Ulrik Sagelvmo

An Inquiry into the Nature and Causes of Misapprehension between the Server Room and Boardroom

Misapprehension between the Server Room and Boardroom

Master’s thesis in Experience-based Master in Information Security
Supervisor: Ivar Kjærem
Co-supervisor: Geir Olav Dyrkolbotn
June 2023

Master’s thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

AI generert

NTNU
Norwegian University of
Science and Technology

Ulrik Sagelvmo

An Inquiry into the Nature and Causes of Misapprehension between the Server Room and Boardroom

Misapprehension between the Server Room and Boardroom

Master's thesis in Experience-based Master in Information Security
Supervisor: Ivar Kjærem
Co-supervisor: Geir Olav Dyrkolbotn
June 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Preface

I am deeply grateful to my supervisor, Ivar Kjerem, for his unwavering support and guidance throughout this work. Special thanks to Geir Olav Dyrkolbotn for believing in my thesis suggestion and serving as the co-supervisor. I would also like to express my heartfelt appreciation to Chrysoula Kielland for validating the statistical analysis. Your contributions have been invaluable.

This thesis, part of the Experience-based program in cybersecurity at the Norwegian University of Science and Technology (NTNU), has been a demanding yet rewarding journey. Balancing this undertaking with full-time employment has tested and strengthened my resilience and tenacity.

The study, conducted in Norway with primarily Norwegian participants, offered unique insights into cybersecurity. The contributions of these participants have been instrumental in shaping this research, and I am profoundly grateful for their input.

I also desired to explore the potential possibilities offered by artificial intelligence, encompassing its positive contributions and gaining insights into its weaknesses. Consequently, during this project, I experimented with various applications utilizing artificial intelligence as an additional resource for the assignment. It is important to note that I have not entirely relinquished the work to artificial intelligence, but rather used it as a source of guidance and suggestions for improvement.

The completion of this thesis marks not just the end of an academic journey, but the beginning of a new phase where I can apply the acquired knowledge to the field of cybersecurity. I hope this work provides valuable insights and encourages further exploration in this crucial field.

Abstract

This thesis critically explores the discord between executive leadership and cybersecurity professionals in the era of rapid technological advancement. It highlights the necessity for an improved dialogue rooted in mutual understanding to bridge the knowledge gap and aid the strategic decision-making process. Amid rising cybersecurity threats, this work underscores the crucial role of informed decision-making that comprehends the broad, transdisciplinary nature of cognitive, social, business, and cyber realms and how these facets should be integrated to guide executive and operational business decisions.

By triangulating grounded theory with gathered data from an open-source strategic cybersecurity decision-making game developed by this thesis. The papers seek to shed light on the intricate dynamics between executive leaders and cybersecurity professionals, focusing on how the transdisciplinary nature of cybersecurity complicates strategic decision-making—identifying what information is of most value to the strategic decision-making process, laying the foundation for well-informed decisions. Further, this research examines the cybersecurity expert's struggles to define precise information requirements for decision-making. Their role is to protect the organisation from various cyber threats and effectively convey the nature of these threats and appropriate countermeasures to the boardroom. This communication barrier often hampers the realisation of well-informed strategic decisions, thereby increasing organisations' vulnerability.

The thesis display an emerging science delving between the cyber domain and cognitive theory tied to decision-making. Due to the limited research and low sampling of the game, no definitive findings tied to what information requirements benefit the strategic decision-making process are evident. However, the thesis introduces the socobertech layer, a critical stage in the conveyors encoding and forming of messages to a receiver or strategic decision-maker to facilitate well-informed decision-making. Additionally, the paper provides a foundation for further research into this emerging transdisciplinary field.

Sammendrag

I en æra med rask teknologisk utvikling, tar denne avhandlingen et kritisk blikk på de bakenforliggende årsakene til at feiltolkninger oppstår mellom toppledelsen og cybersikkerhet eksperter. Oppgaven fremhever behovet for forbedret dialog basert på gjensidig forståelse og tette kunnskapsgapet for å best støtte den strategiske beslutningsprosessen. I møte med en voksende trusel fra cyberdomenet, understreker dette arbeidet den avgjørende rollen til informert beslutningstaking som forstår den brede tverrfaglige naturen og samspillet mellom kognitive, sosiale, forretningsmessige og cybertekniske domener, og hvordan disse aspektene bør integreres for å veilede, utøvende og operasjonalisere forretningsbeslutninger.

Ved å triangulere databasert teoriutvikling med data samlet inn fra et strategisk beslutning cybersikkerhetsspill med åpen kildekode, utviklet av denne avhandlingen, søker oppgaven å belyse den komplekse dynamikken mellom toppledere og cybersikkerhets profesjonelle, med fokus på hvordan den tverrfaglige naturen til cybersikkerhet kompliserer strategisk beslutningstaking. Avhandlingen ønsker å identifiser informasjon som er verdifull for den strategiske beslutningsprosessen, og som legger grunnlaget for godt informerte beslutninger. Videre undersøker avhandlingen cybersikkerhets-ekspertenes kamp for å definere presise informasjonskrav for beslutningstaking. Deres rolle er ikke bare å beskytte organisasjonen mot forskjellige trusler, men å formidle omfanget og risikoen knyttet til disse truslene og passende mottiltak til styret. I denne formidlingen er det gjerne en kommunikasjonsbarrieren som hindrer realiseringen av velinformerte strategiske beslutninger, noe som øker organisasjonenes sårbarhet. Noe denne avhandlingen ønsker å belyse.

Oppgaven viser en fremvoksende vitenskap som studerer forholdet mellom cyberdomenet og kognitiv teori knyttet til beslutningstaking. På grunn av den begrensede forskningen og lav oppsluttning rundt spillet, er det ikke tydelige funn knyttet til hvilke informasjonskrav som er gunstige for den strategiske beslutningsprosessen. Imidlertid introduserer avhandlingen socobertech-laget, et kritisk steg i avsenderens forming av budskap til en strategisk beslutningstaker for å tilrettelegge for godt informert beslutningstaking. I tillegg gir avhandlingen et grunnlag for videre forskning innen dette fremvoksende tverrfaglige feltet.

Contents

Figures

Tables

Code Listings

Acronyms

AI Artificial Intelligence. 67

APT Advanced Persistent Threat. 45

BIA Business Impact Analysis. 69

CEO Chief Executive Officer. 66

CI Confidence interval. 56, 61

CIO Chief Information Officer. 66

CIRA Conflicting Incentives Risk Analysis. 44

CISO Chief information security officer. 46

COO Chief Operating Officer. 36

CSA Cyber Situational Awareness. 16, 95

CSF Cybersecurity Framework. 5, 51

CSMS Cybersecurity Management System. 44–46

ER Experimental Research. xi, 19, 20, 25–29, 37, 41, 49, 63, 68, 70

GTS Grounded Theory Study. xiii, xiv, 19–26, 29, 41–43, 46, 48, 63, 65–67, 69, 70, 141–143

ICT Information and Communications Technology. 5, 12, 14, 16

IP Intellectual Property. 14

ISMS Information Security Management System. 16, 42, 44

ISO International Organization for Standardization. 42, 44

IT Information Technology. 6, 7, 12, 14–17, 48

KPMG Klynveld Peat Marwick Goerdeler. 1

NCSC National Cyber Security Centre. 40

NIFU The Nordic Institute for Studies of Innovation, Research and Education. 1

NIST National Institute of Standards and Technology. xiii, 5, 7, 40, 42, 44, 51, 142

NS Not significant. 61

NSM The Norwegian National Security Authority. 1, 2, 5, 7, 8, 14, 16, 40, 42, 44, 71

NTNU Norwegian University of Science and Technology. xiii, 5, 20, 21, 29, 85, 95

RMF Risk Management Framework. 8

SANS SysAdmin, Audit, Network, and Security. 2, 14, 15, 44

SIPOC Suppliers, inputs, process, outputs, and customer. 14

SMB Small And Midsize Business. 44

SME Subject-matter Experts. 17

SP Special Publications. 5

TTPs Tactics, Techniques, and Procedures. 45

Glossary

Best practice a procedure or approach that has been demonstrated, through research, experience, historical evidence or other means, to yield optimal outcomes. It is typically established or standardized, and suitable for widespread adoption to achieve desired results. Best practices are often regarded as effective solutions to common challenges, and are regularly updated to reflect changing circumstances and evolving knowledge [1]. 12, 17

Business and management level is responsible for how the organisation operationalizes the decisions made by the executive level. Ensuring that policies, procedures, and controls are effectively implemented and enforced throughout the organization. They are responsible for identifying potential risks within their departments, allocating resources to address these risks, and communicating any relevant information to both the executive and tactical levels. 7–9, 12, 27, 48, 71, *see* operational level

Cyber refers to both information, communications, and computer networks [2]. 1, 2, 16, 42, 43, 66, 69

Cyber domain See Cyberspace. xi, 2, 3, 13, 18, 20, 23, 42, 67, 70

Cyber resiliency The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment [3]. xix, 71

Cyber Situational Awareness is a subset of situational awareness focused on understanding the cyber environment by integrating data from various technical and cognitive sources, such as IT sensors and human intelligence, to detect suspicious or interesting activities in cyberspace, comprehend their implications, and predict future events to inform decision-making [4]. 2, 16, 71

Cyber-resilient See cyber resiliency. 1

Cybersecurity the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets [5] [6]. xi, 1–3, 12, 13, 15, 16, 18–20, 26, 37, 42–48, 65–71, 73, 74

Cyberspace a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers [7]. xix, 16, 23, 43

Decipher how effectively the expert identifies the problem's core and gets to the root of the issue to find a solution. This metric evaluates the ability to think critically and analytically in the face of challenges related to cybersecurity. 15

Deliver how well the expert follows through and maintains the new functionality introduced. This metric evaluates how well security improvements are sustained over time and that the organization's security posture continues to improve. 15

Develop how well the expert can introduce new functionality that improves the organization's security posture. This metric assesses the creativity and innovation in developing new solutions to address cybersecurity challenges. 15

Executive level responsible for the high-level strategic management and decision-making. This includes setting the overall mission priorities, defining risk tolerance, establishing organizational values, and managing the budget for the organization. The executives are typically responsible for the overall direction of the organization and ensuring that the organization's objectives align with its overall mission and goals [8]. xxii, 7, 9, 11–13, 27, 44, 48, 71, *see* strategic level

Experimental Research a study in which participants are randomly assigned to groups that undergo various researcher-imposed treatments or interventions, followed by observations or measurements to assess the effects of the treatments [9]. 19

Grounded Theory Study a type of qualitative research aimed at deriving theory through the use of multiple stages of data collection and interpretation [9]. xi, 19, 21, 65–67

Lead how well the expert develops the employees within the organization and inspires others to embrace and prioritize cybersecurity. This metric evaluates the leadership skills and ability to engage and motivate others to support the organization's security goals. 15

Nettskjema A web-based survey tool developed by the University of Oslo [10]. 29–31, 35, 49, 50

NIST SP 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy [11]. 8

NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View [12]. 8

NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations [13]. 8

NS 5814 Requirements for risk assessment [14]. 8, 9, 11

Operation level is responsible for executing implementation, maintenance, and daily operations within the organization. This level focuses on carrying out day-to-day tasks and activities, while also reporting progress, changes to assets, and any emerging threats or vulnerabilities to the higher management levels for review and guidance. 8, 12, 48, *see* tactical level

Operational level constitutes the intermediate layer within an organization's hierarchy, positioned between the strategic level and the tactical level. It is responsible for overseeing day-to-day operations, aligning projects, business tasks, assignments, and work efforts with the strategies and policies established by the executive level. This level plays a crucial role in ensuring that the organization operates efficiently and effectively, in line with the strategic objectives and goals set forth by the top management. 6–9, 25, 51, *see* business and management level

Oria NTNU research search engine and database. 21, 22, 24

Risk uncertainty related to whether an unwanted event will occur and what consequences it may have [14]. 1–3, 7–9, 11, 16, 21, 44, 57, 66, 69

Security culture (cyber) encompasses ingrained behaviours, values, and beliefs within an organization that promote compliance with security policies, foster an understanding of the cautious implementation of requirements, and maintain an environment of trust and integrity [15]. 15, 16, 36, 40, 69

Sociotechnical refer to the intricate interplay and interdependence between human actors and information and communications technology (ICT) operations. The performance, actions, and decisions of individuals hold significant sway over various aspects of complex sociotechnical systems. The sociotechnical aspect is therefore recognizing the way humans interact with technology [16] [17]. 17–19, 27, 41, 42, 74

Socobertech is a term introduced in this thesis that expresses the transdisciplinary field of combining social, cognitive, cyber and technical science. 43, 63, 66, 70, 74

Strategic decision-making A decision of such a nature that it depends on the involvement of the executive level at the strategic level. 2, 3, 7, 8, 12, 18, 20, 27, 41, 42, 44, 46, 63, 65–71, 73, 74

Strategic level focuses on development and implementation of long-term plans and goals that align with the overall vision and mission of the organization. At this level, decisions are made about allocating resources, defining priorities, and determining risk tolerance. The focus is on ensuring that the organization is well-positioned to achieve its objectives and respond to changing conditions in its environment [18]. xxii, 6, 7, 13, 25, 51, 68, *see* executive level

Subject-matter Experts is an individual with extensive knowledge, experience and expertise in a particular field or subject. Often possesses a deep understanding of theory, concepts, principles and practices within their field or subject. 17

Tactical level carries out daily operations in alignment with the organization's objectives and goals. This level focuses on implementing, monitoring, and maintaining exceptional quality in deliverables and services, ensuring that the organization's performance consistently meets or exceeds expectations. The tactical level employs expert knowledge to solve complex and technical challenges for the organization. 6–8, *see* operation level

Twine Open-source game tool [19]. 28, 30, 31, 37, 49

Chapter 1

Introduction

This chapter introduces the thesis and outlines its background, justification, motivation, and benefits. The work is built upon prior research in the field, and the chapter discusses the scope and limitations of the study. Drawing upon this context, the research questions and planned contributions are defined. Finally, a brief description of the thesis structure is provided to offer readers a comprehensive overview of the upcoming sections.

1.1 Background

As a cybersecurity consultant, I guide clients regarding their security posture. This typically requires engaging with organisational leadership since enhancing cybersecurity posture, resilience and maturity requires a concerted effort and commitment from leadership. A significant challenge in the field of security is communicating the imperative for change to leadership teams who may lack sufficient knowledge of the cybersecurity domain yet are ultimately responsible for overseeing their organisation's security posture in today's constantly-evolving threat landscape.

