens, 2018). McFadzean et al. (2006), Siponen (2005), and Siponen and Oinas-Kukkonen (2005) all emphasized the need to incorporate similar aspects in later years (2007). Many other academics have noted the underlying organizational issues, especially concerning policy compliance (Stewart, 2022; Karjalainen et al., 2019). Different theories have been explored recently by researchers in their attempt to discover answers to problems affecting the security of information systems (Zoto et al., 2018; Shahri & Mohanna, 2016; Han, Dai, Tianlin Han, & Dai, 2015; Lubua & Pretorius, 2019; Stewart, 2022). Recognizing diverse IS security concepts and their achievements aid in analyzing the IS security literature and identifying elements that impact an organization IS security. Socio-technical theory, distributive cognitive theory, general deterrence theory and the nine-five-circle theory are the most often used IS security theories.

2.1. Security Theories for Information Systems

2.1.1. Social Technical Theory

The concept of bringing together and considering both "social" and "technical" components as companion pieces of a complex system underpins social-technical theory. Organizations concentrating on a single aspect of the system fail to analyze and comprehend the system's deep linkages. The role of the human factor in IS security has been considered in this theory as an important factor in detecting and preventing data breaches. Many researchers have studied this, and Stewart (2017) pointed out that the human factor plays an important role in cybersecurity. Although many consider cybersecurity a technological factor, social-technical theory remains a practical approach for designing system security and its environment through analysing goals, culture, technology, people, infrastructure, process, and procedure. usability challenges, internal security governance, and security needs (Zoto et al., 2018; Charitoudi & Blyth, 2013). As a result, social technical theory is applicable to explore ways in which people contribute to an organization's IS security based on their perceptions and approach to IS security.

2.1.2. Distributed Cognitive Theory

Distributed cognition, developed by Edwin Hutchins, is the belief that information exists not just inside an individual, but also within the individual's social and physical surroundings. The idea focuses on self-efficient processes by focusing on how a person may use skills rather than what kinds of abilities they have, hence it can be applied to information system security as security self-efficacy (Shahri & Mohanna, 2016). As information is spread more in a virtual environment, the idea recommends collaboration among individuals to achieve common goals. As a result, information system security should be associated with human cognition (Han et al., 2015)

2.1.3. General Deterrence Theory

The goal of general deterrence is to prevent illegal behaviour. To discourage is to deter. According to the concept,

people avoid committing crimes because they fear the harsh repercussions. This idea was used for information system security to induce dread of personal repercussions and deter them from taking actions that might jeopardise the system's security (Hu et al., 2011). As a theory based on certainty and gravity of consequences, it proposes a range of measures/punishments to be implemented depending on the gravity of a given person's illicit actions contrary to information security.

This idea is fundamental in IS security because of the high prevalence of cybercrime and its financial consequences (Lubua & Pretorius, 2019).

2.1.4. Nine-Five-Circle Theory

By considering the organization's security culture, the Nine-Five Circle integrates the three theories to prevent criminal behaviour, improve human behaviour, and improve the design and security of information systems. The theory focuses more on measuring and evaluating the IS security performance of organizations and improving the link between technology, process and human factors (Stewart & Jürjens, 2017; Stewart, 2021; Stewart, 2022). All of the hypotheses above have been discussed; the nine-five-circle theory seems more relevant because it incorporates all three theories and other aspects into one theory, as detailed in all the theories above. This section addresses part of the first research question because, despite numerous researchers' efforts to propose various ideas that could be effective in protecting the security of information systems, the theories have failed to identify the true causes of the problems before attempting to solve them, which is what this study attempts to do. To identify and comprehend the fundamental origin of an IS security breach in an organization, a case study is used in this study.

3. Case Study

The study illustrates the key features of a financial institution's digital strategy implementation programme and how it can help explain constructs of success and critical events in IS security (Doukidis et al., 2020). Due to the company's nature, it was deemed necessary to use staff knowledge and experience to help the company prevent data breaches that could damage its reputation (Collet, 2020; Duc and Chirumamilla, 2019; Stewart & Jürjens, 2018). The company in this study operates in the banking sector and has made the strategic decision to use digitalization to create new value, increase transparency, embrace a Robo-advisor, reduce costs, increase convenience, improve approval rates, increase efficiency and security, and provide consumers with better access to information (Hess et al., 2016; Legner et al., 2017; Stewart & Jürjens, 2018).

To achieve this digitalization goal, the management has set up a dedicated digital department with a team of software engineers to bring the digital transformation to the market (Singh & Hess, 2017; Stewart, 2022). As a result, more than 300 employees have started their duties in the digital department, contributing to the sector's success. This digital department adheres to the organization's numerous standards and centralized IS/IT strategy, yet, the transition to digitalization requires a different approach than the traditional IS/IT strategy. Although, the number of security threats has risen due to the organization's fast digital transformation (Singh & Hess, 2017; Stewart, 2022). As depicted in Figure 1, their existing strategy fails to handle contemporary security risks, causing significant impediments in the digital transformation.

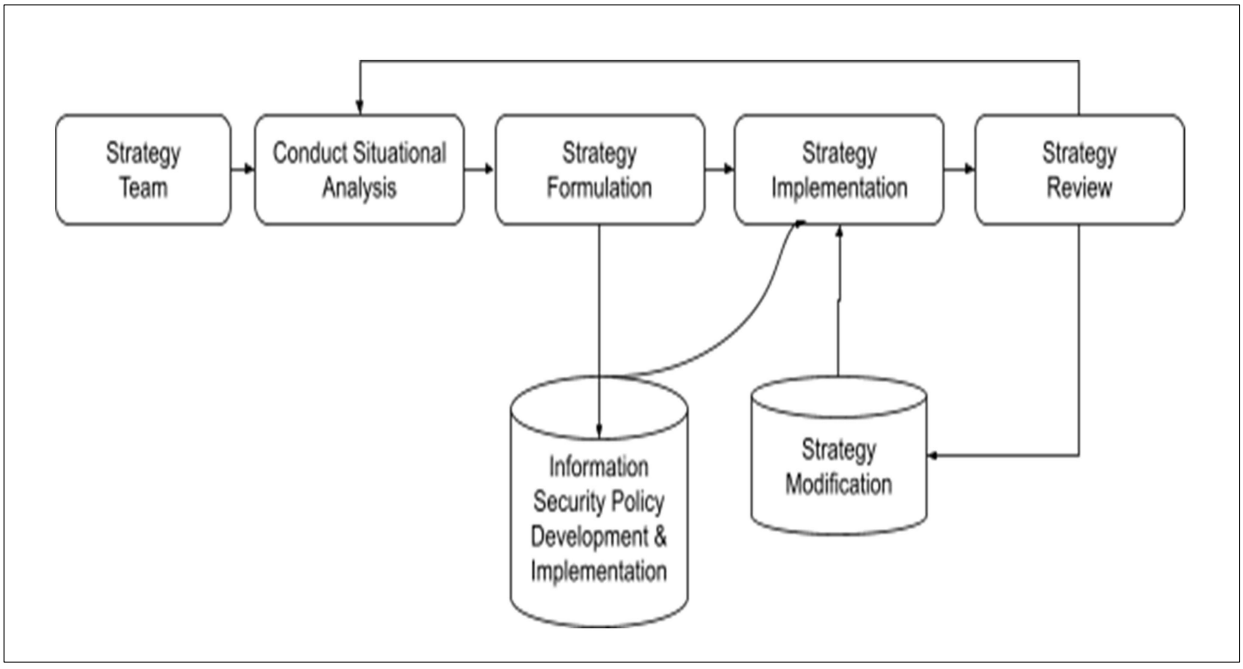

Figure 1. The organisation's current IS strategy and Digital Strategy

3.1. Problem Identification

Based on the information collected during the assessment phase in section 3, it was clarified that data breaches and high funds are among the organization's challenges. According to management, the cost of the most recent data breach was estimated at $4.01 million, with an average data breach of 12 records each year. On the other hand, these episodes have shattered the trust of consumers and partners, forcing investors and customers to cease conducting business with the company (Gordon et al., 2011).

To gain the confidence of consumers and investors and drive digital transformation, the company must have appropriate IS security measures in place to protect itself from cyber-attacks and insider threats while delivering secure services and goods. Understanding IS security qualities is critical for determining which security key elements are essential during digital transformation. Organizations pursuing digital transformation must go beyond the traditional ISO27001 security definition of Confidentiality, Integrity, and Availability (CIA) security baselines and qualities, which has been the core emphasis of any information security strategy (Stewart, 2022). Even though this CIA has become the industry standard, the organization in this study fails to recognize these IS security attributes and thus fails to protect or has inadequate protection; increasing IS security breaches, which will have a significant negative impact on their digital transformation (ITU, 2017; Fields et al., 2016)

4. Research Methodology

The contribution of this paper is twofold: first, it follows a literature review/secondary study and assesses the security of digital transformation in an organization. For this purpose, three public and well-known databases and search engines, namely Google, Wikipedia and Google scholar, were consulted, and a case study supported this work. This paper surveyed the organization, followed by a pilot test, interviews and data analysis (Duan et al., 2019; Zhou, 2020; Kumar et al., 2019; Walsham, 2006). The results are validated using an observational approach (Baskerville, 1999), system evaluation techniques and a feedback technique.

4.1. Content Analysis

This study uses the topic modelling approach to find important hidden topics in the emerging IS academic security literature. The search was limited to abstracts, titles and author keywords of articles published in information management journals with a literary journal guide ranking A or higher between January 2014 and January 2021. To limit the search engine's capacity to discover the document and to determine the fine search, special characters such as ("/", "-", "(", ") were employed. The result was 4298 articles, with a final sample size of 2938 due to some abstracts that were irrelevant to the study. The focus of the 2938 articles was on the security of information systems in the context of digital transformation processes (Huang et al. 2018). Mainstream topics like information security, work environment and demographic factors are ignored in this study.

The collected abstracts were screened for errors by removing certain expressions such as "the, a, are" and performing word normalization to remove redundant or noisy material. The LDA approach is used to model the abstracts of these articles and uncover latent themes (Blei et al., 2003). The ideal number of subjects is estimated using two reduction algorithms proposed by Cao et al. (2009) and Arun et al. (2010) and two maximization techniques offered by Griffiths and Steyvers (2004) and Deveaud et al. (2014).

Like Mahfuth et al. (2017), a research checklist is created to ensure that the data extraction process meets the requirements. The work of Hassan et al. guides the quality of data extraction (2015). This study's checklist employs three scales, each categorized and assigned a score. The final score is calculated by adding the sums of the individual elements on the checklist. The scale runs from 0.5 to 5, with 5 being the highest possible score.

4.2. Discussion of Content Analysis Findings

Table 1 indicates the synthesis's quality rating based on the quality evaluation. The quality ranking of all key research publications is shown in Table 1. Low-quality studies were disregarded because they lacked particular findings or research techniques. Finally, the ideal number of subjects was set at 39, which were then extracted using LDA in the R topic models package.

Exploration Type	Scores
Quantitative	61%
Qualitative	12%
Formal experiments	9%
Mixed Techs	10%
Case study	1% (as indicated in this study)

Table 1. Topic analysis

4.3. Data Collection

The primary data source for this study was a survey conducted to confirm and complement the results. A questionnaire was developed and distributed to 40 security experts, managers, stakeholders and all executives. The management and researchers determined the overall objectives of the survey, resources, budget and timeframe in line with best practices in questionnaire development (Umbach, 2004). By mutual agreement between the researchers and the management, the survey was conducted through an internet, postal, telephone, and face-to-face

interviews (Witmer et al., 1999; Walsham 2006). These methods were agreed upon by the researchers and management based on their advantages and disadvantages. The question format was then designed to include both open and closed questions (Neuman, 2007). The survey also contained closed-ended Likert scale questions that required respondents to select from a list of prepared answers. The flow of questions was then designed to create a logical sequence of questions by rejecting responses from unqualified respondents (Sax et al., 2003), ensuring that respondents felt comfortable and provided truthful information (Myers and Newman 2007; Walsham 2006). The surveys were organized into five sections: (a) introduction; (b) answer pre-screening; (c) welcome questions, (d) progression to more detailed and challenging questions, and (e) conclusion. The questionnaires were evaluated on whether they were required, how lengthy they were, and whether they contained all the information needed for this study. The researcher pretested the questionnaire and, after approval by the client, made changes that resulted in the final layout of the questionnaire, which the client accepted.

The questionnaire received 40 responses from experts involved in the organization's IS strategies and greatly influenced the development of their IS strategy. For the data analysis, SPSS was used. Although the pilot test included 65 questions in the initial phase, only 25 were included in the final questionnaire based on feedback from the pilot test. The interviews lasted 45 minutes. Semi-structured interviews were then conducted to gain a deeper understanding of employees' perceptions and opinions of their current digital strategy, particularly in relation to current cyber threats and their ability to secure their innovative ideas. As in the work of Britten (1995), open-ended questionnaires were used to conduct the interviews, starting with simple questions and progressing to more complex and sensitive topics. The data collection phase was completed with direct participation from staff, the IS strategy department and the IT security department.

The adaptation of the questionnaire contributed to obtaining a clear understanding of the organization in the case study digital transformation processes. For the selection of respondents, a systematic sample technique was adopted (see Table 2).

In this instance, the researcher chose every nth person,

$$\text{where } n = \frac{population\ spopulation\ size}{sample\ size} \quad (1)$$

There were 200 employees divided by ten, giving a total number of two. Every second person was selected here. As a result, the sample size was reduced to 20 participants who were identified anonymously to maintain anonymity (Walsham, 2006), as indicated in Table 2.

During the analysis phase, the interview data were categorized to identify any difficulties about variables impeding digital strategy security growth. These interviews were utilized to validate the content analysis codes in section 4.1 and the components employed in this study.

Group of users	Number of users	Anonymous ID
Senior executives, CIO	2	IDR_01, IDR_02
Digital Strategy Manager	3	IDR_03
IT Decision Maker	3	IDR_04
Security Manager (CISO)	1	IDR_05
IT-Staff & Network	2	IDR_06, IDR_07
DevOPs	9	IDR_08, IDR_09, IDR_10

Table 2. Employee Tags used for Anonymity

4.4. Factors Affecting Digital Transformation Security

The study uncovered 39 studies on information security conducted in both the public and private sectors and by individuals working in these domains. The goal was to figure out why digital security, or IS security, is still an issue for most businesses (such as the case study in this article) and individual users of modern technology.

From the synthesis, the data analysis revealed eight topic areas explored in mainstream IS security research, as described in the preceding section (see Table 2). The findings show that the most common themes in the sector are stakeholder and employee misconceptions about information security which are associated with individual behaviour and negligence. Individual behaviour and compliance are directly connected to the components of the information security myth. Building these connections is vital because employees are willing to accommodate cyber security when they see a need. Several research publications have studied behavioural adjustments to increase security compliance or minimize breaches. Other findings include threat and vulnerability assessment, organization cyber security strategy, software engineers' secure system engineering, security monitoring, advanced threat investigation strategy, and incident reporting and remediation strategy.

5. Developing the Security in Digital Strategy

The study is divided into two sections. The first part of the

study, which lasted from January 2020 to August 2021, included the research review and a case study on the organization. The second phase, called the evaluation phase, started in September 2021 and ended in January 2022. The nine factors and their implementation in the organization are discussed in this phase. The participants'

DSS Constructs		Definition	
Evaluation of threat	SM	IS/IT Strategy and Digital Strategy Misconception	Collett (2020) Karpunina et al. (2019) Stewart (2020) Andriotis et al. (2015), DeWitt et al. (2015), Stewart & Jürjens (2018) Dhillon et al. (2016) Kraemer et al. (2009) Mlitz (2021) Duc & Chirumamilla (2019) Li et al. (2020) Kavuta & Nyamanga (2018) Mahfuth et al. (2017) Glaspie & Karwowski (2018)
Vulnerability and Risk	ETVR	Threats, vulnerabilities, and mitigation techniques that are linked to the digital strategy and assist to reduce the overall risk.	Collet (2020) Stewart (2021) Chooi & Ahmad (2017) Lucila (2016) Flowerday & Tuyikeze (2016) Sohrabi et al. (2016) Soomro et al. (2016) Karyda et al. (2005) Ines (1994) Wood (2004) Baskerville and Siponen (2002) Stewart (2021) Joshi et al. (2017) Stewart & Jürjens (2017) Karumbaiah et al. (2016) Stewart (2022)
Cybersecurity Strategy	CSS	Action plan to improve the security and resilience of electronic products and services. It is an overarching, top-down strategy for cybersecurity that sets out a series of goals and priorities to be achieved within a specific timeframe.	Mlitz (2021) Stewart (2022) Collett 2020) Stewart (2021) Duc and Chirumamilla (2019) Li (2020) Stewart (2020) Doukidis et al. (2020) Stewart & Jürjens (2017) Stewart & Jürjens (2018)
Secure System Engineering	SSE	Integration of secure software engineering tools, methodologies, and processes into the software life cycle.	Bertolino et al. (2014) Ayewah et al. (2008) Acker et al. (2012) Appelt et al. (2014). Stewart & Jürjens (2017) Stewart & Jürjens (2018)
Security Testing and Evaluation	ST&E	Analyse and assess the security measures required to secure digital services and goods. Reduces threats and risks in systems and lowers the likelihood of losses due to a cybersecurity breach.	Moeini et al. (2019) Da Veiga & Martins (2015) Luo et al. (2019) Stewart & Jürjens (2018)

Protective Monitoring	PM	Automatic security checks based on logs created by systems or applications.	Collett (2020) Karpunina et al. (2019) (Terglav et al. (2016)
Strategic Advanced Threat Intelligence	SATI	Strategic threat intelligence provides a comprehensive Overview of an organisation's threat landscape	Stewart (2020) Padayachee (2012) Stewart (2022)
Incident Response and Remediation	IRR	Respond to incidents quickly and efficiently to maximise effectiveness.	Ahmad et al. (2021) Ahmad et al. (2020) Morgeson et al. (1997) Ahmad et a. (2012) Helsloot & Groenendaal (2011)

Table 3. Factors affecting the security of the information system or digital transformation

comments, observations and interviews are used to evaluate this study.