In 2019, the Norwegian ministries recognized the importance of ensuring that Norway possessed the necessary cybersecurity competence to enable organisations to effectively adapt to the evolving risk environment [20]. This strategic initiative was prompted by findings from various investigations, including those conducted by the Lysne Committee, KPMG and The Nordic Institute for Studies of Innovation, Research and Education (NIFU) [21–23]. The investigations highlighted a range of challenges, including a projected shortfall of 4,100 cybersecurity experts by 2030, insufficient understanding of Cyber risks by organisational executives, and the societal, economic costs of a general lack of cybersecurity competence that prevents the development of a cyber-resilient society.

In its 2023 report on Cyber competence in Norway, the Office of the Auditor General (OAG) criticized the Norwegian ministries for inadequate follow-up on the 2019 cybersecurity strategy [24]. The The Norwegian National Security Authority (NSM) has also warned that the country's lack of security consciousness poses a significant threat to national security [25].

Recognizing the Cyber competence shortage in Norway, exploring ways to optimize existing resources is necessary. One approach is to enhance the security awareness of executive leaders, which requires cybersecurity professionals to change the way communication is done with leaders and facilitate for strategic decision-making in a more efficient manner [25].

1.1.1 Keywords

Strategic decision-making, cybersecurity, risk management, business communication system operations and management, asset, threat and vulnerability assessments, cyber situational awareness.

1.1.2 Problem description

Acknowledging the limited familiarity of some executive leaders in the Cyber domain, cybersecurity experts face the challenge of enabling these strategic decision-makers to make well-informed decisions for their organisations. This thesis, therefore, raises the following problem statement: *How can cybersecurity professionals effectively communicate complex cybersecurity issues to non-technical leaders and facilitate their understanding of potential risks and implications, to improve strategic decision-making?*

Continuation of existing work

This master's thesis is "*standing on the shoulders of giants*", and a continuation of the master's thesis written by Tiril Ligaya Tinde under the name "*Cyber Threat Information Requirements for strategic decision-making*" [26]. A bachelor's project read during the grounded theory study by Artūrs Umbraško, Kacper Lewandowski and Danie Dahl named OS Runner combined with SysAdmin, Audit, Network, and Security (SANS) *Cyber42* Security Leadership Simulation, has been influential during the experimental research phase and development for the decision-making game in this master's thesis [27, 28]. Lastly, this thesis is built on the project "*The benefit of value assessments in strategic security decision-making and management of operations*" delivered by the author of this thesis in the course 'IMT4205 Research Project Planning', a precursor for the master's thesis course [29].

1.2 Scope and limitations

The goal of this master's thesis is to investigate what aspects of cybersecurity should be prioritised to enable strategic decision-makers to make well-informed decisions regarding the Cyber domain. While the topic of cybersecurity and decision-making is broad, this thesis narrows the focus to compare the value of asset assessments versus threat and vulnerability assessments.

The study is conducted within a Norwegian context. However, the findings and insights presented in this paper may also be relevant and applicable to other contexts and countries, given the global nature of the Cyber domain and human behaviour.

1.3 Research questions

The priori hypothesis of this thesis is that asset assessment provides a stronger foundation for strategic decision-making and operation management than a threat or vulnerability assessment, particularly for business executives who are making decisions in the context of the Cyber domain. It should be noted that asset, threat, and vulnerability assessments must be combined to describe the risk to leadership. However, this thesis posits that the primary focus should be on assets to facilitate informed decisions. To address this hypothesis, the project poses three research questions (**R1-R3**).

R1: What information related to cybersecurity is key for strategic
decision-making and management of operations based on ground theory?

> *Research question R1 should clarify if there is evidence in grounded theory that asset assessment facilitates an improved strategic decision-making compared to threat and vulnerability assessments.*

R2: What cybersecurity factors are important for strategic decision-making and management of operations observed in the game?

> *Research question R2 should identify if there is evidence that an increase in focus on asset assessment provides improved strategic decision-making compared to threat and vulnerability assessments in the cyber game.*

R3: How do key cybersecurity information for strategic decision-making and management of operations overlap with cybersecurity factors from the game?

> *Research question R3 should identify if there is any merit to the hypothesis by comparing the result of research questions R1 and R2.*

1.4 Thesis outline

The structure of the thesis is as follows:

2 Theory: The theory chapter lays the groundwork for this thesis, offering a comprehensive overview of the key concepts and theoretical foundations relevant to the research questions.

3 Methodology: outlines the research design and methods used in this thesis, including the data collection process and analysis methods. It explains how the research questions will be addressed and justifies the chosen approach.

4 Analysis: explores the results in detail, discussing key themes and trends and drawing on relevant literature and theory to provide a deeper understanding of the data. The analysis chapter also provides insights into the research questions and hypotheses.

5 Discussion: interprets the findings presented in the analysis chapter and connects them to the research questions and the theoretical framework established in the theory chapter.

6 Conclusion: summarises the study’s key findings, highlighting the main contributions and insights generated from the research. It also discusses the implications of the results for the research questions and the broader field, including potential limitations and areas for further research.

Chapter 2

Theory

As a master's thesis on information security management, this paper's theoretical framework is not exhaustive. However, it is highly complex and interrelated, requiring a transdisciplinary perspective and a strong understanding of information security principles. This chapter provides a working understanding of these subjects. Note that this work is partially a continuation of the preliminary project [29].

2.1 From the server room to boardroom

This master's thesis in Information Security is an experience-based program offered by NTNU, specializing in security management [32]. One of the key competencies expected of a security expert is understanding the place of information security and its role within a business or organisation. However, there are a lot of different views and research from other sectors and industries on how to optimize and run an organisation and its digital infrastructure and systems. This paper captures the most basic and standard theory among these with a basis from NIST (*You can read more about why in table 2.1*).

National Institute of Standards and Technology (NIST), plays a key role in developing essential measurement solutions [30]. Significantly, for this thesis, the organisation is also responsible for establishing standards and promoting technological advancements that strengthen information security. Additionally, NIST Special Publications (SP) 800-series is commonly adopted in the US and growing in popularity with NIST Cybersecurity Framework (CSF) outside of the United States [31]. It has influenced NSM "basic principles for ICT security" (grunnprinsipper for ikt-sikkerhet) and provides a glossary that covers all topics in this paper.

Table 2.1: Why NIST is used for this paper

2.2 The boardroom

A business can be effectively structured into a hierarchical organisation to fulfil several objectives, such as establishing clear lines of authority, enhancing decision-making processes, promoting accountability, encouraging specialization and expertise, and fostering coordination and collaboration. Such an organisation also contributes to the stability and predictability

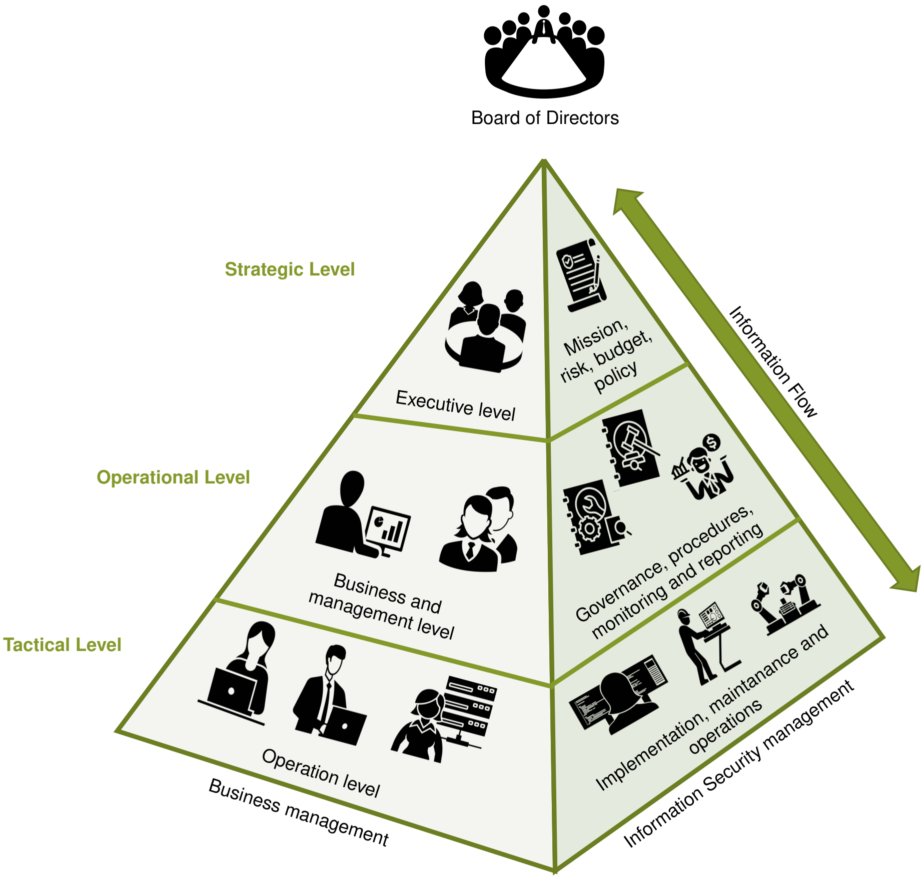

Board of Directors
Strategic Level
Operational Level
Tactical Level
Executive level
Mission, risk, budget, policy
Business and management level
Governance, procedures, monitoring and reporting
Operation level
Implementation, maintanance and operations
Business management
Information Security management
Information Flow

Figure 2.1: Generic business structure [18, 34]

of the business [33]. In this paper, we present a generic
organisational hierarchy, as depicted in Figure 2.1, which is based on NIST CSF "*Information and Decision Flows within an organisation*". The business is divided into three general levels: the strategic level, operational level, and tactical level. The left side of the pyramid in Figure 2.1 represents the business management aspects of the organisation, while the right side delineates the specific roles each level plays in information security management [29].

Before delving into the business structure employed in this paper, it is crucial to emphasize the findings of *Withman* and *Mattord* in their book *Management of Information Security*. They assert that the organisation and management of businesses can vary significantly, particularly in digital security, where differences exist between sectors and within the same sector [35]. The *International Labour organisation* identifies 22 distinct industries and sectors on their website [36], each of which possesses unique characteristics based on their history, field of knowledge, and reliance on digital systems. Moreover, most businesses structure their organisations to optimize their services and products cost-effectively [37], which implies that they tailor their IT systems to their business models. *Håkon Bergsjø* suggests that, while IT systems may share core similarities across sectors, it is the history, experiences, standards, competencies, and specific operations of a business or sector that significantly influence their approach to digital security [29, 38].

This master's thesis aims to achieve a high degree of general validity; thus, a generic description of business organisation is utilized. NIST outlines a generic organisational model in the publication *Managing Information Security risk: organisation, Mission, and Information System View* [12], which is also adopted by NSM [34]. This paper employs a model (Figure 2.1) that combines the frameworks developed by NIST and NSM to enhance general validity and encompass all relevant factors for this master's thesis. Nevertheless, readers should remember that this structure is not exhaustive and has been tailored to suit digital security [29].

The **strategic level**, also referred to as the executive level, C-level, or policy level, constitutes the highest echelon of an organisation's hierarchy. This level comprises senior executives concentrating on organisational risk and providing direction through priorities, risk assessments, and budget allocation [18]. These executives are accountable for the organisation's overall performance and are responsible for its strategic decision-making. As depicted in Figure 2.1, the executive level reports to the board of directors, a group of individuals who are often elected or appointed to govern the organisation. The board of directors is accountable to the organisation's shareholders, responsible for safeguarding and enhancing shareholder value by making decisions that foster the organisation's growth and profitability [39]. In the context of information security management, the role of the executive level is to establish the organisation's mission priorities, risk appetite, budget, and overarching policies. They convey their intentions, priorities, available resources, and risk tolerance to the operational level [18] while simultaneously receiving reports and feedback from the business and management level [29].

The **operational level** plays a vital role in an organisation's hierarchy, acting as a bridge between the strategic (executive) level and the tactical (operation) level. This level is responsible for reporting essential information to the executive level, emphasising business risks, risk profile changes, and emerging risks that necessitate oversight and governance. While continuously monitoring and evaluating how the organisation is aligned with their goals and objectives.

The role of the operational level in information security management is to oversee the day-to-day operations, monitor the effectiveness of the risk management activities, and adjust them as needed to address changes in the risk landscape. The business and management level is responsible for developing and implementing procedures based on the policies set by the executive level, governing the organisation and ensuring that they are consistent in their risk management approach across the organisation [29].

The **tactical level** plays a crucial role in implementing and adhering to the procedures and guidelines established by the operational level. It is important to note that while the operation level oversees tactical implementation, operation, and maintenance, the operational level remains accountable for the outcomes. The tactical level focuses on executing daily operations in alignment with the organisation's objectives and goals, as directed by the operational level [29].

In addition to implementing, monitoring, and maintaining exceptional quality in deliverables and services, the tactical level ensures that the organisation's performance consistently meets or exceeds expectations. By applying expert knowledge and specialized skills, the tactical level addresses the organisation's complex and technical challenges, contributing to its overall success. This level collaborates closely with the operational level to ensure seamless integration of processes, systems, and activities across the organisation.

In the information security management context, the tactical level implements the security controls required to mitigate organisational risk, set by the business and management level. Often developing guidelines and operational procedures to ensure consistency and adherence to laws, regulations, and organisational policies and procedures.

2.2.1 Risk

The primary objective of risk management is to attain security, which can be defined as the real or perceived state of absence from unwanted events, fear, or danger [40]. However, achieving absolute security is an unrealistic goal within an organisational context. Risk management and implementing security and safety measures to mitigate the probability of unwanted events constitute the preferred course of action. A comprehensive risk assessment process is crucial to gain insight into these events [29].

The *NIST Risk Management Framework (RMF) for Information Systems and organisations* (NIST SP 800-37) offers a flexible yet comprehensive set of guidelines for implementing a risk-based approach to security management [11]. Although primarily designed to be used in conjunction with NIST SP 800-53 (*Security and Privacy Controls for Information Systems and organisations*), it can be adapted to accommodate any control framework [13]. However, NIST SP 800-37 is oriented towards information systems and may inadvertently lead organisations to focus on compliance or security controls, even when utilized alongside NIST SP 800-39 (*Managing Information Security Risk: organisation, Mission, and Information System View*) [41] [29].

Considering the focus of this paper on strategic decision-making, a more appropriate framework would be *NS 5814: Requirements for Risk Assessment* [14], an updated standard from 2021, compared to NIST SP 800-37 from 2018 and NIST SP 800-39 from 2011. Widely adopted in Norway, NS 5814 is recommended by NSM and builds upon international risk management frameworks, such as ISO 27005, ISO 31000, and NIST 800-37 and 800-39 [29].