The eight constructs are discussed in more detail at this stage.

5.1. Security Misperception

The role of security in digital transformation, is highly misjudged by executives and IT decision-makers in various organizations (Collett, 2020; Karpunina et al., 2019). Stewart (2020) emphasized the importance of managers' perception of security. He pointed out that the misperception of security among managers and employees is due to several factors that prevent organizations from developing a well-defined secure culture. In addition to Stewart, other research studies have also attempted to identify the various reasons for the varying degrees of challenge in developing a digital security strategy. For example, managers' perceived conflict between security and usability (Andriotis et al., 2015; DeWitt et al., 2015). Stewart (2020) examined the various academic literature and reports from information security institutions on the evolution of security. He highlighted four factors that influence the misperception of security: speed, usability, privacy and value (Stewart & Jürjens, 2018). Various organizations consider security at the expense of usability, leading to a significant conflict between security and usability (Dhillon et al., 2016). According to Kraemer et al. (2009), organizational and human aspects are closely linked to information security, while Stewart (2020) emphasizes how the interaction between people and technology can improve information security. Without user engagement, the development and implementation of DSS would be challenging, so user behaviour in the context of the digital security lifecycle is critical to success.

Apart from the misconceptions of the executives, there was also a huge misconception about secure coding among the software engineers (Mlitz, 2021) and the security teams (Duc & Chirumamilla, 2019, Li et al., 2020) due to factors such as lack of security knowledge, lack of teamwork, budget constraints, lack of prioritization of security, lack of commitment, security tools and culture, security controls to be implemented and their proper implementation. Considering the incentives between the security and software development teams, both teams were encouraged to play on the same team to avoid disagreements by aligning their interests and creating complimentary incentives. Several data breaches resulted from security failures that hindered the remediation of vulnerabilities in digital products and services (Stewart & Jürjens, 2018; Collett, 2020; Karpunina et al., 2019). Software engineers who refuse to adhere to an established security framework or security standards are also a major bottleneck in many organizations, as this leads to shadow IT. Stewart (2022) defines shadow IT as a means of misusing information systems, e.g, the unauthorized storage and processing of data.

After the perception improvement phase, the management, security, and software development team engaged and collaborated to improve the security posture of their digital transformation. The researcher further developed a solution suitable for the company to improve the existing misperception of security.

5.2. Evaluation of threat Vulnerability and Risk

A cyber threat is defined as any harmful behaviour aimed at causing harm to cyberspace (anything connected to a computer): Cyber threats include data breaches, identity fraud, ransomware, data corruption, and so on. Once attackers attempt to infiltrate a system, they try to undermine the system's confidentiality, integrity, and availability (CIA). These three concepts form the CIA triad, sometimes referred to as the AIC triad.

Confidentiality preserves the privacy of the data or information, i.e. access to confidential data must be restricted to authorized persons. Integrity preserves the legitimacy and integrity of the data or information, i.e., data and information must not be manipulated by an unauthorized user during transmission or storage. Availability refers to the accessibility of the service or data, i.e., authorized users should be able to access the services and data at

any given time.

Digitization requires a "security by design" approach that minimizes vulnerable coding errors and vulnerabilities. To achieve this, software engineers were provided with security guidelines, including the Open Web Application Security Project's (OWASP) Top 10 White Paper, the Groupe Spéciale Mobile Association's (GSMA) "GSMA IoT Security Guidelines & Assessment", the IoT Security Foundation's "Secure Design Best Practice Guides" and the Cloud Security Alliance's "Future Proofing the Connected World: 13 Step to Developing Secure IoT Products". The researcher and the external security organization provided several security training and awareness sessions at all development and deployment stages, managed by the facilitators. Security testing was conducted during the development cycle to identify security issues. The main objective of this phase was to ensure that the digital strategy in this work resulted in a secure digital product and services.

5.3. Cybersecurity Strategy

Due to the large data, they manage, the organizations in this study are perfect targets for cyber attackers (Collett, 2020; Stewart, 2021; Chooi & Ahmad, 2017). The lack of a security strategy within the digital transformation strategy has contributed to their current vulnerability. This phase should identify the recommended cybersecurity strategy and how comprehensive these studies are within the organization. Although several researchers and practitioners have recommended their security strategies, these recommendations cannot be applied to the organization in this study, as observed by Stewart (2020). The same security framework cannot be applied to multiple organizations due to different needs. Therefore, the researcher proposes his strategy in this study by adapting key points from previous studies and neglecting industrial norms.

The purpose of the cybersecurity strategy in this study is to assure the CIA of the organization's digital transformation, which has been accomplished by providing proactive, effective, and active assistance and development. As the cybersecurity strategy is an overall plan to ensure digital transformation security, it is crucial to update the digital security strategy regularly. Considering the importance of people in cyber security strategy, establishing a rigid security culture is an essential factor in an organization.

Although this study does not omit information security policies (Lucila, 2016; Flowerday and Tuyikeze, 2016; Stewart, 2022), compliance (Sohrabi et al., 2016) and information security management (Flowerday and Tuyikeze, 2016), cybersecurity requires a more proactive approach as opposed to a reactive approach (Soomro et al., 2016; Stewart & Jürjens, 2017). Organizations with various security requirements and objectives have different security requirements and objectives (Karyda et al., 2005; Ines, 1994; Wood, 2004). According to Baskerville and Siponen (2002), it is critical to understand the organization's security requirements while designing security initiatives. As a result, the organization should define its security objectives, including the level of security it aspires to attain. Here, the focus was on preventing cyberattacks and incidents in advance. The company's cyber threat landscape situation was analyzed by exploring the products and services developed and the types of cyber-attacks to which they are exposed (Collett, 2020; Stewart, 2021). Next, the threats in the supply chain were analyzed, e.g., compromised components used for the final products utilized by the company's customers and partners. The advanced awareness of the company's threats enabled the researcher and participants to develop an effective cybersecurity strategy. During this phase, the threat attributes faced by the organization were presented descriptively. The NIST cybersecurity framework was then used to assess the cybersecurity maturity level. This assessment was divided into the following categories: (i) policy, (ii) governance and (iii) incident recovery skills (Joshi et al., 2017; Stewart & Jürjens, 2017). The assessment covered traditional IT operations technology, the Internet of Things and systems.

As mentioned earlier, cybersecurity is a continuous process rather than a product (Stewart, 2021). As a result, the stated cybersecurity program was continually amended to meet the established strategic goals. The defined solutions were submitted to management for assessment, feedback, and approval. Management expressed support since the misconception concerns were first handled (Stewart & Jürjens, 2017; Stewart, 2022). The whole approach was extensively documented to meet the strategic objectives, including risk assessments, cybersecurity plans, policies, guidelines, and procedures. Individual duties were clearly stated, and feedback was obtained from participants. Cybersecurity awareness and training efforts were also conducted (Stewart & Jürjens, 2017; Karumbaiah et al., 2016).

5.4. Secure System Engineering

Software engineering is critical to digital transformation (Mlitz, 2021; Stewart, 2022), which brings with it a number of challenges, such as cyber threats which could lead to organizational financial loss (Collett, 2020; Stewart, 2021). According to a study by Duc and Chirumamilla (2019), attackers often look for vulnerabilities in software designs and architectures to gain access to a person's or company's information. Stewart (2022) concluded in his study that compliance is not synonymous with security and that companies relying on industry standards to improve digital security need to develop an application security strategy rather than depending on an industry standard. Based on this study, the software development team identified the critical security factors that must be considered at all stages to create effective and resilient software that can withstand all security attacks (Li, 2020; Stewart, 2020). In addition to software security, additional measures were taken to prevent malware, denial-of-service attacks and hacking (Doukidis et al., 2020). The re-

searcher, including the CISO and security strategy facilitators, explained to the executives the importance of storing, processing and transmitting consumer data, leading the executives to identify significant threats to their digital transformation strategy posed by insecure software. Management was advised to give software security the highest priority and to invest in improving software security measures (e.g., through training and seminars on software security) (Collett, 2020). The organization's digital transformation can be protected from the threats of data leaks, data breaches and financial theft by integrating security into the digital strategy (Stewart & Jürjens, 2017; Stewart & Jürjens, 2018). At the end of this phase, the managers recognized the need to allocate sufficient resources to ensure that software was developed with security in mind to prevent intrusion by attackers. This phase emphasized the importance of software security for rapid and effective digital transformation in the organization.

5.5. Security Testing and Evaluation

Risk assessment includes security test and evaluation (ST&E). To test and improve software security, vulnerability detection and security assurance through security testing are usually used at this point. Implementing appropriate security testing procedures has become critical in conducting effective and efficient security testing, so this testing stage was crucial. This phase was also concerned with developing refined approaches and applying and disseminating them in practice (Bertolino et al., 2014; Ayewah et al., 2008; Acker et al., 2012; Appelt et al., 2014).

The researcher at this stage focused on three groups that contribute to digital transformation, namely humans, processes and products, all of which contribute to system security. As Stewart & Jürjens (2017) states, the NFC addresses the interrelationships between these three groups and provides a solution to the problem. In this study, the human aspect consists of the software engineers, staff and IT managers (Stewart & Jürjens, 2017), the process consists of manual and automated procedures (Acker et al., 2012), while the product is represented by the digital product or service (Stewart & Jürjens, 2018). In general, the same security challenges are common to all, but each group faces challenges when continuously complying with the established security rules.

5.5.1. Humans

Due to various challenges, cyber security training and awareness measures have been implemented, including a strict security policy required for compliance at all product life cycle stages of the product life cycle.

5.5.2. Process (Technology)

According to Stewart (2022), developmental security testing/evaluation encompasses the entire system development lifecycle, including all post-design phases. This phase demonstrates that the required security controls have been implemented correctly, are operating as expected, security policies have been enforced appropriately, and comply with established cybersecurity standards.Any inclusion of vulnerable components from suppliers or changes to these components may impact the security posture of the final product and the security controls currently implemented in this study (Bertolino et al., 2014; Appelt et al., 2014). Therefore, it is critical to establish rigid control levels to allow software engineers to perform additional security testing/assessment to reduce or eliminate uncertainties. When testing custom software applications, Stewart (2022) recommends static analysis, dynamic analysis, binary analysis or a mixture of these three approaches, which can be performed during code review or using different tools (e.g., binary analyzers and application scanners) (Ayewah et al., 2008).

The researcher and the security team developed security assessment rules and procedures followed by the engineers (Stewart, 2022). These plans specified the types of analyses, tests, evaluations and reviews that should be performed for software and firmware components, the level of rigour and the artefacts produced during these processes (Bertolino et al., 2014; Ayewah et al., 2008; Acker et al., 2012; Appelt et al., 2014). Stewart's (2022) definition of security testing/evaluation refers to the severity and complexity of the evaluation process (e.g., black-box, grey-box or white-box testing), as shown in Figure 2. The security testing/evaluation coverage refers to the scope (i.e., quantity and type) of artefacts included in the evaluation process.

5.6. Protective Monitoring

In this study, more vulnerabilities, e.g., related to human error, and their software products and systems, were uncovered through proactive monitoring (Moeini et al., 2019; Da Veiga & Martins, 2015). This technique involved security inspections and audits conducted by the security review team and facilitators. This monitoring aimed to obtain performance feedback that enabled corrective action to be taken before failures occurred in developing and implementing the digital security strategy.

Thus, to achieve this effectively, the researcher set up a risk assessment team led by a competent person to assess the existing work practices based on the proposed NFC methodology and organizational systems (Luo et al., 2019). Their main role was to be proactive by conducting work-specific risk assessments, analyzing the level of implementation of the proposed framework, reviewing the adequacy of the implementation of the digital strategy, and overseeing the overall cybersecurity management system through monitoring and audits (see Figure 9) (Luo et al., 2019).

Furthermore, a system was set up to establish ground rules that would be followed by all employees and comply with legal obligations. According to the researcher, the importance of this step was to analyze the for organization's financial and operational aspects and identify and assess vulnerabilities. Since security is not a product, but a continuous process, this study conducted

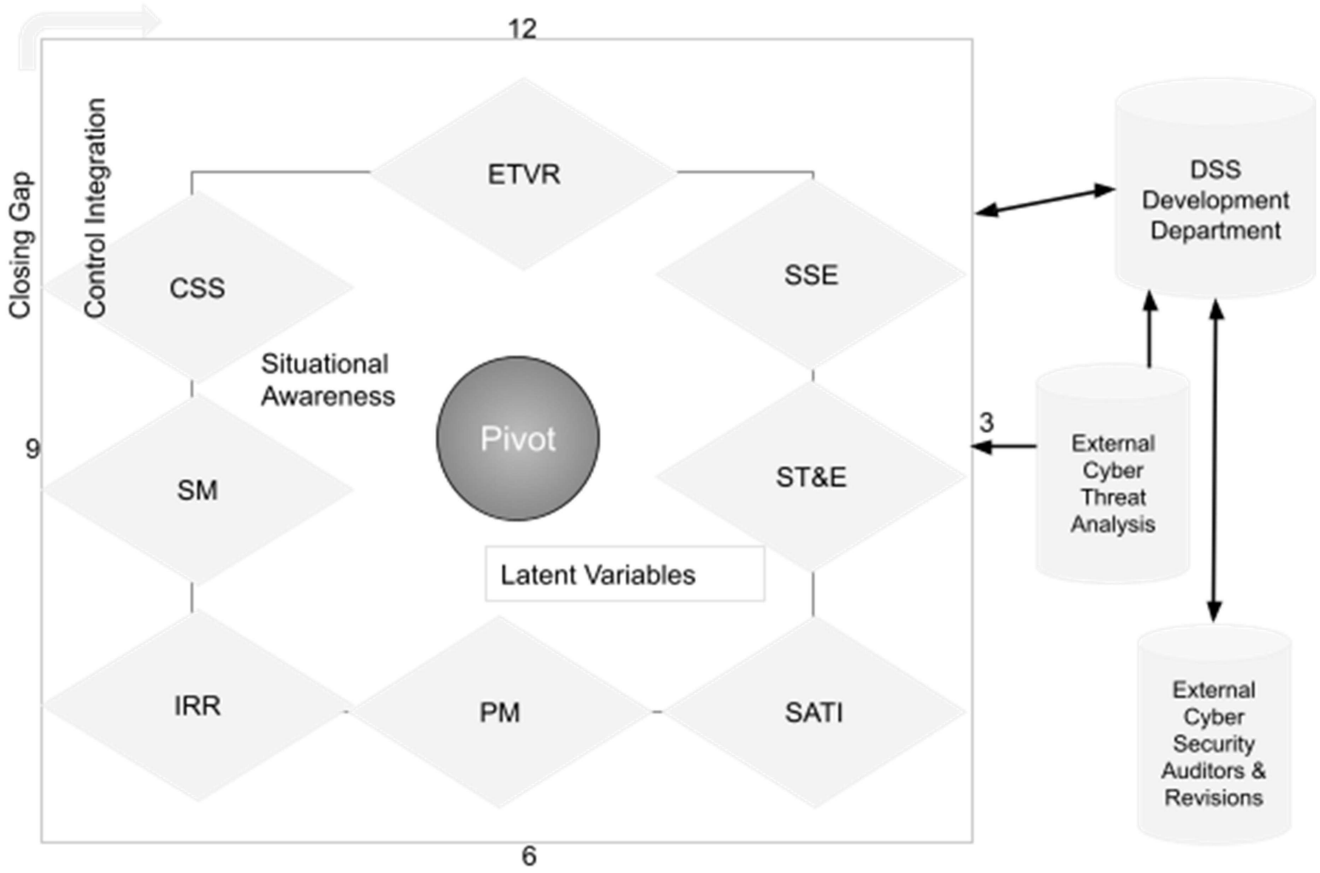

Figure 2. Digital transformation security framework consisting of all 8 constructs, latent variables and other components

proactive monitoring at regular intervals to determine what needs to be updated and what needs to be fixed. The main objective of this proactive monitoring was aimed at developing a concept for the security and sustainability of digital products and services (Stewart & Jürjens, 2018).

This approach contributes to maintaining digital security and improving the security performance of digital transformation (Stewart & Jürjens, 2018; Collett, 2020; Karpunina et al., 2019).

This phase allowed the researcher to assess the extent to which the security strategy guidelines proposed in this study were followed. The involvement of managers was crucial in this phase as they were to ensure that their involvement promoted good performance (Terglav et al., 2016).

5.7. Strategic Advanced Threat Intelligence

Threat intelligence has been neglected in the development of a digital strategy. According to Stewart (2020), threat intelligence is critical in developing security strategies. Incorporating threat intelligence issues into the digital security strategy or IS/IT security strategy can help organizations identify vulnerabilities during the development lifecycle. It also improves security awareness among employees. When engineers know which vulnerabilities to strengthen during the development lifecycle, they be come aware and can identify where a hacker might make a request or attack the product and services.