The paper will reference the risk management model of NIST SP 800-39 but utilize the risk assessment model outlined by NS 5814. As risk assessment is the central focus of this paper, it will provide a more detailed description of this aspect. An overview of the risk assessment process from NS 5814, including all steps, is illustrated in Figure 2.2 [14, 40].

Risk assessment

Standards Norway defines risk in NS 5814 as "*uncertainty related to whether an unwanted event will occur and what consequences it may have*" [14], which encompasses and extends the definition used by NIST SP 800-37, 39, and 53 (*Risk: A measure of the extent to which a potential circumstance or event threatens an entity, and typically is a function of (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.*). A noteworthy distinction is that NS 5814 incorporates uncertainty in addition to likelihood and consequence [29].

For strategic decision-makers, it is vital to understand the uncertainty inherent in the underlying data used for risk assessment. This should be done alongside evaluating the confidence of the assessment by considering the reliability and accuracy of sources [42]. Therefore, this paper uses the definition of risk set by NS 5814 [29].

To effectively understand an organisation's risks, it is imperative to follow all four steps of the risk assessment process rigorously (see figure 2.2). A critical aspect is assessing organisational risk, which involves comprehending tangible and intangible assets. Identifying these assets early in the risk assessment process is crucial to safeguard what is most important to the organisation. Consequently, the step of determining *values to be protected* is of significant importance, necessitating involvement from the executive level and potentially including input from the business and management level and the operational level as well. Without valuable assets, no risks exist, as no unwanted events would result in loss of value or wastage of assets [14] [29].

Once the organisation discerns its values, threats with the potential to cause unwanted incidents can be identified. These threats possess the capability to inflict harm on the organisation's assets. Factors such as presence, capacity, intention, history, and target selection are crucial when evaluating the threats posed to organisational values [29].

Risk analysis

The industry standard for describing risk was for long the two-factor model. Where risk was calculated as the likelihood times the consequence, this was improved upon when the three-factor model was introduced, also known as the risk triangle. Determining risk to be a product of value, threat and vulnerability. The organisation still evaluated likelihood and consequences; however, these parameters were evaluated based on the assessments of value (A), threat (T) and vulnerability (V).

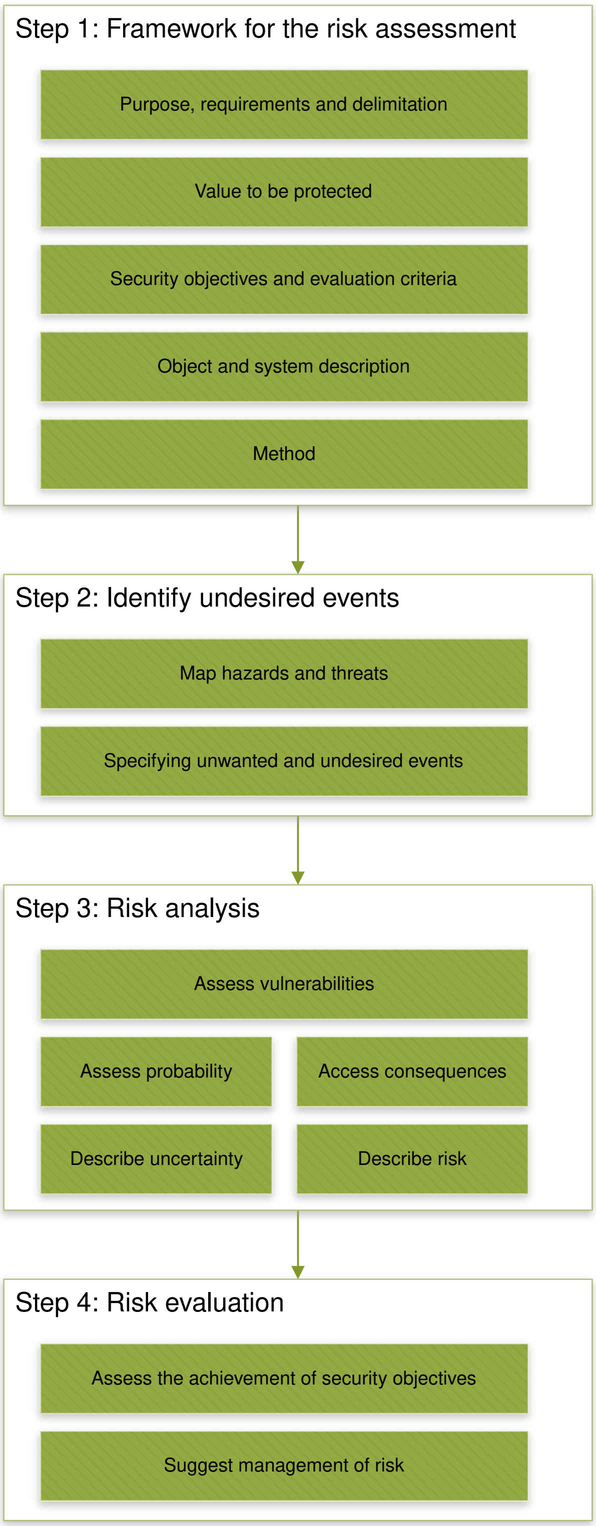

Step 1: Framework for the risk assessment
Purpose, requirements and delimitation
Value to be protected
Security objectives and evaluation criteria
Object and system description
Method
Step 2: Identify undesired events
Map hazards and threats
Specifying unwanted and undesired events
Step 3: Risk analysis
Assess vulnerabilities
Assess probability
Access consequences
Describe uncertainty
Describe risk
Step 4: Risk evaluation
Assess the achievement of security objectives
Suggest management of risk

Figure 2.2: Risk assessment process [14]

This can be mathematically expressed as [29, 43]:

$$Risk = f(A, T, V)$$

A mathematical expression of risk for an event X can be expressed through likelihood (P) times consequences (k) based on value (A), threat (T) and vulnerability (V) in the following way [29, 43]:

$$Risk = r[k(A, V|X), P(X)]$$

Note that X is given as an expression of an unwanted incident based on a threat (T) [29, 43].

Uncertainty and determining risk

Although mathematically expressing risk may seem practical, NS 5814 contends this approach is inadequate as it fails to communicate the inherent uncertainty in risk assessment. The three-factor model does not reveal the validity of the determined risk, which can lead to decision-makers basing their choices on inaccurate or flawed premises not conveyed through the risk assessment. As a result, NS 5814 argues that risk analysis must account for uncertainty, including evaluating uncertainty associated with values, threats, vulnerabilities, probability, and consequences [29].

Risk communication

During risk evaluation and subsequent decision-making, NS 5814 posits that risk is best communicated using a bow-tie diagram [14]. The strengths of this method lie in its ability to convey the immediate risk to an asset while simultaneously illustrating unwanted incidents, uncertainty, threats, vulnerabilities, mitigations, preventions, consequences, and barriers. This comprehensive representation equips decision-makers with the necessary information to make well-informed judgments. For the executive level decision-makers, as their decisions carry significant implications for the organisation while they have limited time to make these determinations [26, 29].

2.2.2 Managing risk

Following the risk evaluation, the subsequent decision involves determining the appropriate risk treatment strategy. Risk treatment strategies are typically categorized into five principles: *defence (1), transference (2), mitigation (3), acceptance (4), and termination (5)* [35]. For the scope of this master's thesis, only defence and mitigation strategies are relevant, as they necessitate management by all tiers in the organisation and require executive-level decision-making based on reports from tiers 2 and 3 (operational and tactical)[29].

A risk defence strategy aims to prevent unwanted incidents by focusing on preventative controls and barriers, corresponding to the bow-tie diagram's left side. In contrast, a risk mitigation strategy seeks to minimize the impact of unwanted incidents, concentrating on mitigating controls and barriers, as represented by the right side of the bow-tie diagram. The industry best practice has long been a combination of both strategies, employing a risk-based approach that incorporates both preventive and mitigating controls [18, 29, 34, 35].

2.2.3 Strategic decision-making

Peter Weill has defined six IT governance archetypes based on where in the organisation the responsible decision-making body is in the organisational hierarchy [44]. The six are as follows:

- **Business Monarchy** when decisions are made exclusively by the executive level.
- **IT Monarchy** when decisions are made by subject matter experts on either the business and management level or the operation level.
- **Feudal** when decisions are made in isolated business departments without considering the rest of the business.
- **Duopoly** when decisions are made by IT experts on the business and management level with one other group.
- **Federal** when decision is made by the executive level and relevant parts of the business and management level. The involvement of IT on the operation level is optional.
- **Anarchy** when decision-making is without central direction and made in silos.

When an archetype is employed, the nature of the IT decisions is often the significant factor. Questions regarding digital architecture, infrastructure, network, business application, IT investments are usually not handled by one body in the organisation. However, in regards to strategic decision-making, the IT decisions are of such a nature that they must be taken by the executive level. More often than not, it is not a business monarchy decision but rather a federal one.

2.3 The server room

As more solutions and businesses rely on ICT, the number and variety of specialities within the field are expanding. In Information Technology, experts specialise in a wide range of areas: administration, management, governance, software development, networking, web development, cloud computing, database administration, data analytics, and artificial intelligence. Among these numerous specialities, this thesis focuses on one binding domain: cybersecurity.

A cybersecurity expert is tasked with interpreting the requirements and controls stipulated by higher-level authorities, leveraging these to design and implement optimal security solutions for the organisation. Consequently, they must deeply understand the organisation's vision, mission, and goals, as well as the inherent risks, applicable laws, regulatory frameworks, and contractual obligations that influence decision-making. When a decision has substantial organisational impact, it escalates to a strategic level, necessitating involvement from the executive level. In these cases, the role of lower-level personnel pivots to providing the executive level with the necessary resources to make the most informed decision possible.

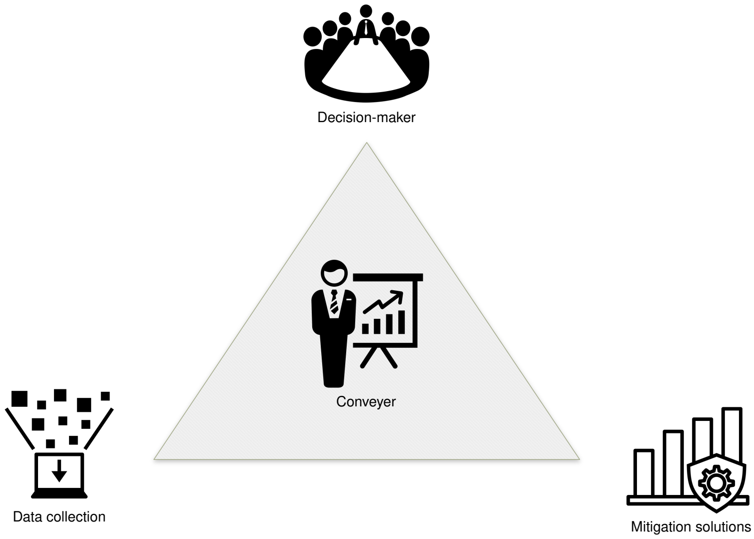


Figure 2.3: Conveying a message (Adopted to the defensive operations in the Cyber domain)[42, 45]

2.3.1 The art of conveying technical information

When the cybersecurity expert reports back to the executive level, their role transitions into that of an advisor, aiming to inform and enlighten the decision-makers. This dynamic is depicted in figure 2.3, where the role of the cybersecurity expert is labelled as the 'conveyor', responsible for informing the decision-makers.

When an expert presents information to the decision-makers, it is typical for the knowledge of the decision-makers to be considerably less extensive. Moreover, the expert, or conveyor, has likely dedicated a significant amount of time to studying the matter at hand, not only in data collection but also in evaluating potential solutions. Therefore, the expert is tasked with balancing multiple perspectives. They must explain the data collection process and the analysis results in a manner that enables decision-makers to understand the basis upon which they are making decisions. This includes informing them about the confidence level of the information - essentially, the degree to which the data can be deemed credible and reliable [42].

The dataset is typically explained first, followed by presenting potential actions or decisions to the decision-makers, as illustrated by 'mitigation solution' in Figure 2.3. To make informed decisions, the proposed solutions must be described not only in terms of their nature but also in terms of their implications for the business. This encompasses considerations such as short- and long-term effects on the organisation, whether the solution is cost-saving or necessitates increased budget and resources, if it impacts the corporate culture, and whether organisational changes are required. These are just a few examples of questions that may provide crucial information to decision-makers, depending on the nature of the decision.

Key to success

According to SANS, if the conveyor is to succeed in their task, providing the strategic decision makers with the most beneficial prerequisites for their task. The conveyor has to understand the decision-makers and their motivation. Understanding the stakeholders and power distribution. That can be done by putting the parties into a SIPOC (Suppliers, inputs, process, outputs, and customer) diagram. Then putting the necessary parties into a power interest grid. Identifying who you need to 'monitor', 'keep satisfied', 'keep informed' or 'managed closely' [37].

Strategic decision makers, such as the board of directors, are swamped, have to make rapid decisions with limited information, and run complex enterprises [37, 46]. Fundamental principles for the conveyor are to talk business and not technology, with measurable metrics that have a business impact.

2.3.2 Managing digital security

One of the challenges IT personnel face when communicating digital security to a workforce less acquainted with the digital domain is its multi-faceted nature. Digital security, as defined by the ISO 27000 series, encompasses people, processes, and technology security. The NSM has built upon the ISO 27000 standard, proposing four basic security principles: security management (1), physical security (2), personnel security (3), and Information and Communications Technology (ICT) security (4) [47]. Digital security interweaves with all these principles. While ICT security is the most obvious, given that it is what most people associate with digital security, it is not the only component. Indeed, ICT security becomes irrelevant if a threat actor can physically steal your digital data by taking the server's hard drive or if an insider decides to download Intellectual Property (IP). Similarly, an organisation lacking security management will likely falter at every stage, failing to identify its values or assets. Without understanding your risks, managing digital security can become complex. Thus, digital security forms part of all four basic principles and must be managed across physical, human, organisational, and ICT domains.

Security culture

In the article "*Defining organisational information security culture—Perspectives from academia and industry*" based on a survey with 512 respondents from industry and academia, the following comprehensive definition of information security culture is suggested:

> *Information security culture is contextualised to the behaviour of humans in an organisational context to protect information processed by the organisation through compliance with the information security policy and procedures and an understanding of how to implement requirements cautiously and attentively as embedded through regular communication, awareness, training and education initiatives.*
>
> *The behaviour over time becomes part of how things are done, i.e., second nature, due to employee assumptions, values and beliefs, and their knowledge and attitude towards and perception of protecting information assets. The information security culture is directed by the vision of senior management together with management support in line with the information security policy and influenced through internal and external factors, supported by an adequate ICT environment, visible in the artefacts of the organisation and behaviour exhibited by employees, thereby creating an environment of trust with stakeholders and establishing integrity [15, p. 19].*

This positions security culture as perhaps the most holistic measure of an organisation's cybersecurity efforts. It encapsulates all four basic security principles and integrates aspects of human behaviour, the role of management, and the maturity of the IT department [47–50].

According to SANS, there are four skills that a cybersecurity expert must utilize to contribute to building a healthy security culture [37].

- **Decipher -** how effectively the expert identifies the core of the problem and gets to the root of the issue to find a solution. This metric evaluates the ability to think critically and analytically in the face of challenges related to cybersecurity.
- **Develop -** how well the expert can introduce new functionality that improves the organisation's security posture. This metric assesses creativity and innovation in developing new solutions to address cybersecurity challenges.
- **Deliver -** how well the expert follows through and maintains the new functionality introduced. This metric evaluates how all security improvements are sustained over time and that the organisation's security posture continues to improve.
- **Lead -** how well the expert develops the organisation's employees and inspires others to embrace and prioritize cybersecurity. This metric evaluates

the leadership skills and ability to engage and motivate others to support the organisation's security goals.

2.3.3 Information Security Management System

Multiple standards and frameworks exist to help structure the approach to managing digital security. These are often referred to as Information Security Management System (ISMS); generally speaking, they contain a list of security controls to reduce risk to your organisation ICT systems. Well, know frameworks and standards including ISO 27002, NIST CSF, NIST 800-53, NIST 800-171, NSM Basic principles for ICT security 2.0, CSA CCM, COBIT, SWIFT CSCF, and PCI DSS. There also exist ISMS designed for operational security, adherence to legal requirements and dedicated to cloud security. The consensus of these frameworks is that the organisation should use an risk-based approach to security, adopted to their organisation. Implying that organisations have organisations risk assessment as an input to the ISMS. Moreover, organisations should ideally make a ISMS suited for their organisation, considering their structure, strategy, services, ICT environment and other factors that are of importance when making a ISMS. A framework-independent approach where the organisation shop organisation ween frameworks and standards is a reasonable approach, usually relying on one framework as a base. This can change if the organisation seeks organisation certification.

2.4 Cyber situational awareness

In 2014 a review of 102 articles on Cyber Situational Awareness (CSA) was analysed by *Ulrik Franke and Joel Brynielsson*, with the focus of the study being on national Cyber strategies [4]. Describing cyber situational awareness as a subset of situational awareness focused on understanding the Cyber environment by integrating data from various technical and cognitive sources, such as IT sensors and human intelligence, to detect suspicious or interesting activities in Cyberspace, comprehend their implications, and predict future events to inform decision-making [4].

CSA is, therefore, essential for the cybersecurity expert. Understanding of the current state of an organisation's Cyber environment and the ability to anticipate potential threats and vulnerabilities. Gathering, analyzing, and analysing relevant data on the organisation's network activities and potential adversaries. CSA is crucial for maintaining an effective cybersecurity posture, as it enables decision-makers to recognize and respond to potential Cyber threats, vulnerabilities, and incidents in a timely and informed manner. By understanding the Cyber environment comprehensively, organisations can better protect their digital assets, mitigate risks, and keep their critical information and systems' confidentiality, integrity, and availability. Leading to a better security culture, [51, 52].

Chapter 3

Methodology

This chapter initiates by expounding the rationale behind the methodologies employed to address the research inquiries, followed by an exhaustive account of the implementation of the methods and the research undertaking.

3.1 Research premise

The main contribution of this paper is to enable further research in the field of sociotechnical studies by addressing the gap between IT and executive decision-making. Prior research has involved interviewing subject-matter Experts SME, who provided answers based on the assumption that all necessary resources were available and their ideas were fully recognized. However, such information may not be applicable in real-world situations where best practices are often known, but limited resources and time constraints can hinder their implementation. Therefore, this study aims to provide a more nuanced understanding of the challenges faced by executives in balancing information security needs with practical constraints in the business environment.

In recent years, research has been conducted to investigate the significance of privacy and security to individuals. However, several studies have demonstrated a cognitive dissonance between what people report and their actual behaviour in relation to these concerns [53–57]. When we combine this with the *marginal costs* mistake described by Clayton M. Christensen in his article "*How Will You Measure Your Life?*" we get a hard environment for cybersecurity experts to operate [58]. Because the marginal cost mistake is when a person justifies for themselves that "*just this once, it's ok*", and from there get led down a path of ultimately comes at the full cost of the choice [58]. In cybersecurity, this would be if an organisation chose to not buy antivirus software because nobody will attack them and the employees are smart. When the threat from antivirus rises and the organisation now should invest in additional intrusion detection and prevention solutions, this is now a more significant investment since they did not invest in antivirus. The organisation have not yet been infected by a virus so they continue to "*just this* *once*" not invest in security. Time and time again we see that these kinds of companies are the ones exposed to attacks. According to the Norwegian Computer and Data Breach Survey 2022 the number one reason organisations exposed to security breaches reasons why they got hit is "*Random events or bad luck*". Of the organisations that have been attacked, 61% state this as their number one reason [59]. However, they have likely gone down the path of *marginal cost*.

The premise for the employment of methods in this paper is that we need to include realistic restrictions such as budget, resources and time when discussing cybersecurity. How people say they will act, is not always the way they act [60]. Lastly, people do not think incidents will happen to them and often fall into the marginal cost fallacy. Based on this premise the paper utilizes research methods that will give more insight into the sociotechnical aspects of strategic decision-making in the Cyber domain.

3.2 The choice of methods

To select the most appropriate method that aligns with the research problem and adheres to the research premises, the study consulted "*Practical Research: Planning and Design*" by *Paul D. Leedy* and *Jeanne Ellis Ormrod*[9].

3.2.1 Quantitative versus qualitative, why not both?

The initial step in developing the methodology for this thesis involved deciding whether to employ quantitative or qualitative research methods. Quantitative methods seek to explain and predict phenomena by analyzing numerical data, often through the measurement of variables and the examination of statistics and aggregated data or samples. In contrast, qualitative methods aim to describe and explain factors, focusing on the analysis of textual data to identify patterns and themes [9].

The objective of this thesis is to describe and explain the most significant factors influencing strategic decision-making when data is presented to decision-makers in the cybersecurity context. However, reaching a robust conclusion within the time frame of this thesis was assessed to be improbable. As *Tiril* highlights in her paper, the structured literature search revealed that the field of studying strategic decision-making related to cybersecurity has limited academic research available [26, p. 35-36]. To achieve a defensible conclusion, a convergent design employing mixed methods was adopted, with the aim of identifying consistencies or inconsistencies among the findings, thereby enhancing the validity of the study. The convergent design is illustrated in figure 3.1. The primary rationale behind this approach is to reinforce the potential findings in the master’s thesis, ensuring a more robust and reliable outcome.

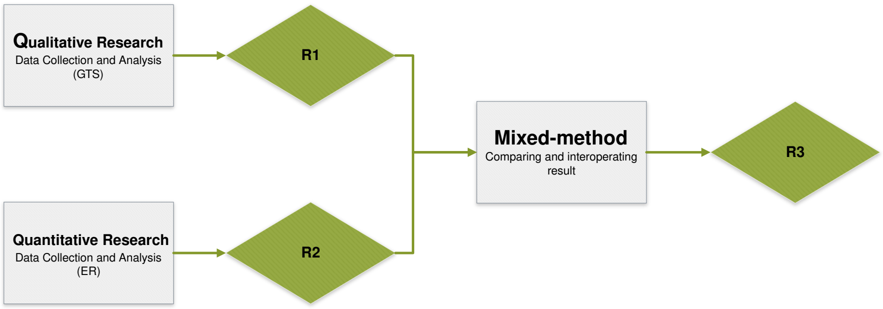

Qualitative Research
Data Collection and Analysis (GTS)
R1
Quantitative Research
Data Collection and Analysis (ER)
R2
Mixed-method
Comparing and interoperating result
R3

Figure 3.1: The convergent design of this master's thesis

3.2.2 New knowledge

Important for the thesis is to provide new knowledge to the field of cybersecurity and decision-making theory, and knowledge that can be used by future cybersecurity experts. On a topic that devolves between social science, organisational science and technical science, referred to as sociotechnical by Grethe Østby [61], this can be challenging to do because the thesis must take into consideration organisational physiology, human perceptions, technology aspect and digital security knowledge when examining the problem statement. Bringing in challenges with 3^{rd} variables and next too impossible to say anything about causality. This limits especially qualitative papers on the topic because they are in nature weak to subjective and potentially biased information [9, 62, 63]. This is backed by the paper "*The power of interpretation: Qualitative methods in cybersecurity research*" where the researchers inspected 160 papers that used qualitative methods and identified that these papers often lacked rigour and details in observations and mostly relied on interviews followed by case studies and observations [64]. This thesis will therefore employ a Grounded Theory Study (GTS) approach combined with Experimental Research (ER).

3.3 Applied research methodology

The research design employed for the master's thesis is illustrated on figure 3.2, with the four distinct phases making up the research project. Figure 3.1 illustrated the convergent design of the master's thesis, however in practice, as shown in figure 3.2 a combination of convergent and exploratory design was used. As data from the qualitative method GTS was used as input into the quantitative method ER, and compared in a convergent manner to triangulate data in phase four. A mixed-method design is well suited to address the sociotechnical challenges of the research questions. By combining qualitative and quantitative methods and using triangulation between the data. Increase the completeness of the data and compensate for weaknesses. Not shown on the illustration 3.2 is *phase 0: Research Project Planning* a preliminary project for this master's thesis project. A part of the

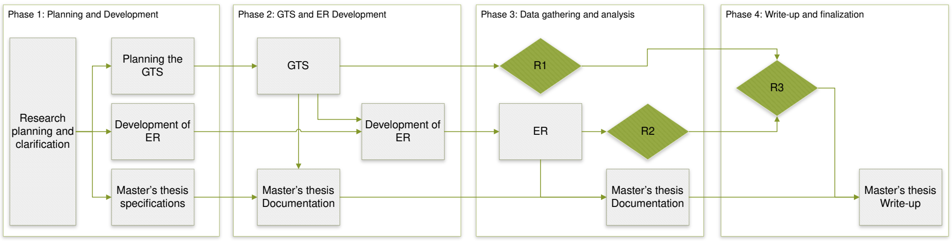

Phase 1: Planning and Development
Research planning and clarification
Planning the GTS
Development of ER
Master's thesis specifications
Phase 2: GTS and ER Development
GTS
Development of ER
Master's thesis Documentation
Phase 3: Data gathering and analysis
R1
ER
R2
Master's thesis Documentation
Phase 4: Write-up and finalization
R3
Master's thesis Write-up

Figure 3.2: Applied research methodology

subject *IMT4205 - Research Project Planning* at NTNU. Resulting in a project plan for this thesis, with an outline for a problem description and ideas for methodology. This meant that phase 1 started quickly 2nd January 2023.

Phase 1: Planning and Development started with scoping and planning the GTS, researching and developing the game for the ER. Continue the specifications of the master's thesis, clarifying and articulation the goals of the project while dividing it into principal problems and manageable research questions.

Phase 2: GTS and ER Development focused on GTS and finishing the development of the game the framework for the ER.

Phase 3: Data gaterhing and analysis started with lunching and publishing the game. While players played the game and participated in the ER, the collected data from the GTS was analysed and used to answer **R1**. Later in phase 3 data from the ER was collected and analysed to answer **R2**. Simultaneously, was documentation of the execution and results documented in the thesis.

Phase 4: Write-up and finalization begun by triangulating the analysed data from **R1** and **R2** to answer **R3**. After addressing **R3** the write-up of the project was the last standing part.

3.3.1 Grounded theory study

The main objective of the GTS was to answer **R1**. Additionally, to collect and analyse both research literature and publications on strategic decision-making in the Cyber domain. This thesis problem statement is derived from data collected in the field over multiple years. Moreover, it contradicts some academic research and commonly held assumptions about communicating cybersecurity to strategic decision-makers. The GTS refers to the idea that the theory of this thesis has emerged from the field rather than from researching literature. Not only is GTS helpful when current theories are lacking and inadequate, it has its roots in sociology, and is well suited for focusing on processes with human interactions and actions [9].

The grounded theory study collects data that have been collected in the field of information security management combined with current best practices, common standards and frameworks. The ground theory study is suited because the process, actions and interactions of people are of value. For that reason, papers with

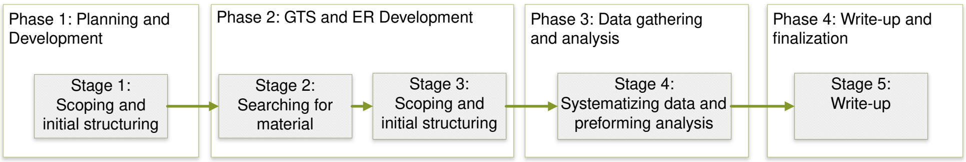

Phase 1: Planning and Development
Stage 1: Scoping and initial structuring
Phase 2: GTS and ER Development
Stage 2: Searching for material
Stage 3: Scoping and initial structuring
Phase 3: Data gathering and analysis
Stage 4: Systematizing data and preforming analysis
Phase 4: Write-up and finalization
Stage 5: Write-up

Figure 3.3: Stages in the Grounded Theory Study

case studies, interviews, and that detail real-world examples with perspectives and voices of people studied is of high value to the project. Uncovering a deeper understanding of a "real world" issue that has many dimensions and layers.

The GTS had five distinct stages illustrated in figure 3.3. A proven structure in accordance with Jill K. Jesson book on structured literature reviews suited to address research questions and is reproducible [65].

Stage 1: Scoping and initial structuring. In the first phase the goal was to identify what knowledge the project needed to obtain to answer the research questions, and how to obtain that knowledge in a rigorous manner. This included identifying search engines and databases for research litterateur and applicable publications. Types of literature that would be sought-after, and for the GTS this is wider than traditional research literature, because of the field-based nature.

The project has mostly used Oria a search service provided for students at NTNU, with access to over 209 research databases [66]. Among them are widely used databases such as *ACM, IEEE Xplore, JSTOR, ScienceDirect, SpringerLink, Scopus, and Web of Science* [67]. In addition to Oria the project used `google.com`, `scholar.google.com`, `elicit.org`, `the.iris.ai`, `semanticscholar.org`, and `researchrabbit.ai`. If other tools than Oria granted valuable hits, the paper often specifically searches for them in Oria afterwards to be able to access all content in the papers. Due to most papers being behind a subscription or paywall with only metadata and abstracts available as open source.