Improving threat intelligence can alert both engineers and staff of malicious attempts. These alerts may also enable them to take the appropriate action and report incidents to the security department. About Padayachee (2012), the intelligence value of threats obtained by an organization is defined as the difference between the direct and indirect benefits of specific knowledge about their threats. Thus, the threat information derived in this study was documented and distributed to software engineers and the entire organization (Stewart, 2022). In conclusion, a strategic threat intelligence system was established to direct the digital transformation department. Stewart (2020) recommends that staff in the critical data department receives regular security training to strengthen their cybersecurity skills and ensure that all digital department staff participate in cyber defence. All members of the digital department were keen to learn more at this stage. They were aware of the importance of cyber security and its advantages.

5.8. Incident Response and Remediation

This section effectively handles security-related incidents, covering technical, cultural and organizational aspects. Recent reports show an increasing number of cyber security incidents resulting in significant financial losses

(WEF, 2019). Even though the organization in this study has a specific cybersecurity budget, incidents continue to occur. The linear incident response system depicted in Figure 3 is used in this study to prevent, identify, mitigate, remediate, and educate on cybersecurity incidents.

Due to the complexity and persistence of their cyber threats, a specialized cyber security incident response team was critical to the security strategy proposed in this study (Morgeson et al., 1997; Ahmad et a., 2012). This team involves members from the IT department, legal department, corporate communications, human resources and other departments. A contingency plan (e.g., based on NIST Special Publication 800-61 Revision 2) is then provided to the team to manage such situations from early detection to recovery. Five key persons were then

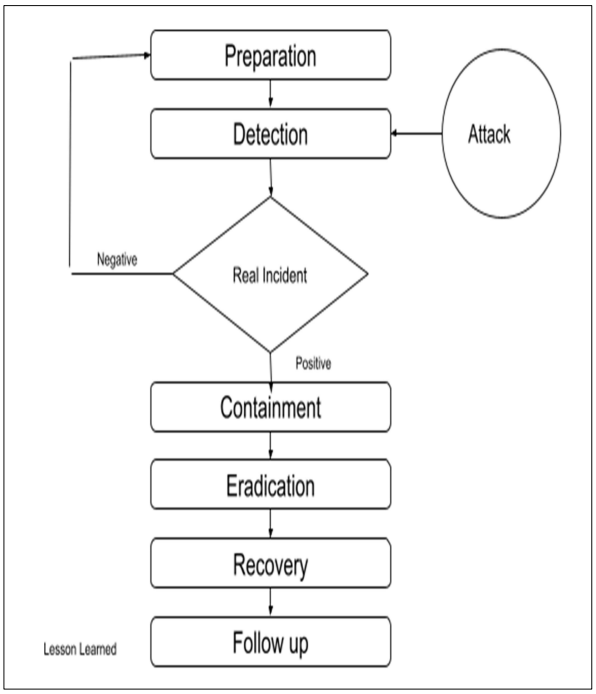

Figure 3. Linear incident response framework

selected to manage the incidents, conduct the incident investigation, analyze the scale of the incident, determine the role of crisis communication and make leadership decisions (Helsloot & Groenendaal, 2011). The team was trained on handling security incidents, covering everything from detection to reporting, which led to a standardized protocol for reporting cybersecurity issues across the organization. To aid in identifying and mapping possible intrusions, incident response teams were given a suite of software tools that allowed them to scan network traffic records and visualize information flow. The training phase improved the team's cyber situational awareness to gain advanced knowledge of their systems and network activities, which also helped to conduct a continuous risk assessment (Ahmad et al., 2021).

This stage of the research gave the incident response team the capacity to prevent and identify incidents in the first place, as well as the technological capability to respond to cybersecurity incidents (Ahmad et al., 2020).

6. Observations and Writing Up of the Results

The observation is based on a systematic strategy in which greater emphasis was placed on specific actions to emphasize the differences in this study (Angrosino & dePerez, 2000). Due to the obvious length of the period, the researcher could observe and participate in a range of activities over a more extended period. As a result, 20 members of the digital department could define the study's impact on their daily activities and how the findings could improve their existing strategy security development process.

Building relationships requires trust for individuals to open up. Other good practices, such as ethics, have been explored to reduce researcher bias and increase the efficiency of the field experience.

Before analyzing the eight constructs of the elements of success or failure, a basic question needs to be answered. When and how can it be determined whether a digital strategy security program is a success or a failure? The assessment procedure was carried out methodically to determine the answer to the question, as in the work of Bishop et al. (1998). Each participant in the study was interviewed twice. This was in the form of a personal interview and a group interview. Participant observation was

Participant Groups	Interviewee
#1	Interviewee #IDR_01 noted that cybersecurity knowledge growth has increased over time, while #IDR_04 noted the positive change in executive attitudes and behaviours towards cybersecurity strategy, and #IDR_05 saw that the misconception of security is also a key construct for the organisation's strategic goals."
#2	Interviewee #IDR_05 specifically pointed out that this study has provided criteria and benchmarks for good security architectures and solutions, as well as methods to achieve them. Better mechanisms to hide and/or manage complexity were also cited by #IDR_06, while #IDR_04 noted that their previous incident response processes lacked flexibility. Respondent #IDR_03 mentioned that prior to this study, most of their systems were not creating event logs, which was a barrier to incident detection.
#3	Interviewees #ID_08, #IDR_09, IDR_10 and IDR_06 pointed out that the availability of capable staff has always been a major obstacle to an effective data security strategy, but this study has removed that obstacle.

Table 4. Summary of the Results Achieved During the first phase

also conducted to gather additional data. The overall findings were reassuring, as listed in table 4.

In summary, the structures underpinning organizational outcomes may be recognized and understood within the proposed framework and are characterized by the following constructs:

• A coherent and well-defined DSS;

• Maintain close coherence between the DSS and the organization;

• An appropriate focus on all the different dimensions of digital strategy and security;

• A thorough assessment of the organizational and corporate landscape.

Issue	Method	Source of Evidence
Improve the costs associated with the security programmes of the digital strategy.	Interview	IDR_01
Improve the level of knowledge in the field of digital transformation security.	Interview	IDR_04
Improved awareness and elimination of misperceptions.	Interview	IDR_02, IDR_03, IDR_04, IDR_05, IDR_06, IDR_09 IDR_10
Improved digital transformation strategy aligned with corporate security.	Interview	Senior Executive
Monitor staff understanding and commitment to "Secure by Design" to eliminate misunderstandings.	Participatory observation	Researchers
Improved management willingness to invest in cybersecurity projects.	Participatory observation	Researchers
Examine the actions of stakeholders and staff.	Direct Observation	External Auditors

Table 5. Summary of the Results Achieved During the first phase

Despite the beneficial results listed in Table 5, there were still some issues that this research tackles to remedy some of the organization's inadequacies.

a. Assessing the security programme for the digital strategy is a controversial and sensitive issue that needs to be addressed. This is crucial for the long-term sustainability of the digital transformation project and the implementation of the budgeting process, which is also necessary for the full recognition of the security function of the digital strategy in the company.

b. In addition, the digital strategy security programme should continue to involve the entire organizational pipeline. The DSS framework has been kept simple in design: Digital security strategy is about human compliance with defined policies, not computer capability.

c. The simplicity and ease of use of the DSS framework is an important attribute that helps in developing the security programme for the digital strategy within the organization and other organizations. However, more specific and complex technologies are likely to be critical. So that you know – the three bullet points have been addressed accordingly.

A continuous update and improvement of the digital strategy were carried out to address the open points (a) and (b). In contrast, the third point was addressed by reiterating the NFC life cycle during a change that affects the current established strategy.

Questions	Extremely satisfied	Somewhat satisfied	Neutral	Some what dissatisfied	Extremely dissatisfied
Following this study, how satisfied is your organisation with the overall finding that compliance with an industry standard does not convey security and that it is therefore necessary to develop security best practices and train software developers on security issues?	10	0	0	0	0
How satisfied are you with the improvement in developers' behaviour and attitude towards vulnerability of their application after this study?	10	0	0	0	0
How satisfied are you with the knowledge derived that lack of security leads to a data breach and therefore the need to thoroughly read application's security policy and participate in security training is very important?	10	0	0	0	0
Following this study, how satisfied are you that management has invested in security projects to improve the security awareness of all developers and employees who use the application for their daily activities?	9	1	0	0	0
How satisfied are you with the knowledge acquired from this study?	10	0	0	0	0