During stage 1 categories and sub-categories were developed for classifying the data. This is shown on 3.1. Resource type is standardised by Oria, the table lists the types that was used in the project. Associated keywords or search terms are shown in table 3.2 and lists IEEE taxonomy keywords, search terms and strings used when searching for literature on the different search tools. Category research quality indicates the substantialness of the literature by evaluating it. Considering if the paper is peer-reviewed, has a scientific structure like IMRaD, has citations from other papers, and the overall relevance of the paper. The last category indicates if the paper supports the hypothesis of the master's thesis, is neutral and does not sway in any direction or if it contradicts it.

Stage 2: Searching for material began in January 2023 after phase 0 that included an initial review of related literature. Using keywords from table 3.2 in Oria yielded thousands of hits on multiple, and some was in the millions, such as risk management with 2 447 293 hits. To be able to limit the number of hits multiple tactics were employed. Oria has functionality for filtering resource type,

Table 3.1: Category and sub-categories in the GTS

Category	**Description and sub-categories**
Title	Name of the publication
Author(s)	Name of author (s)
Year published	Year of the publication
Resource type	Article Books and book chapters Dissertation (Bachelor's, Master's, and Ph.D.) Dataset Interview Journal Report Publication Standards and frameworks
Associated keyword or search term	See table 3.2
Search tool	Oria Google scholar Elicit Iris Semantic scholar Research rabbit
Research quality	Low Moderate High
Validation of the hypothesis	Supporting Neutral Contradicting

Table 3.2: Search terms used in the GTS

Type of term	Search terms
Keywords	Cyberspace / Cyber domain Cybersecurity (Cyber security) Digital security Context awareness Cyber situation(al) awareness Cybersecurity game Information security game Decision making Decision maker Decision theory Strategic decision-making Information security management systems Risk management Asset assessment Threat assessment Vulnerability assessment Communication system security Security management Security management best practice Behavioural science cybersecurity Social cybersecurity Sociotechnical cybersecurity Business management Business management best practice Business communication system operations and management
Search strings	Decision-making related to cyber Risk assessment in cybersecurity Cybersecurity risk decision making Value-focused assessment of information system security in organisations Cyber information requirements for strategic decision-making What information related to cybersecurity is key for strategic decision-making and management of operations based on ground theory?

publication date, topics, language, relevance and more. The advanced search functions specify what field should or should not contain what search term, and combine these in a Boolean search string. This functionality was heavily used to narrow down relevant sources by tuning the filtration and adding keywords or other relevant search terms. Hits that were projected in Oria was quickly assessed by examining the research quality and relevance of the literature. Due to the vast amount of different combinations and volume of research browsed it was deemed not to be feasible to document every search. Moreover, it would provide little value. However, every search term that granted a hit that was used in the project as a result of the GTS was documented and categorized in accordance with table 3.1. The full table of documents can be viewed in appendix H.

Search tools beside Oria were used, however using only keywords for these granted hits that were not useful. Searches with the other tools, therefore, were always done by strings with multiple keywords combined. These are listed in the table in appendix H.

Stage 3: Assessment of findings and quality control encompassed a thorough review of each document that passed stage 2 and successfully completed the initial research quality control and relevance check. In this stage, the credibility, transferability, dependability, and confirmability of the literature and data were assessed. By comparing various sources of information, identifying patterns and themes, and eliminating irrelevant or low-quality data, the research's rigour and trustworthiness were ensured. The results of this stage can be found in Table 3.3.

Table 3.3: Documents included in the thesis as a result of the GTS

Resource type	References	Total
Articles	[68–72]	5
Books and book chapter	[40, 46, 73–76]	6
Dissertation	[26, 27]	2
Dataset	[77]	1
Journals	[78–83]	6
Report	[43]	1
Publication	[84]	1
Standards and frameworks	[11–14, 18, 34, 47]	7
Total		29

Stage 4: Systematizing data and performing analysis. The objective of this stage was to organize and systematically examine the data to derive meaningful insights. All documents and resources listed in table 3.3 were examined. Data and notes extracted from the documents were compared and analysed in the context of **R1**. The result of this stage was then written down in stage 5 and into the master's thesis.

Stage 5: Write-up is the most relevant stage for the thesis, and the result of this stage can be viewed in chapter 4. Answering **R1**, and providing insight into the grounded theory put into an academic context.

3.3.2 Experimental research

The primary objective of the Experimental Research (ER) was to address research question **R2**. This involved the systematic collection of field data, which was then contrasted with the data gathered from the GTS. The distinctive strength of ER is its profound capability to elucidate causal relationships among variables, allowing for an in-depth exploration of the interactions and influences that these variables exert on one another [9].

The ER methodology demonstrates remarkable proficiency in manipulating the variable pertaining to value assessment through a strategically designed experiment. This technique enables an unparalleled degree of control over the experiment's implementation, facilitating the isolation of other variables, thereby ensuring a more rigorous and systematic investigation.

However, the ER approach is not devoid of certain weaknesses. Potential limitations tied to the method include issues with representativeness, reliability, validity, and causality. Concerns regarding representativeness arise from the potential for the sample used in the experiment to inadequately reflect the broader population, thus potentially limiting the generalizability of the findings. Reliability issues may surface if the experiment, when repeated under the same conditions, fails to produce consistent results. Validity concerns could manifest if the experiment does not accurately measure what it intends to. Lastly, the issue of causality can pose challenges in determining whether the relationship between variables is indeed causal or merely correlational. The way this thesis addresses each of these will be elaborated in the following text.

Participation in the game is freely accessible to anyone who can reach the specified URL and agrees to the stated terms and services. Nevertheless, the principal target audience comprises strategic decision-makers from both the strategic level and operational level, who are encouraged to engage in the digital security management game.

Concerning reliability, the game is projected to demonstrate a substantial degree of result reproducibility, contingent upon the acquisition of an adequate sample size. The reliability of this research tool stems from its ability to generate consistent outcomes, assuming a sufficiently large and diverse participant pool.

However, potential limitations to this reliability, as well as the representativeness of the data, predominantly lie within the characteristics of the target population. The participant pool, largely Norwegian, and anticipated to be in social proximity to the author, could inadvertently introduce a bias that may constrain the generalizability of the findings to a broader or more diverse demographic.

Designing the experimental research game

The four stages of the ER paralleled the overarching phases of the research project, as depicted in Figure 3.4. The process commenced with a research phase, which also involved the high-level design of the game. During this initial stage, a broad framework for the game's structure and output was established.

With this high-level design in place, the next step involved selecting a game engine that would best support the design and meet the requirements of the ER. The choice of engine was guided by factors such as flexibility, compatibility with the design, and ease of use, among others.

In the second stage, the focus shifted to the actual development of the game, culminating in the game's publication. This phase encompassed various tasks, including programming, testing, and refining the game based on feedback.

Upon reaching a sufficient number of samples, the third stage was initiated. This stage was dedicated to data collection and analysis. The data generated by the game was meticulously collected, organized, and analyzed, with an emphasis on extracting meaningful patterns and insights.

The final stage, stage 4, involved writing up the results. These results were then integrated with the findings from the GTS. This combined analysis served to answer research question 3. This comprehensive write-up incorporated not only the findings but also a discussion of their implications, providing a full account of the research outcomes.

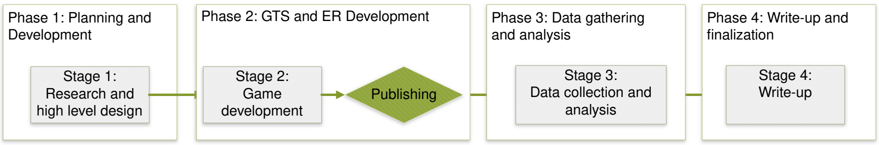

Phase 1: Planning and Development
Stage 1: Research and high level design
Phase 2: GTS and ER Development
Stage 2: Game development
Publishing
Phase 3: Data gathering and analysis
Stage 3: Data collection and analysis
Phase 4: Write-up and finalization
Stage 4: Write-up

Figure 3.4: Stages in the Experimental Research

Stage 1: Research and high-level design

In the first phase, the early research design for the game was decided. Using a *true experimental within-subjects design* in which all participants receive treatments [9]. This design fits well because a specific hypothesis is defined. The hypothesis is that a cybersecurity expert should lean towards a focus on business assets rather than threats and vulnerabilities to and in the business when a strategic decision-maker is supposed to make a decision based on his/her presentation.

Design of the game is illustrated on figure 3.5. The players n are randomly divided into two groups 50/50. Research group R_A and R_B respectively. When entering the game they will receive information Z identical for both groups. However, a seed A will be added to Z, containing additional information about assets linked to Z. This is seed A_A. Or seed A_{TV} containing additional information about threats and vulnerabilities linked to Z. They continue to play the exact same game ER with identical scoring, using their different seeds. The last step in the game is to observe the scoring S. The hypothesis is that $S_A > S_{TV}$. Implying that group R_A will outperform group R_B based on their different treatment or seed in this case. It being a causality or cause-and-effect relationship between a high score in S and the seed A_A. A being the independent variable and the S dependent variable.

The game was designed to be digital not only to be easily distributed but to manage and limit the effects from other 3^{rd}, mediating and moderating variables. As mentioned prior the human aspects and interactions with the sociotechnical nature of the subject makes this field difficult to measure. Utilizing a digital platform to tell written stories and scenarios identically to every player is therefore important, ensuring that the experience is as close to identical between every participant, and minimizing the effect of other variables. Moreover, the treatment of seed A is localized and can not possibly spread between R_A and R_B.

Based on the result of ER, the thesis seeks to answer research question **R2**. If $S_A > S_{TV}$ the hypothesis of the thesis is strengthened, if not the ER provides no merit to the value of focusing on the asset assessment for strategic decision-making.

According to *Statistics Norway*, as we entered 2018, there were 577,067 registered businesses in Norway [85]. Given this figure, it is reasonable to postulate that there exists a population R of strategic decision-makers that exceed 5000. This estimation is significant, as it aligns with the Mills Gay theory, which suggests an ideal sample size of $n = 400$ for straightforward surveys when the population R is greater than 5000 [9]. This theory provides a useful benchmark, guiding the sampling strategy for this research.

By assuming that the result will have a normal (Gaussian) distribution, the thesis employs statistical analysis to do a more precise estimate of the sample size. Achieving a statistical power of at least 0.8 with an α of 0.05 and an effect size of 0.5, the sample size must be equal to or greater than 102 (see table 3.4 for calculation). This is calculated by using a t-test as a base, suited due to requiring a lower collection of samples to answer a question related to a greater population. Quantifying the difference between the mean of the two groups ($S_A and S_{TV}$) [86].

R_A and R_B are considered independent since they are divided, and not sampled multiple times nor are the seeds A_A and $A_T V$ enhanced between the groups. The tail is set to one, because the hypothesis is that the mean of $\overline{S_A} > \overline{S_{TV}}$. A medium effect size d is used with a level of significance α set to 0.05, with a statistical power of at least 0.8. The aim is to secure a more robust sample size, ideally exceeding 102. The challenge lies in recruiting participants who possess reasonably similar backgrounds, knowledge, and experiences, which is likely to be a complex endeavour. To mitigate this issue, the game's participation criteria are open-ended, designed to enhance the sample size and thereby enrich the thesis's data foundation. For that reason the sample set and data are not limited and strictly representative of the group executive level or business and management level, but more generalized.

Stage 2: Game development

A significant part of the thesis was the development of the game. This is detailed in section 3.4 of this chapter. Enabling the reproduction of the game from scratch and following the building and technical structure of the game. This stage further

Table 3.4: Power analyses for sample size using G*Power [87, 88]

t tests	Means: Difference between two independent means (two groups)	
Analysis	A priori: Compute required sample size	
Input	Tail(s)	= one
	Effect size d	= 0.5
	α err prob	= 0.05
	Power $(1-\beta$ err prob)	= 0.80
	Allocation ratio $N2/N1$	= 1
Output	Noncentrality parameter δ	= 2.5248762
	Critical t	= 1.6602343
	Df	= 100
	Sample size group 1	= 51
	Sample size group 2	= 51
	Total sample size	= 102
	Actual power	= 0.8058986

developed the design for the game and put it into the game engine Twine. Able to meet the requirements for the ER and to build on the figure 3.5.

$$\begin{tikzcd}
 & R_A \arrow[r] & Z+\ A_A \arrow[r] & ER_A \arrow[r] & S_A \\
n \arrow[ur] \arrow[dr] & & & & \\
 & R_B \arrow[r] & Z+\ A_{TV} \arrow[r] & ER_{TV} \arrow[r] & S_{TV}
\end{tikzcd}$$

Figure 3.5: Experimental research game design

Before publishing the game, marking the end of stage 2, a pilot of the game was tested by two people without any instructions or prior information about the game. This was to evaluate if the game was understandable and easy to use. The feedback from the pilot resulted in adding a tutorial in the game and some minor changes before the game was released on `itch.io`, and the link to the game on itch was published through personal networks and social media.

Stage 3: Data collection and analysis

This stage started after no more samples were received. Specific variables and scores were pushed into a spreadsheet directly after each completed playthrough of the game. This spreadsheet was the foundation of the analysis. An essential step in the study was to evaluate the data's correctness. Ensuring no joke responses or duplicates have been received, whether anyone has just entered random answers or anything else that may indicate an invalid response. From there, statistical analysis was performed to validate the data and hypothesis testing the result.

Table 3.5: Tools that NTNU have a data processor agreement and for what classification of personal data they can be used for [90].

Tool	Public	Internal	Confidential	Highly Confidential
Zoom	Yes	Yes	No	No
Teams	Yes	Yes	No	No
MachForm	Yes	Yes	No	No
Microsoft Forms	Yes	No	No	No
Nettskjema	Yes	Yes	Yes	Yes

Stage 4: Write-up

It started with documenting the findings related to research question **R2** and then comparing **R1** with **R2** to illuminate **R3**. This stage was shared for both GTS and ER and was a part of the write-up and finalization of the research project and the master's thesis.

3.4 Development of the decision-making game

This section will describe the process from start to end in researching, developing and launching the decision-making game.

3.4.1 Choosing the tool for the game

While developing the decision-making game, several tools were evaluated for their suitability. An essential requirement was that the selected tool has a data processor agreement in place with NTNU to ensure that any collection of personal data complied with relevant Norwegian laws and regulations. Table 3.5, sourced from [89], outlines the tools currently holding such an agreement.

Unfortunately, none of the evaluated tools were found to possess the necessary capabilities required for the development of the decision-making game. Specifically, the tool would need to be able to manage multiple variables and update them accordingly, perform calculations, and handle logical conditions seamlessly and efficiently. However, Nettskjema can collect responses through the use of their provided code that can "*Embed the form on a website*", incorporating the form into a website [10]. Nettskjema was therefore chosen to collect consent and ensure informed, voluntary participation.