Table 6. Matrix Table Question & Respondents

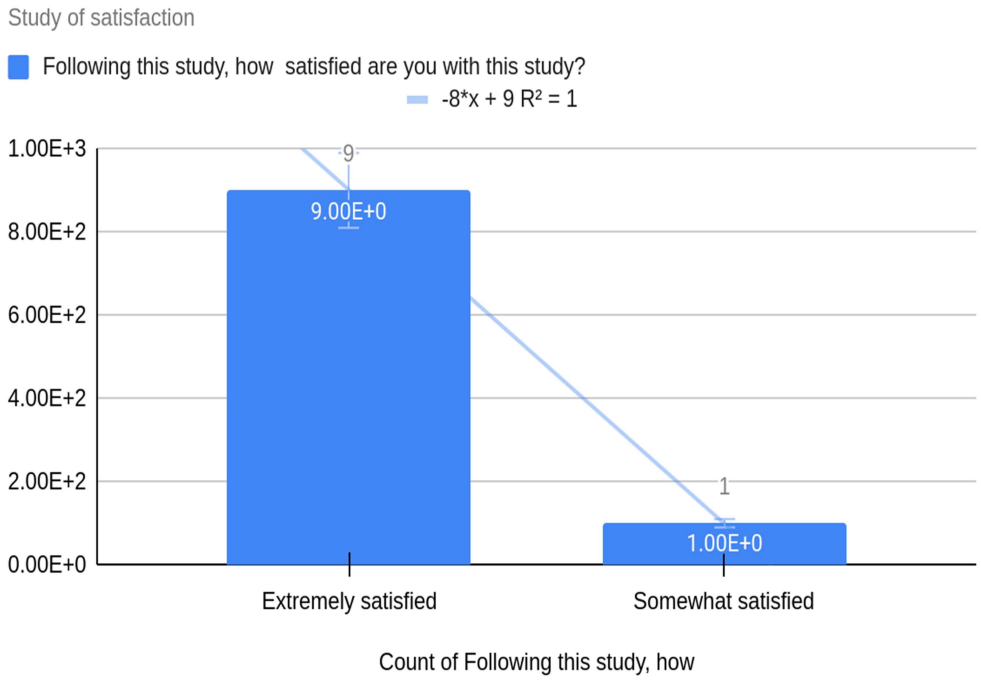

Figure 4. Observation

The recommended strategy improved the company's digital sovereignty and consequently its digital transformation, strengthening its digital economy. A security-by-design strategy was a critical component of this study and one of the key technological enablers. The strategic framework recommended in this paper sets out the organization's cybersecurity policy, divided into key principles, scopes of action and a set of strategic targets.

Matrix Table 6 summarizes the multiple-choice questions with the corresponding answers and scales. The significant drop in Figure 5 is due to participants' dissatisfaction with the study's focus on digital transformation and not on other departments.

7. Success Factors

Although eight constructs were considered crucial for achieving a secure innovation process for digital transformation in an organization, management and employee acceptance contribute to its success. According to Stewart (2022), security initiatives are useless if they are not used. Therefore, teams were continuously trained to use the proposed framework after first improving their misconceptions about security. As in the work of Stewart (2022), organizational commitment contributed positively to the success of this study.

Software development is critical to digital transformation, and any threat can result in financial loss to the business. Regular training of the software development team is a crucial factor that must be considered at all stages to create effective and resilient software that can withstand most security attacks. The security team and the software developers must work in harmony with each other. It is necessary to integrate the digital transformation of a company into a security process for the digital strategy, which can contribute to the security of the digital transformation in a company.

The evaluation of threats, vulnerabilities and risks is intended to promote the development of a digital security strategy as it enhances the confidentiality, integrity, availability, authenticity, authority, verifiability and non-repudiation of critical assets. This construct helps preserve data and systems' security during digital transformation initiatives.

The cybersecurity strategy helps to ensure data security during digital transformation in all endeavours that deal with sensitive data.

Given that the cybersecurity strategy is an overall plan to ensure the security of the digital transformation, it is crucial to regularly update the strategy when something changes that may affect the security of the product or service. The cybersecurity strategy must be proactive, and its landscape must be addressed and analyzed regularly.

Protective monitoring of the digital strategy security development and implementation process contributes to the success factor for the security of the digital strategy (Moeini et al., 2019; Da Veiga & Martins, 2015). This can be achieved by addressing all vulnerabilities that arise from human error, software products and systems.

Frequent security inspections and audits need to be con-

ducted and monitored to assess the improvement and impact of each vulnerability and how they can be mitigated and improved. Inadequate monitoring of digital strategy security initiatives can contribute to financial losses and failure of digital strategy security. Therefore, competent managers must be deployed to conduct regular risk assessments to achieve this effect.

Advanced threat intelligence aims to support the development of the security of the digital strategy by increasing the perceived importance of cyber security within the organization, thus contributing to the improvement of security culture. This strategy considers the different parties' best interests and the characteristics of information systems (IS) and information technology (IT). Developing a security culture requires both leadership and comprehensive cooperation, both of which are imperative to the achievement of the security of a digital strategy. Cybersecurity should be an intrinsic aspect of corporate governance, and all parties need to understand the significance of security. All individuals involved should take responsibility for participating in establishing and evolving culture of security as a mindset in the assessment and implementation of digital security or IS/IT strategy security.

8. Discussion

The study compares the major underlying assumptions to understand better the challenges of digital transformation in traditional IT/IS strategy techniques. The misconception of digital strategy and IT/IS strategy was one of the major outcomes of this study. Software engineers tackle security initiatives as an afterthought, so usability often takes precedence over security (Stewart, 2022). In subsequent years, other IS security initiatives have proposed several mainstream programmes, such as information security policy (Flowerday & Tuyikeze, 2016; Lucila, 2016), human behaviour and compliance (Furnell and Clarke, 2012; Crossler et al., 2013; Stewart, 2022).

Other literature evaluations, on the other hand, have encouraged academics to consider digital transformation security and IS/IT security. The contributions of research to the eight security constructs in this work were examined from several angles. These eight constructs' technical, intellectual, and organizational levels were addressed. This study deals with the security of information systems from the perspective of digital security strategy.

9. Implications

In this study, a conceptual framework was developed to explain the influences on the development and outcomes of the digital strategy. The study considers past papers and a case study. This study has significant implications for practice. For example, the proposed framework with the eight constructs tends to explain the influences on digital transformation and information security research findings.

The framework provides a new perspective to study the evolution of an organization's digital transformation, secure digital strategy development, and some success factors. This work has justified the applicability of the proposed framework to elucidate the actions required in digital strategy projects by systematically testing the interrelationships between all eight constructs, thus answering research question 2.

This study has brought a new perspective to explain why digital transformation strategies require more than the traditional IS or IS/IT strategy process. Furthermore, incorporating security into IS/IT security or digital security involves the engagement of several factors that must work together to achieve a successful security strategy.

In practice, this study can serve as a reference for innovative organizations and their managers to set up a strategic security process by highlighting the context of digital strategy to enhance staff recognition, e.g., by providing them with security training to improve staff awareness. While playing an important role in digital strategy, other latent variables such as business strategy and business processes are not the main key to developing a secure digital strategy. Therefore, a secure digital strategy can be achieved by combining the eight constructs in this study by arranging them in a structured way for an effective digital strategy security development and implementation.

10. Limitations

As the study was conducted in Germany and most of the data were collected digitally, it cannot be applied to all companies; consequently, further research is needed to assess different organizational contexts.

11. Conclusion

The research questions in this study contribute to developing and implementing a secure digital strategy. Eight constructs were analyzed and evaluated to create a model for developing a secure digital strategy. The research included a comprehensive examination of the current state of digital strategy security and the reasons for its success or failure. The synthesis of the literature is used to determine the most important/critical factors for IS security so that organizations do not make the wrong decisions. The study found that a misconception of security among various factors by leaders in an organization, leading to ignorance of security among employees and affecting the culture of security, is seen as the main obstacle to embedding security in strategic digital transformation, which answers the research question 2 (Parsons, McCormac, Butavicius, & Ferguson, 2010). Apart from the importance of management involvement and employee acceptance of information security, the study also identified other factors such as threat vulnerability and risk as-

sessment, which include threats, vulnerabilities and mitigation techniques that are linked to the digital strategy and help reduce overall risk. Cybersecurity strategy includes an action plan to improve the security and resilience of electronic products and services. It is an overarching, top-down cyber security strategy that sets out a series of objectives and priorities to be achieved within a specific time frame. Secure systems engineering involves integrating secure software engineering tools, methods and processes into the software life cycle. Security auditing and assessment involves analysing and evaluating security measures required for the security of digital services and goods. The goal is to reduce systems' threats and risks and the likelihood of losses due to a cyber security breach. Protective monitoring includes automatic and manual security checks based on logs generated by systems or applications. Strategic advanced threat intelligence includes strategic threat intelligence to provide a comprehensive overview of the threat landscape of an organization. Finally, there is the incident response and remediation factor, which provides for proactive, rapid and efficient incident response to ensure maximum effectiveness. The important aspects to consider when creating and implementing a digital security plan in an organization are addressed in this response to research question 1, which is part of the gaps in the previous literature on IS/IT strategy.

Insufficient understanding of these key factors for digital transformation security has led to a persistent risk to corporate information security. Furthermore, the factors identified in this study play an important role in security and form a common attribute, namely a combination of humans (knowledge, education and training), technology (secure programming and coding) and processing (continuous security training of employees and constant network monitoring). Therefore, the paper proposes the solution of using the nine-five-circle theory to ensure that other theories such as (social, technical theory, distributed cognitive theory and general deterrence theory) are considered in information security initiatives.