3.4.2 Nettskjema

Ensuring that all candidates playing the game were informed and had given their consent, Nettskjema was the tool of choice. It is a web-based survey tool that the University of Oslo develops and a tool that NTNU has a data processor agreement with [10]. A form was created using Nettskejma and embedded into the game using the code from code listing 3.1.

Appendix D describes the form and setting used. The form can be viewed in section D.1 and the settings in section D.2.

Code listing 3.1: Code used for embedding the form into the game

```
<script type="text/javascript"
src="https://nettskjema.no/static/js/external-embedding.js">
</script><iframe class="nettskjema-iframe"
src="https://nettskjema.no/a/327476?embed=1"
title="Participation␣in␣the␣strategic␣decision␣making␣game"
frameborder="0" width="100%"></iframe>
```

3.4.3 Twine

The tool used to develop the decision-making game is Twine [19]. An open-source tool with extended functionality for telling interactive, nonlinear stories that can handle variables and conditional logic. Additionally, the tool is free, easy to use and lean, can quickly be published on the web and handle multiple story formats and coding languages, and runs only locally in the browser of the player, thereby not sharing any private information [91–93].

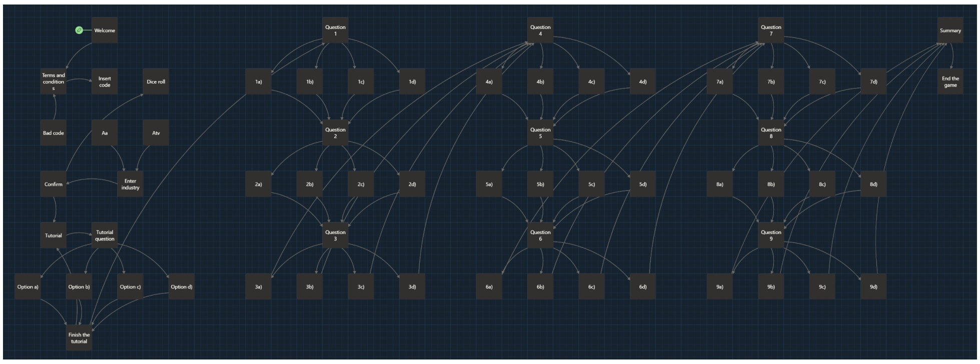


Figure 3.6: Twine passage overview

Game structure

The game can be segmented into four distinct phases, each serving a specific purpose in achieving the research objectives. These phases include the enrollment phase, where participants are registered to play the game (Nettskjema), followed by the tutorial phase, which provides an overview of the game mechanics and rules. The playing phase represents the main segment of the game, where participants engage in gameplay, and the final phase marks the game's conclusion.

Enrollment phase commences when the player runs the game and is greeted by a welcome passage. The message informs the player that the game is part of a research project, and to proceed; they must read and agree to the terms

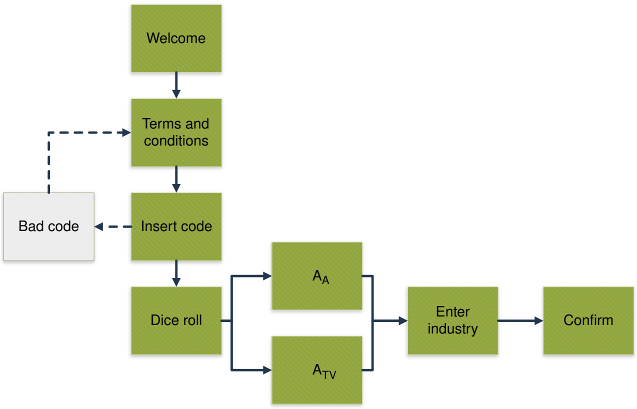


Figure 3.7: Enrollment phase

and conditions. If the player declines to agree to the terms and conditions, the game stops at this point. On the other hand, if the player agrees to the terms and conditions, they are prompted to provide a unique five-digit number that they will input into the game to continue. This process ensures that every player is informed about the research project's purpose, their involvement, their rights and privacy, and that their participation is voluntary. The thesis also uses this five-digit number to ensure that the information collected is from legitimate players by comparing it with the information in Nettskjema by date. The Nettskjema form used in the enrollment phase is included in Appendix D.1. The enrollment phase continues when the player submits their five-digit number in Twine. In the background the player is assigned a seed show on code listing 3.2 line 1. The function assigned the player randomly with either the value 1 or 2. Where 1 puts the player in the A_A seed and 2 in the A_{TV} seed as shown on code listing 3.3. The player is then promoted to download the PDF file *Trouble-free Logistics*. Depending on their seed, they will download either *Trouble-free Logistics Aa* or *Trouble-free Logistics Atv*. After downloading the document, they can continue the enter industry passage. In this passage, the player must answer three questions with drop-down menus, each shown with options in table 3.6 respectively. The enrollment phase is after the player confirms they have the PDF and that their industry information is correct.

Code listing 3.2: Insert code passage

```
1  (set: $Seed to (random: 1,2))
2  (set: $password to (prompt: "Insert␣the␣code?",""))
3  {
4  (if: (num:$password) >= 10000 and (num:$password) <= 100000)[(go-to: "Dice␣roll")]
5  (else: )[(go-to: "Bad␣code")]
6  }
```

Tutorial phase is meant to introduce the game rules, mechanics, resources and skill points visually and give first-hand experience to the player to mitigate misunderstandings of how the game works. The passages in the tutorial phase are shown in figure 3.8. The player can retake the tutorial as many times as they

Table 3.6: Enter player information question 1-3 with options

1. Select the industry that aligns most closely with your current occupation:
Agriculture, forestry and fishing
Mining and quarring
Manufacturing
Electricity, gas, steam and air conditioning supply
Water supply; sewage, waste management and remediation
Construction
Wholesale and retail trade
Transportation and storage
Accommodation and food services
Information and communication
Finance and insurance
Real estate
Professional (consultatory), scientific and technical activities
Administrative and support services
Defense and public administration; compulsory social security
Education
Human health and social work
Arts, entertainment and recreation
Other service activities
2. Select how long how you have worked in that industry:
0-2
3-5
6-10
11-20
21 or more
3. Select the level you work at in that industry (see illustration below):
Senior Executive
Business
Implementation

Code listing 3.3: Dice roll passage

```
{
(if: $Seed is 1)[(go-to: "Aa")]
(else: )[(go-to: "Atv")]
}
```

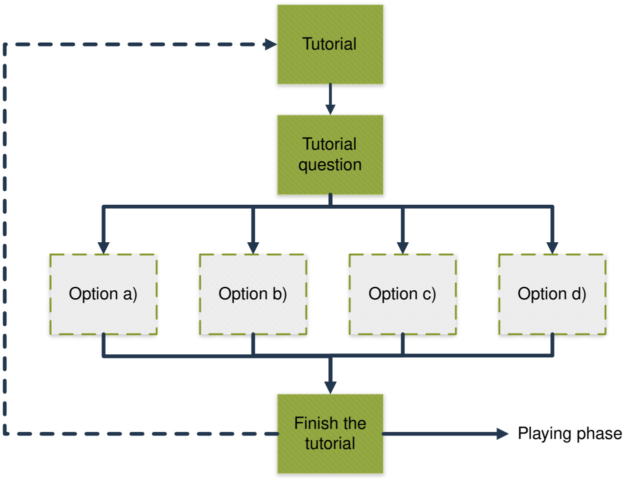


Figure 3.8: Tutorial phase

want. However, when they choose to begin the game, there is no way to go back.

Playing phase consists of nine questions, each with four options for the player to consider based on the scenario question. The player starts with the values set shown on code listing 3.4. Figure 3.9 shows that for each question *n*, the player has to choose between options a,b,c or d. Each option has a different cost associated with it in the form of capital and days. The player is then rewarded or penalised based on the scoring of the chosen option. The reward or penalty is incrementing or redacting the culture score, deciphering, developing, delivering or leading points. After answering the ninth question the playing phase is over.

Code listing 3.4: Start values

```
{(set: $Culture to 20)
(set: $Capital to 600000)
(set: $Day to 54)
(set: $Decipher to 4)
(set: $Develop to 4)
(set: $Deliver to 4)
(set: $Lead to 4)
(set: $Q1 to 0)
(set: $Q2 to 0)
(set: $Q3 to 0)
(set: $Q4 to 0)
(set: $Q5 to 0)
(set: $Q6 to 0)
(set: $Q7 to 0)
(set: $Q8 to 0)
(set: $Q9 to 0)}
```

Final phase consist only of two passages, namely the*Summary* passage and the *End the game* passage. The summary passage is of great importance because its in this passage the final calculations are done based on the rules of the game and presented to the player. Moreover, a script is only now run that sends the variables shown in lines 52-72 in code listing 3.5 to a web application ran on

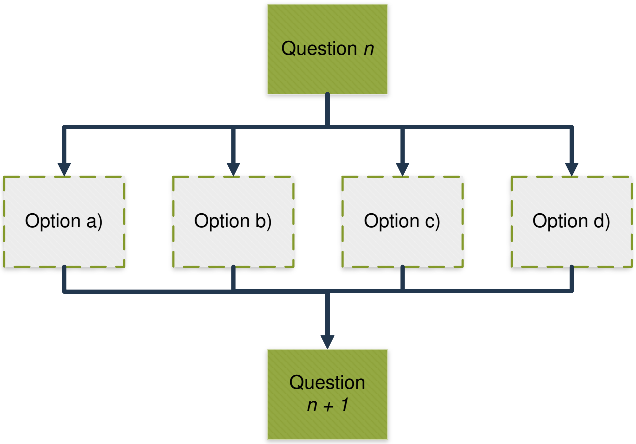


Figure 3.9: Playing phase

a Google account that puts these variables into a spreadsheet for later analysis. The game is finished when the player exits the last passage thanking them for participating.

Code listing 3.5: Summary passage

```
##Summary
{(if: $Capital < 0)[You are over budget with (abs:$Capital) $ and loose (print:
(round:(abs:$Capital/10000))) culture points.
(Set: $Culture to it + (round:($Capital/10000)))]
(else:)[You have $Capital $ left and gain (print:(round:($Capital/50000)))
culture points. (Set: $Culture to it + (round:($Capital/50000)))]

(if: $Day < 0)[You are (abs:$Day) days over budget and loose (abs:$Day)
culture points.  (Set: $Culture to it + $Day)]
(else:)[You have $Day days left and gain (print:(round:($Day/4)))
culture points. (Set: $Culture to it + (round:($Day/4)))]

(if: $Decipher > 8)[You gain (print:$Decipher-8) culture points for decipher.
(Set: $Culture to it + ($Decipher-8))]
(else:)[You gain no additonal culture points for decipher.]

(if: $Develop > 8)[You gain (print:$Develop-8) culture points for develop.
(Set: $Culture to it + ($Develop-8))]
(else:)[You gain no additonal culture points for develop.]

(if: $Deliver > 8)[You gain (print:$Deliver-8) culture points for deliver.
(Set: $Culture to it + ($Deliver-8))]
(else:)[You gain no additonal culture points for deliver.]

(if: $Lead > 8)[You gain (print:$Lead-8) culture points for lead.
(Set: $Culture to it + ($Lead-8))]
(else:)[You gain no additonal culture points for lead.]
}
###Your final culture score is: $Culture<hr>
###Resources:
Captial of $Capital $ (print: ’<progress␣value="’ + (text: $Capital) +
’"␣max="600000">␣/progress>’) $Day days left: (print: ’<progress␣value="’ +
 (text: $Day) + ’"␣max="54">␣/progress>’)
```

```
###Points:
Culture score: $Culture | (print: '<meter␣value="' + (text: $Culture) +
'"␣min="0"␣max="100"></meter>')
Decipher: $Decipher | (print: '<meter␣value="' + (text: $Develop) +
'"␣min="0"␣max="20"></meter>')
Develop: $Develop | (print: '<meter␣value="' + (text: $Develop) +
'"␣min="0"␣max="20"></meter>')
Deliver: $Deliver | (print: '<meter␣value="' + (text: $Deliver) +
'"␣min="0"␣max="20"></meter>')
Lead: $Lead | (print: '<meter␣value="' + (text: $Lead) +
'"␣min="0"␣max="20"></meter>')
{<!--
(print: (history:))
-->

<script src= jquery -3.3.1.min. j s ></script>
<script>
var sendData = JSON.stringify({
"Industry": $Industry,
"TimeIndustry": $TimeInIndustry,
"LevelIndustry": $LevelInIndustry,
"Seed": $Seed,
"Culture": $Culture,
"Capital": $Capital,
"Day": $Day,
"Decipher": $Decipher,
"Develop": $Develop,
"Deliver": $Deliver,
"Lead": $Lead,
"Q1": $Q1,
"Q2": $Q2,
"Q3": $Q3,
"Q4": $Q4,
"Q5": $Q5,
"Q6": $Q6,
"Q7": $Q7,
"Q8": $Q8,
"Q9": $Q9,
"Code": $password
});

$.ajax({
url:"https://script.google.com/macros/s/AKfycbzWgr7eRAkw_JZgdz90n1yhCmcXvQHvML
wIjil7e8golEmL4mQ2bUKGJn5xFJ58bZyV/exec",
method:"POST",
dataType: "json",
data: sendData
}).done(function() {})
</script>}
[[End the game]]
```

3.4.4 Game design and data collection

Data collection is done twice during the game. First, in Nettskjema, that only collects the count of responses to the *I agree to the terms and conditions* and collects the five-digit number of the participants choose to participate. The second data collection that happens is through an HTTPS POST message during the *Summary*

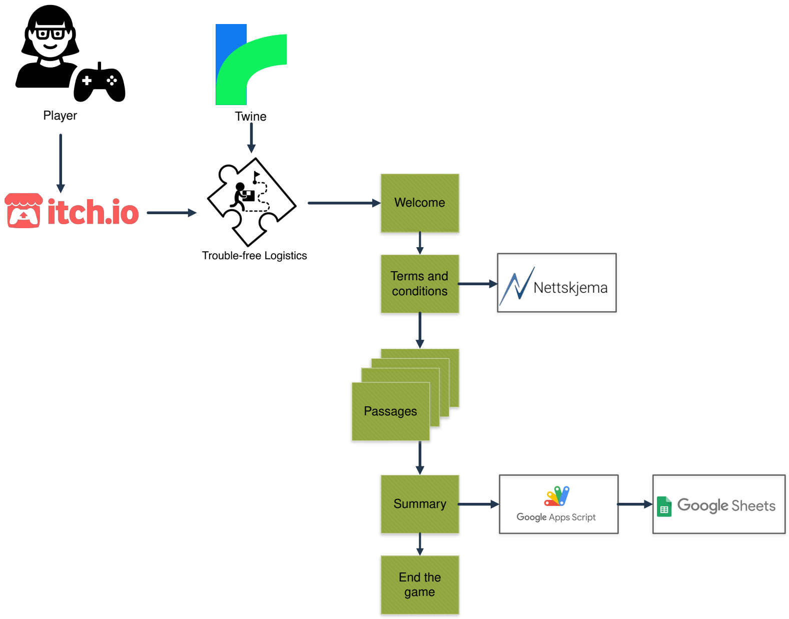


Figure 3.10: Data collection and high-level overview

passage shown on code listing 3.5 line 49-82. A code produced by *Dan Cox* from the article *Working with Google Sheets in Twine*, and modified for the decision-making game [94]. The same is true for the code for the Google Apps Script Web Application and is shown on code listing F.1 [94]. The Web Application pushes the variables into a Google Sheet and adds a new row for each HTTPS POST message received. Figure 3.10 shows how this ties together.