More empirical research is needed to validate or make the approach more effective. An extension to other scenarios in the same sector for comparisons and cross-analysis would greatly benefit. It could also be applied to other sectors where different aspects focus. The significance of raising awareness of the security of digital strategies is highlighted in this study, which will serve as an incentive to prioritize appropriate digital security and its communication to employees. This will act as an incentive to bridge the gap between the percentage of organizations that take security precautions and those that do not. When it comes to security, the challenges of digitization for businesses undergoing digital transformation are numerous in German.

References

[1] Acker, S.V., Nikiforakis, N., Desmet, L., Joosen, W. & Piessens, F. (2012). *FlashOver:Automated Discovery of Cross-Site Scripting Vulnerabilities in Rich Internet Applications*.

[2] Ahmad, A., Desouza, K.C., Maynard, S.B., Naseer, H., Baskerville, R.L. (2020) How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, 71, 939–953.

[3] Ahmad, A., Hadgkiss, J. ,Ruighaver, A.B. (2012) Incident response teams – Challenges in supporting the organizational security function. Computers and Security, 31 (643–652).

[4] Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M., Baskerville, R.L. (2021). How Can Organizations Develop Situation Awareness for Incident Response? A Case Study of Management Practice, *Computers & Security*, Vol. 101, p. 1–15

[5] Al-Omari, A., El-Gayar, O., Deokar, A. (2012) *Security policy compliance: User acceptance perspective*, IEEE, 45, 1–10.

[6] Albrechtsen, E. (2007) A qualitative study of users' View on information security. Computers and Security, 26, 276–289.

[7] AlHogail, A. (2015). Design and validation of information security culture framework, Computers in Human Behavior, 49, 567–575.

[8] Alhogail, A., Mirza, A., Bakry, S.H. (2015), A comprehensive human factor framework for information security in organizations. *Journal of Theoretical and Applied Information Technology,* 78, 201–211.

[9] Alhogail, A., Mirza, A. (2014). A framework of information security culture change. *Journal of Theoretical and Applied Information Technology*, 64, 540–549.

[10] Allam, S., Flowerday, S.V., Flowerday, E. (2014) Smartphone information security awareness, A victim of operational pressures. Computers and Security, 42, 56–65.

[11] Ande, R., Adebisi, B., Hammoudeh, M., Saleem, J. (2020) Internet of Things: Evolution and technologies from a security perspective. *Sustainable Cities and Society*, 54, 101728, https://doi.org/10.1016/j.scs.2019.101728.

[12] Andriotis, P., Oikonomou, G., Mylonas, A., Tryfonas, T. (2016) A study on usability and security features of the android pattern lock screen. *Information and Computer Security*, 24, 53–72.

[13] Appelt, D., Nguyen, C.D., Briand, L.C., Alshahwan, N. (2014) Automated testing for sql injection vulnerabilities: An input mutation approach. *In*: Proceedings of the 2014 International Symposium on Software Testing and Analysis. ISSTA, 2014, 259–269, New York, NY, USA ACM.

[14] Arbanas, K., Žajdela Hrustek, N.Ž. (2019) Key success factors of information systems security. *Journal of Information and Organizational Sciences*, 43, 131–144.

[15] Arbanas, K., Žajdela Hrustek, N.Ž. (2019) Key success factors of information systems security. *Journal of Information and Organizational Sciences*, 43, 131–144.

[16] Arbanas, K., Žajdela Hrustek, N.Ž. (2019) Key success factors of information systems security. *Journal of Information and Organizational Sciences*, 43, 131–144.

[17] Arun, R., Suresh, V., Madhavan, C.V.Murthy, M.N. (2010) On finding the natural number of topics with latent dirichlet allocation: Some observations, *Pacific-Asia conference on knowledge discovery and data mining*. Springer: Berlin, p. 391–402.

[18] Ayewah, N., Hovemeyer, D., Morgenthaler, J.D., Penix, J., Pugh, W. (2008) Experiences using static analysis to find bugs. *IEEE Software*, 25, September/October, 25, 22–29, Special issue on software development tools.

[19] Baskerville, R.L. (1999) Investigating information systems with action research. *Communications of the Association for Information Systems*, 2, [DOI: 10.17705/1CAIS.00219].

[20] Bertolino, A., Traon, Y.L., Lonetti, F., Marchetti, E., Mouelhi, T. (2014), Cleveland, Ohio, USA Coverage based test cases selection for XACML policies. *In*: Proceedings, (March) 31 IEEE Seventh International Conference on Software Testing, Verification and Validation, Workshops, Vol. 2014. *IEEE Computer Society*, p 12–21.

[21] Blei, D.M., Ng, A.Y., Jordan, M.I. (2003). Latent dirichlet allocation. *Journal of Machine Learning Research*, 3, 993–1022.

[22] Britten, N. (1995) Qualitative interviews in medical research. *BMJ*, 311, 251–253 [DOI: 10.1136/bmj.311.6999.251] [PubMed: 7627048].

[23] Cao, J., Xia, T., Li, J., Zhang, Y. & Tang, S. (2009) A density-based method for adaptive LDA model selection. *Neurocomputing*, 72, 1775–1781.

[24] Charitoudi, K. & Blyth, A. (2013) A socio-technical approach to cyber risk management and impact assessment. *Journal of Information Security*, 04, 33–41.

[24] Chooi, S.T. Ahmad, K.M. (2017). National cybersecurity strategies for digital economy IEEE. *In: ternational Conference on Research and Innovation in Information Systems (ICRIIS)*, Vol. 2017, p. 1–6.

[25] Collet, S. (2020) What is security's role in digital transformation? https://www.csoonline.com/article/3512578/what-is-securitys-role-in-digital-transformation.html, Vol. 2020. [Online; accessed 23-September-2022].

[26] Da Veiga, A., Martins, N. (2015) Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers and Security*, 49, 162–176 [DOI: 10.1016/j.cose.2014.12.006].

[27] Deveaud, R., Sanjuan, E.,Bellot, P. (2014) Accurate and effective latent concept modeling for ad hoc information retrieval. *Document Numérique*, 17, 61–84, document no. ´erique.

[28] Dhillon, G., editor (1997). Managing Information System Security. Macmillan Education: UK.

[29] DeWitt, A., Kuljis, J. (2006) Aligning usability and security: A usability study of polaris. *ACM International Conference Proceeding Series*, 149, 1–7 [DOI: 10.1145/1143120.1143122].

[30] Dhillon, G., Oliveira, T., Susarapu, S., Caldeira, M. (2016) Deciding between information security and usability, Developing value based objectives. Computers in Human Behavior, 61, 656–666 [DOI: 10.1016/j.chb.2016.03.068].

[31] Dhillon, G., Smith, K., Dissanayaka, I. (2021) Information systems security research agenda: Exploring the gap between research and practice. *Journal of Strategic Information Systems*, 30 [DOI: 10.1016/j.jsis.2021.101693].

[32] Dhillon, G., Backhouse, J. (2001) Current directions in IS security research: Towards socio-organizational perspectives. *Information Systems Journal*, 11, 127–153.

[33] Doukidis, G., Spinellis, D. & Ebert, C. (2020) Digital transformation-a primer for practitioners. *IEEE Software*, 37, 13–21

[34] Duc, A.N., Chirumamill, A. (2019). Identifying security risks of digital transformation-an engineering perspective, In Conference on e-Business, e-Services and e-Society, p. 677–688. Springer.

[35] Eder-Neuhauser, P., Zseby, T., Fabini, J. (2018). Malware propagation in smart grid monocultures Malware-Ausbreitung in Smart Grid-Monokulturen. *Elektrotechnik und Informationstechnik*, 135, 264–269.

[36] Flowerday, S.V., Tuyikeze, T. (2016) Information security policy development and implementation: The

what, how and who. *Computers and Security*, 61, 169–183.

[37] Glaspie, H.W., Karwowski, W. (2018) Human factors in information security culture: *A literature review. Advances in Intelligent Systems and Computing*, 269–280.

[38] Gordon, L.A., Loeb, M.P., Zhou, L. (2011) The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19, 33–56.

[39] Griffiths, T.L., Steyvers, M. (2004) Finding scientific topics. Proceedings of the National Academy of Sciences, 101 (Supplement 1), 5228–5235.

[40] Han, D., Dai, Y., Han, T., Dai, X. (2015). Explore Awareness of Information Security: Insights from Cognitive Neuromechanism, *Computational Intelligence and NeuroCience*, p. 1–11.

[41] Hassan, N.H., Ismail, Z., Maarop, N. (2015) Information Security Culture, A systematic Literature Review. *The 5th International Conference on Computing and Informatics*, p. 456–463. instanbul: The 5th International Conference on Computing and Informatics.