Game scenario and mechanics

In the game, the player plays the Chief Operating Officer (COO) in the fictitious business named *Trouble-free Logistics*. They receive a PDF with information about the company, its business model, organisation and security maturity assessment (See appendixC for the PDF). With this information, the player is asked to "*base your decisions on what you think will yield the best security culture for Trouble-free Logistics after completing all nine scenarios*". They will face nine fictitious scenarios based on known digital security challenges and incidents from the past ten years. The purpose is to simulate real situations that strategic decision-makers may encounter, a practice used exclusively as a pedagogical instrument. The game mechanics are divided into two categories—the resources, and the player's budget, namely capital and days. The player starts the game with a capital of 600 000 $ and 54 days. Each option the player chooses through the nine scenarios in the game has a capital and a daily cost associated with it. The second category is skill points. This category consists of culture score, decipher, develop, deliver and lead. The player is given the following description for each:

Table 3.7: Itch post [97]

Account	Forum or group	Date	Views
ulrikasa	Game - Twine	06.03.2023	464

Post text
This is a cyber strategic decision-making game! A part of the research project for the master-thesis titled “The benefit of value assessments in strategic security decision-making”. If you want to try it and participate, go head!

- **Culture score:** A measure of the overall security culture within Trouble-free Logistics, reflecting the organisation’s maturity and resilience related to cybersecurity.
- **Decipher:** A measure of how effectively you identify the problem and get to the root of the issue to find a solution. This metric evaluates your ability to think critically and analytically in the face of challenges related to cybersecurity.
- **Develop:** A measure of how well you are able to introduce new functionality to Trouble-free Logistics that improves the organisation’s security posture. This metric assesses your creativity and innovation in developing new solutions to address cybersecurity challenges.
- **Deliver:** A measure of how well you follow through and maintain the new functionality introduced to Trouble-free Logistics. This metric evaluates your ability to ensure that security improvements are sustained over time and that the organisation’s security posture continues to improve.
- **Lead:** A measure of how well you are developing the employees within Trouble-free Logistics and inspiring others to embrace and prioritize cybersecurity. This metric evaluates your leadership skills and ability to engage and motivate others to support the organisation’s security goals.

3.4.5 Hosting and sharing the game

After developing the game in Twine, the game was converted to an HTML file using the *Publish to File* function in Twine. The HTML file was then published on `itch.io` a free hosting marketplace for independent digital creators [95].

The sampling for the ER was done primarily through social media, on `itch.io`, `reddit.com`, `facbook.com` and `linkedin.com`. Table 3.7, 3.8, 3.9 and 3.10 shows under what account the game was published, in what forum or group, and on what day. The last column shows the posts’ views or impressions on May 1st, 2023. Note that the posts on Facebook and LinkedIn are in Norwegian and targeted at a Norwegian audience. These are, for convenience, translated into English in this thesis using ChatGPT, but can be viewed in Norwegian in appendix I [96].

Table 3.8: Reddit post [98]

Account	Forum or group	Date	Views
u/SawRiverHill	r/takemysurvey	10.03.2023	171

Post text
The benefit of value assessments in strategic security decision-making (Gamified survey for EVERYONE) `https://ulrikasa.itch.io/trouble-free-logistics`

Table 3.9: Facebook post [99]

Account	Forum or group	Date	Views
Ulrik Sagelvmo	IT-sikkerhet	19.03.2023	Uknown

Post text
Hello! In connection with my master's thesis at NTNU Gjøvik, I have developed a cybersecurity game and now need someone to play it. It occurred to me that this forum is a perfect fit. So, if you're interested in testing a game that deals with cybersecurity and tests your decision-making abilities, why not give it a chance and try "Trouble-Free Logistics" today? `https://ulrikasa.itch.io/trouble-free-logistics` Here's some more information: The game has been developed as part of my master's thesis, where I aim to shed light on the type of information that provides the most value for a strategic decision-maker. You will be thrown into realistic scenarios that businesses may face and will have to make decisions based on the information you receive in the game. The game is built upon the "SANS Cyber42 Security Leadership Simulation," academic research, and experiences from various organisations. The data from the game will be used to assist future security experts in presenting actionable and rational reports to management, ensuring good and effective decision-making together. By completing the game, you are making a difference! Thank you in advance for your participation!

Table 3.10: LinkedIn posts (1-3) [100]

Account	Forum or group	Date	Impressions
Ulrik Sagelvmo	From personal account	19.03.2023	1848

Post text (1)
Would you like to try a cybersecurity game? A game that challenges your decision-making skills? Perhaps learn something new or get inspired? Well, here's your opportunity: `https://lnkd.in/dUMmkknm` The game has been developed as part of my master's thesis, where I aim to shed light on the type of information that provides the most value for a strategic decision-maker. You will be thrown into realistic scenarios that businesses may face and will have to make decisions based on the information you receive in the game. The game is built upon the "SANS Cyber42 Security Leadership Simulation," academic research, and experiences from various organisations. The data from the game will be used to assist future security experts in presenting actionable and rational reports to management, ensuring good and effective decision-making together. By completing the game, you are making a difference! So why not give it a chance and try "Trouble-Free Logistics" today? Thank you in advance for your participation!

Account	Forum or group	Date	Impressions
Ulrik Sagelvmo	From personal account	27.03.2023	227

Post text (2)
Haven't had a chance to try the cybersecurity game yet? On April 3rd, I will begin compiling data from the game to try to determine which information provides the most value for decision-makers. To have the best possible dataset, I would like even more people to try the game. So, you still have the opportunity to test it if you haven't already. If you enjoyed it and believe it could be interesting for others, please feel free to share the game!

Account	Forum or group	Date	Impressions
Ulrik Sagelvmo	From personal account	28.04.2023	362

Post text (3)
Update on the #cybersecuritygame Firstly, I want to thank everyone who has participated. I hope you found it challenging yet enjoyable. I have received several inquiries about the best "Culture score." So, I would like to share the Top 3 list, which is as follows: **1.** 83, **2.** 81, **3.** 79. If you haven't had a chance to try the game and want to see how you perform, you still have the opportunity here:

Table 3.11: Listing what table contains the different scenarios and scoring in appendix G

Scenario	Scenario description table	Scoring table
1	G.1	G.2
2	G.3	G.4
3	G.5	G.6
4	G.7	G.8
5	G.9	G.10
6	G.11	G.12
7	G.13	G.14
8	G.15	G.16
9	G.17	G.18

3.4.6 Scenarios and scoring in the game

The nine questions presented to players in this study are based on fictitious scenarios drawn from a range of known digital security challenges and incidents within the past decade. These scenarios aim to simulate real-world situations encountered. Inspiration for the scenarios was to have the best possible dataset gathered from a variety of sources, primarily news articles from reputable outlets such as BBC, WIRED, ThreatWire, NRK, NSM, and Digi [101–105]. The scenarios were structured with reference to the SANS Cyber42 game [28].

All scenarios, including the four alternatives, responses, and scoring, are listed in tables in Appendix G, as they take up considerable space. Table 3.11 provides an overview of which scenario is included in Appendix G, along with the corresponding scoring table.

Each scenario was developed individually, and once a scenario had four distinct alternatives, the cost and scoring of each option were determined. To minimize personal bias, the allocation of costs and points was based solely on reputable sources such as NIST, NSM, the National Cyber Security Centre (NCSC) of the United Kingdom, and best practices supported by academic papers [30, 106, 107]. Furthermore, allocating costs and points was performed for each question in isolation. As a result, the optimal path or strategy for playing the game was unknown, except for the pilot version, where the optimal approach was to save as much money as possible until the end of the game. However, due to the adjustment of evaluation criteria at the end of the game, the pilot version placed too much emphasis on capital and days remaining, resulting in a high culture score for the player. To improve security culture, the company must invest in security, and the evaluation criteria were adjusted to avoid overemphasizing the value of having capital or days left over.

Chapter 4

Results and analysis

This chapter commences by presenting the findings of the conducted research methods, namely the Grounded Theory Study and the Experimental Research. Subsequently, it provides a detailed account of the methods used for analysing the gathered data.

4.1 Result of the Grounded Theory Study

In total 29 papers were selected and studied as a part of the GTS. An overview of these has been presented in chapter 3 and table 3.3. A more extensive list can be viewed in appendix H, showing all papers with search terms and tools, the evaluation of the quality of the paper and in what way it is validating the hypothesis of this thesis.

4.1.1 An emerging science

This research project builds upon the foundational work established in Tiril Tinde's master's thesis [26]. In the results of the literature review, Tinde's research substantiates that the literature review unveiled a significant scarcity of materials directly related to the problem being investigated [26, p. 35]. Going into the GTS therefore, the thesis expected to identify few directly relevant papers.

However, the scope of the current thesis extends beyond the confines of Tinde's research problem and is not exclusively reliant on research literature. While this broader approach allows for a more comprehensive array of sources, it's important to note that these additional sources may possess lower credibility. Therefore, evaluating these sources' validity and relevance becomes critical in this expanded research landscape.

Expanding the collected documentation reveals that the sociotechnical aspect of strategic decision-making remains a relatively under-investigated area of research. Nevertheless, this topic is integral to the burgeoning field of *social cybersecurity*, a discipline that leans heavily towards applied research within the realm of computational social science [68, p. 366-368].

The primary focus of this field revolves around social network analysis, data mining, and artificial intelligence, with disinformation emerging as the dominant theme [68]. Interestingly, the literature within this field presents novel tools and metrics devised to bolster the decision-making process, thereby enabling a metrics-based approach for communicators.

However, while these papers contribute valuable tools and information to the field, they fail to delve into the critical information needs of the decision-makers. They offer more information, which does not necessarily translate into a positive outcome. A potential pitfall of this approach is information overload, which could inadvertently hinder rather than aid the decision-making process. This was common for papers not to make it past stage 3. There were papers examining cybersecurity and/or decision-making, often tied to incident response, financial business decisions, state terrorism or infrastructure (both smart cities and critical infrastructure). The papers that talked about both or either one and that did not make it into stage 4 often did not investigate what cybersecurity information is of importance to strategic decision-making to make informed decisions. Therefore, they did not provide insight to answer research question **R1**.

4.1.2 Cyber and behavioural science

NIST, ISO and NSM alongside academia have for a long while talked about cybersecurity consisting of multiple pillars. ISO talks about technology, people and processes, while NSM and NIST focuses on physical, digital, personnel, organisational [47, 108]. Collier *et al.* in the paper "*Four domains of cybersecurity: a risk-based systems approach to cyber decisions*" talks about physical, informational, cognitive and social pillars [83]. As the frameworks of NIST, ISO and NSM are not specifically tailored to facilitate strategic decision-making, they have a different perspective and focus on the construction of well-structured ISMS.

To be able to provide insight into a transdisciplinary and often complex environment Carley suggest utilising a framework to limit misunderstanding, straightening findings and bridging the different organisational levels [68, p. 371]. Among the research papers, there seems to be an agreement that when cybersecurity is combined with decision-making it was treated as interdisciplinary. In this way, the previously mentioned frameworks focused on cybersecurity. However, the GTS suggest that when decision-making and cybersecurity are examined it should be done transdisciplinary, as illustrated in figure 4.1. Combining different sciences to better understand the research problem. Carley gives a word of caution, and states that although it seems that there is little research in the sociotechnical domain. This might be because it hasn't gotten a foothold yet. Not having dedicated conventions, journals or venues that are dedicated to the transdisciplinary field.

In the chapter 2 the term sociotechnical was introduced to emphasise the interplay and interdependence between people and the Cyber domain, but still limited within cybersecurity. Making this definition only covers the subject interdisciplinary. Acknowledging that conveying technical information about Cyber and under-

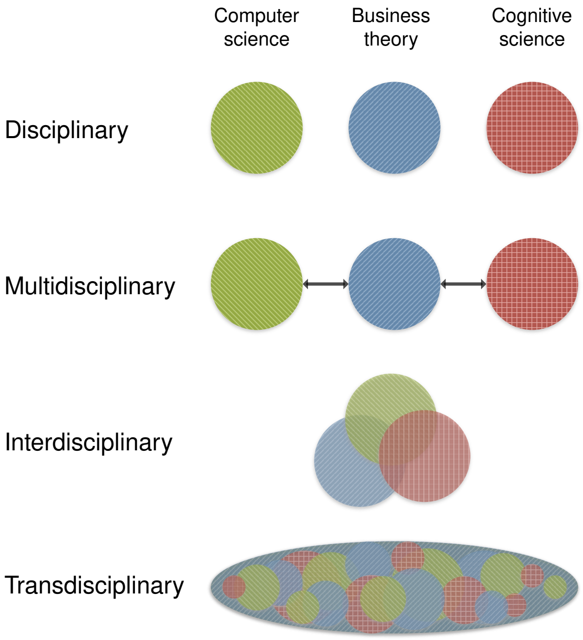


Figure 4.1: Illustration of different ways of combining and viewing multiple disciplines

standing decision theory is an emerging science and that it is transdisciplinary. In the book "*Theory and Models for Cyber Situation Awareness*" Liu *et al.* their guiding principle to make scientific advances in cyber situational awareness is through a multidisciplinary approach [76, p. 8]. Combining computer and information science with cognitive theory and decision-making and learning science. Building on work from this book, the thesis coins the term socobertech to specifically point to the transdisciplinary nature of the field, covering the social and human aspects, cognitive science and both Cyber and technical computer science. In this specific context, it is used to try to understand the human-cognitive process and decision-making in Cyberspace, and more precisely cybersecurity [73].