[42] Helsloot, I., Groenendaal, J. (2011) Naturalistic decision making in forensic science: Toward a better understanding of decision making by forensic team leaders. *Journal of Forensic Sciences*, 56, 890–897

[43] Hess, T., Matt, C., Benlian, A., Wiesböck, F. (2016)," Options for formulating a digital transformation strategy. MIS Quarterly Executive, 15.

[44] Hu, Q., Xu, Z., Dinev, T., Ling, H. (2011) Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM*, 54, 54–60

[45] Huang, A.H., Lehavy, R., Zang, A.Y., Zheng, R. (2018) Analyst Information Discovery and Interpretation Roles: A Topic Modeling Approach. *Management Science*, 64, 2833–2855.

[46] ITU. (2017). Global Cybersecurity Index (GCI). International Telecommunication Union: Geneva.

[47] Karjalainen, M., Sarker, S.,,Siponen, M. (2019) Toward a theory of information systems security behav-iors of organizational employees: *A dialectical process perspective. Information Systems Research*, 30, 687–704.

[48] Karjalainen, M., Sarker, S., Siponen, M. (2019) Toward a Theory of Information Systems Security Behaviors of Organizational Employees: *A Dialectical Process Perspective. Information Systems Research*, 30, 687–704.

[49] Karpunina, E.K., Konovalova, M.E., Shurchkova, Julia, V.S., Isaeva, Ekaterina, A., Abalakin, A.A. (2019), Economic security of businesses as the determinant of digital transformation strategy: In: Institute of Scientific Communications Conference., pp. 251–260.

[50] Karumbaiah, S., Wright, R.T., Durcikova, A., Jensen, M.L. (2016) Phishing training: A preliminary look at the effects of different types of training. *In*: Proceedings of the 11th Pre-ICIS Workshop on Information Security and Privacy, pp. 1–10.

[51] Kraemer, S., Carayon, P., Clem, J. (2009) Human and organisational constructs in computer and information security: Pathways to vulnerabilities. *Computers and Security*, 28, 509–520.

[52] Kumar, D., Sharma, A., Kumar, R., Sharma, N. (2019) Restoration of the network for next generation (5G) optical communication network, *In*: 2019 International Conference on Signal processing and Communication (ICSC), Vol. 2019. *IEEE Publications*, p. 64–68. Search in Google Scholar.

[53] Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N., Ahlemann, F. (2017) Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. Business and Information Systems Engineering, 59, 301–308 [DOI: 10.1007/s12599-017-0484-2].

[54] Li, P.L., Ko, A.J., Begel, A. (2020) What distinguishes great software engineers? *Empirical Software Engineering*, 25, 322–352 [DOI: 10.1007/s10664-019-09773-y].--

[55] Lubua, E.W., Pretorius, P.D. (2019) Ranking Cybercrimes based on their impact to organisations' welfare, THREAT Conference Proceedings. Proceedings, (1–11).Johannesburg: THREAT Conference.

[56] Lucila, N.B. (2016) Information security policy development: *A literature review. Int. J. Innov. Res. Inf. Secur.*, 3, 1–7.

[57] Lundgren, B., Möller, N. (2019) Defining information security. *Science and Engineering Ethics*, 25, 419–441.

[58] Luo, A., Guchait, P., Lee, L. Madera, J.M. (2019) Transformational leadership and service recovery performance: The mediating effect of emotional labor and the influence of culture. *International Journal of Hospital*-Management, 77 (4) 31-39

[59] Moeini, M., Rahrovani, Y., Chan, Y.E. (2019) A review of the practical relevance of IS strategy scholarly research. *Journal of Strategic Information Systems*, 28, 196–217.

[60] Morgeson, F.P., Aiman-Smith, L.D. & Campion, M.A. (1997) Implementing work teams: Recommendations from organisational behaviour and development theories. In: Advancesin Interdisciplinary Studies of Work Teams, Vol.

4 (edited by M. M. Beyerlein, D. A. Johnson & S. T. Beyerlein). Elsevier Science & Technology Books: Amsterdam.

[61] Neuman, W.L. (2007) Basics of social research. Qualitative and Quantitative Approaches, 2nd edn. Allyn & Bacon: Boston, USA.

[62] Paananen, H., Lapke, M., Siponen, M. (2020) State of the art in information security policy development. Computers and Security, 88, 1–14.

[63] Padayachee, K. (2012) Taxonomy of compliant information security behavior. Computers and Security, 31, 673–680.

[64] Samonas, S., Coss, D. (2014) The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information Systems*, (Security), 10, 21–45.

[65] Sapronov, K. (2020) The human factor and information security. Kaspersky Sausalito, C. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. *Cybercrimme Magazine*: New York, USA.

[66] Sax, L.J., Gilmartin, S.K., Bryant, A.N. (2003) "Assessing response rates and non-response bias in web and paper surveys, *Research in Higher Education*, 44, 4, 409–431.

[67] Shahri, A.B., Mohanna, S. (2016), The Impact of the Security Competency on Self-efficacy in Information Security for Effective Health Information Security in Iran, *The Advances in Intelligent Systems and Computing*, 445, 51–65.

[68] Singh, S., Hess, T. (2017)," How chief digital officers promote the digital transformation of their companies. *MIS Quarterly Executive*, 16.

[69] Siponen, M., Baskerville, R., Kuivalainen, T. (2005)," Integrating security into agile development methods. In: Proceedings of the of HICSS.

[70] Sohrabi, N., Von Solms, R., Furnell, S., Elizabeth, P., Africa, S. (2016) *Information security policy compliance model in organisations. Computers and Security,* 56, 1–13.

[71] Soomro, Z.A., Shah, M.H., Ahmed, J. (2016) Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36, 215–225.

[72] Stewart, H. (2020). Information technology and cyber security unplugged. The Interrelationship Between Human Technology and Cyber Crime Today, English edn, Rohhat 4 (edited by M. M. Beyerlein, D. A. Johnson & S. T. Beyerlein). Elsevier Science & Technology Books: Amsterdam. LTD 2020.

[73] Stewart, H. (2022) The hindrance of cloud computing acceptance within the financial sectors in Germany. *Information and Computer Security*, Vol No. ahead-of-print., 30, 206–224 https://doi.org/10.1108/ICS-01-2021-0002.

[74] Stewart, H. (2022) A systematic framework to explore the determinants of information security policy development and outcomes. Information and Computer Security, Vol No. ahead-of-print.

[75] Stewart, H. (2022) Security versus Compliance: An Empirical Study of the Impact of Industry Standards Compliance on Application Security. *International Journal of Software Engineering and Knowledge Engineering*, 32, 363–393 [DOI: 10.1142/S0218194022500152].

[76] Stewart, H., Jürjens, J. (2017) Information security management and the human aspect in organisations. Information and Computer Security, 25, 494–534 [DOI: 10.1108/ICS-07-2016-0054].

[77] Stewart, H., Jürjens, J. (2018) Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*, 26, 109–128 [DOI: 10.1108/ICS-06-2017-0039].

[78] Terglav, K., Konecnik Ruzzier, M.K., Kaše, R. (2016) Internal branding process: Exploring the role of mediators in top management's leadership–commitment relationship. *International Journal of Hospitality Management*, 54, 1–11 [DOI: 10.1016/j.ijhm.2015.12.007].

[79] Thorwat, S.R. (2018) ICT in higher education: Opportunities of urban colleges and challenges of tribal colleges, international research. J*ournal of Multidisciplinary Studies*, 1–6.

[80] Walsham, G. (2006) Doing interpretive research. European Journal of Information Systems, 15, 320–330 [DOI: 10.1057/palgrave.ejis.3000589].

[81] WEF & W. (2019). The Global Risks Report 2019. World Economic Forum Switzerland: Geneva.

[82] Witmer, D.F., Colman, R., Katzman, S.L. (1999) From paper-and-pencil to screen-and-keyboard: Towards a methodology for survey research on the Internet. In: Doing Internet Research: Critical Issues and Methods for Examining the Net. London (edited by S. Jones). *SAGE*, p. 145–161.

[83] Zoto, E., Kowalski, S., Lopez-Rojas, E.A., Kianpour, M. (2018) Using a socio-technical systems approach to design and support systems thinking in cyber security education, 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18), p. 123–128. Tallinn]- Estonia: 4th International Workshop on Socio-Technical Perspective in IS development (STPIS'18).

APPENDIX

Acronyms	
IS/IT	Information Systems/Information Technology
ICT	Information and Communications Technology
RQ	Research Question
CIA	Confidentiality, Integrity, Availability
LDA	Latent Dirichlet Allocation
SM	Security Misperception
NFC	Nine-Five-Circle
ETVR	Evaluation of Threat Vulnerability and Risk
CSS	Cybersecurity Strategy
SSE	Secure System Engineering
ST&E	Security Testing and Evaluation
PM	Protective Monitoring
SATI	Strategic Advanced Threat Intelligence
IRR	Incident Response and Remediation
DSS	Digital Strategy Security