4.1.3 Uncertainty and rationality

Understanding the transdisciplinary nature of strategic business decision-making on cybersecurity-related topics brings with it a complex nexus of variables and a network of dependencies. Two of the most significant variables discussed by the papers in the GTS are uncertainty and rationality. Considering human-related, cognitive, and social factors that underline the message sent to decision-makers, that sometimes does not act in a perfectly rational manner from a cybersecurity expert standpoint. The papers from the GTS have a consensus in that they either quantify or model the uncertainty and rationality. Building matrices, constructing benchmarks, and comparing data to support rational decisions.

Quantify and modelling uncertainty and rationality

A functional ISMS that adapt to risk and protects the assets of the organisation is the goal of security is often measured and in that quantified. Standards developed by NIST, ISO and NSM are constructed to ensure that security actually protects the assets by measuring and testing the security controls. Evaluating if the security measures are effective. These measures are in place based on the perceived cybersecurity risk of the business, and the perceived value of their operations. These measures, therefore, are not optimized to be presented to decision-makers.

Bojanić *et al.* suggest using a Cybersecurity Management System (CSMS) in order to structure the strategical security decisions [84]. A system that can take different forms, but should be designed for the specific business. Perform computational modelling and simulation, preferably supported by artificial intelligence built on the intellectual property of the organisation. Similar systems and computational modelling is suggested by Keller and Ho, Rass, Liu *et al.*, Stepanova *et al.*, Bojanić *et al.* [72, 74, 76, 77, 84].

A model that future builds on the CSMS is the Conflicting Incentives Risk Analysis (CIRA) framework [109, p. 327-341]. Arguing that risk management is about aligning incentives and understanding stakeholders, much in the same way as SANS and their curriculum on strategic cybersecurity Kim. CIRA plots the approach to risk mitigation on an incentive graph, identifying the strategy the risk owner should take in order to mitigate the risk. This approach would support the cybersecurity expert in their approach to facilitate strategic decision-making. Taking into consideration human motivations and incentives.

4.1.4 Unquantifiable

When faced with the challenge of complex variables and uncertainties, a common approach in academia is to collect data and quantify it. This has led to insightful studies and improved knowledge of cybersecurity. Unfortunately, when theory meets practice it can be hard to adapt to the business vision, goals, missions or strategy. Sometimes, the problem is that the business does not have direction or overarching strategy. Common for a Small And Midsize Business (SMB), that does not have time or resources to prioritize long-term detailed planning. A quantification more often than not involves many assumptions, and does not recognize the number of decisions that have to be made on a executive level. These decisions are often interlinked and have multiple dependencies and impacts on each other. Quantifying or modelling something that holistically addresses the strategic decision-making in the business is resource intensive for most businesses. Especially, in an environment that changes as rapidly as computer technology and the threat and vulnerability landscape. Moreover, incomplete knowledge about next year's budget, or poor formal planning processes and management culture. Maybe, power in the organisation is personalised and it functions reactively and ad-hoc. Then it becomes next to impossible to facilitate strategic decision-making through quantification and modelling. LeVeque notes that it is a large leap from academic papers to a practical proven, methodology useful for business decision-making [46, p. 203].

Game-Theoretic Approach

Liu *et al.* writes that further investigation should be done into game-theoretic and control-theoretic solutions to investigate reasoning under uncertainty [76, p. 45]. While also improving CSMS enabling and facilitating informed decisions. In the book "*Cyber-Security in Critical Infrastructures: A Game-Theoretic Approach*" Rass analyses multiple game-theory approaches to cybersecurity decision-making [74]. That also accounts for businesses having multiple goals and objectives, applying mathematical decision-making through game theory. With the benefit that it is possible to perform analysis that has bounded rationality. Implying that the decision-maker always acts in a perfectly rational way. Therefore, excluding variables that are hard to account for. Losing validity, but increasing the reliability. Some uncertainty can be accounted for by statistics and by stochastically adding randomness [74, p. 99]. A game-theoretic approach to decision-making is manageable but struggles when it is deployed in a real-world setting. This is especially true for private businesses. Because their threat landscape is more varied and possible with a greater of number of different actors. A nation can perform game theory on a rational Advanced Persistent Threat (APT), however, this becomes more difficult to do for a private business. It might be more valuable for a private business to focus on common vulnerabilities and Tactics, Techniques, and Procedures (TTPs).

4.1.5 Making cybersecurity decisions

The paper "*The Good, the Bad and the Ugly: A Study of Security Decisions in a Cyber-Physical Systems Game*" by Frey *et al.* has more or less the same problem description as this thesis [79]. Investigating the decision-making progress related to determining security requirements in an organisation. Studying how 'security experts', 'computer scientists' and 'managers' played a cyber-physical systems game. To measure how effective the strategies and decision-making of the different demographics were. Each group got evaluated on 'data protection', 'intelligence gathering', 'human factors' and 'technological solutions'. The game revealed strategies deployed and repeated by different demographic and identified patterns that lead to good practices and patterns that lead to errors and pitfalls. The paper concludes that an approach to cybersecurity decision-making that uses a balanced holistic approach is the most beneficial long-term approach. That "tunnel vision" and strong "know it all" champions can have a bad influence on decision-making [79, p. 531-532]. Interestingly, the game revealed that the 'security experts' was overconfident neglecting intelligence gathering and to focused on advanced technical solutions, skipping basic protection [79, p. 529].

In a recent survey, 600 board members were questioned regarding their attitudes and activities pertaining to cybersecurity. The findings support the result from the game of Frey *et al.* in that interactions between board members and CISO are lacking. Furthermore, cybersecurity is viewed by board members as a technical topic, and security professionals are failing to show the importance of cybersecurity [110]. Implying that 'security experts' are overconfident in their knowledge, and fail to communicate with the board members on a fundamental level, tying security to the business.

4.1.6 Just do it!

As technology continues to advance at a rapid pace, the landscape of threats and vulnerabilities becomes increasingly complex and difficult to fully comprehend. A different approach can be taken when combining the work of Sallos *et al.* and LeVeque [82, p. 591] [46]. The approach of not having a systematic approach or the strategy of not having a strategy. This mindset raises critique towards the classical ways of strategy work and that in today's environment, this is outdated [46, p. 188]. A more agile approach that allows for flexibility and rapid adaptation is the way forward. Building functional security today is of greater value than spending time and resources on strategic long-term planning, building CSMS that quantify and model cybersecurity to facilitate decision-making or constructing temporary decision matrices that all are going to be outdated fast and probably not be of great value because of the low real-world validity.

4.1.7 Facilitating for strategic decision-maker(s)

The GTS findings are constructed into a model illustrated in figure 4.2. The model is not all-encompassing or includes all factors and variables of the analysis. It is meant to provide elucidation on the topic of strategic decision-making within the field of cybersecurity when viewed as a discipline that is transdisciplinary. This model will be further explained and discussed in chapter 5.

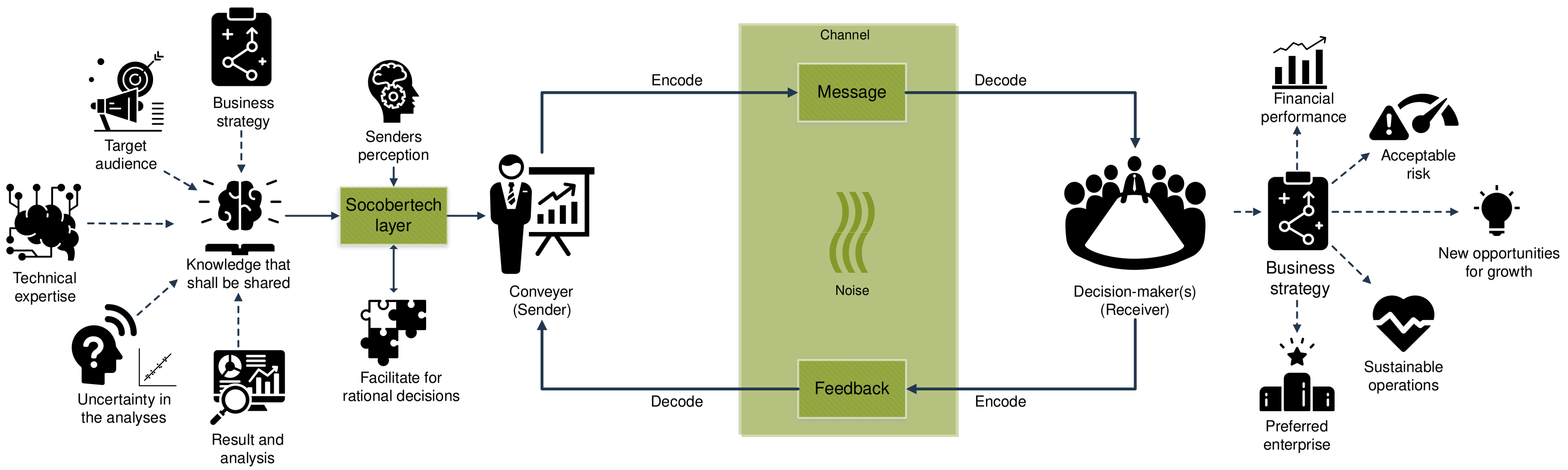


Figure 4.2: The transdisciplinary nature of conveying a message to strategic decision-maker(s) in the field of cybersecurity

4.1.8 Additional findings

The main objective of the GTS was to answer research question **R1**. It has resulted in findings relevant not directly linked to research question **R1**, but the problem description of the thesis, and is therefore included here.

IT governance

The most influential contribution to IT governance that the board and executives can make is to have an explicit governance structure involved in IT and cybersecurity management. Peter Weill and Jeanne Ross found that firms that scored above-average on IT governance practices measured 20% higher returns on assets over three years [46, 70].

According to LeVeque, a cybersecurity practitioner operating at the operation level or business and management level should possess a comprehensive understanding of how digital security integrates with the respective organisation, and be cognizant of the associated risks [46, p. 7]. This is important because the information must not only "feel right" to the cybersecurity expert, but "feel right" to the executives as well. For that reason, the information must possess sufficient integrity and be proportional to the weight of the decisions. At the executive level, it is important that the result of the decision can be adopted by the organisation without changing the day-to-day practice. That it achieves organisational goals and aligns with the business strategy. This entails that the information and the foundational data must be understandable for non-technical executives and tied to organisational assets important for operations[46].

Value of information

The assessment of information's value is a critical factor when evaluating information security. Traditional tangible assets, familiar to economists, have a rich history of valuation and a well-understood contribution to an organisation's worth. This understanding facilitates the calculation of physical, personal, and organisational security measures required to safeguard these tangible assets, rendering the process more straightforward and comprehensible [46].

In contrast, the valuation of intangible assets, such as digital information and data, presents a more complex challenge. The value these assets bring to an organisation can be difficult to ascertain, often depending on specific circumstances. For example, certain data may only carry value when combined with other data or may offer competitive advantages. Some data may hold future potential or serve as a basis for analysis to aid decision-making. In other instances, the value might only be recognized by external parties.

Therefore, the process of securing such assets must take into account these nuanced aspects of data and digital information value. This further emphasizes the need for a comprehensive understanding of digital security within the organisation, including the various ways in which intangible assets can contribute to organisational value.

4.2 Result of Experimental Research

This section presents the results from the ER game. Data was obtained through the collection of complete submissions and will be presented through tables, graphs and visual illustrations.

4.2.1 Players demographics

The game was initiated by a total of 464 players, as demonstrated in Table 4.1. Out of these, 41 players successfully completed the game. Additionally, there were 137 submissions registered in Nettskjema, with 133 of these agreeing to the terms and conditions and providing a code for the game. However, only 41 of these submissions were registered in the web application. Analysis of the provided codes revealed that there were 104 unique five-digit codes. The most frequently used code was "12345", which was used 16 times. In the final submissions collected in the web application, there were two entries with the code "12345", although these were not submitted on the same day.

Table 4.1: Responses

Application	Number of submissions
itch.io	464
Nettskjema	137
Web-application	41

Submissions

Out of the 464 players who entered the game, only 30% completed the form with the terms and conditions, and a mere 9% finished the game. The substantial decrease in the number of players from starting the game to completing the enrollment phase could be attributed to various factors such as time constraints, the unfriendliness of the game, game malfunctions, subpar graphical assets, disagreement with the terms and conditions, information overload, or multiple visits by the same participant.

The terms and conditions required players to dedicate their attention for the next 20 minutes. If a participant lacked the time, they were more likely to quit without providing any response. The default version of Twine, which does not feature the most updated graphical assets that modern players might be accustomed to, could be uninviting to some when combined with the embedded form from Nettskjema. This might have also caused crashes or malfunctions.

Participants who disagreed with the terms and conditions may have found it more convenient to close the game rather than explicitly answering "no." The terms and conditions are lengthy to ensure that players receive all the necessary information, but this might have been overwhelming and demotivating for some, even before starting the game. Lastly, the drop in players between the game's launch and the enrollment phase could be attributed to players quitting and re-entering the game.

Out of the players who completed the enrollment phase, only 30% managed to finish the game and successfully register their scores with the web application. The discrepancy between registrations in Nettskjema and the web application could be attributed to various factors such as network issues, time constraints, lack of motivation, fatigue, poor programming, application downtime, or technical malfunctions.

While Google Apps Script reported an error rate of 0%, it must be noted that this figure would remain unaffected if the web application failed to receive an HTTPS POST message. However, Google Analytics reported zero downtime for the entire research project.

Even if `itch.io` experienced downtime, it should not have adversely affected gameplay. Once a player started the game, it ran locally on their browser, only requiring an internet connection when reaching the final passage, where the HTTPS POST message is generated. Therefore, any connection issues at this stage would prevent a completed game from being registered with the web application.

The programming skills of the author may not be impeccable, potentially leading to misconfigurations or programming errors that could cause some submissions to not be registered with the web application. Although this possibility was thoroughly tested during the development phase and sporadically tested during the live game period, there were no dropped submissions. However, the possibility cannot be entirely ruled out.

The game, being somewhat demanding, required the full attention of the player, testing their cognitive abilities. The high volume of information combined with complex scenarios, the pressure of evaluation, and scoring may have led some players to quit. If the game did not meet a player's expectations or failed to motivate them, it may have further contributed to players abandoning the game before completion.

Distributions

During the enrollment phase, players responded to three self-related questions. The distribution of responses is presented in Table 4.2.

In the first question, players were prompted to "*Select the industry that aligns most closely with your current occupation*". The options provided corresponded to the industries and sectors enumerated by the *International Labour organisation*. Only the options that garnered one or more responses are displayed in Table 4.2. Among these, the "*Information and Communication*" category had the highest representation at 36%, closely followed by "*Professional (Consultatory), Scientific and Technical Activities*" at 34

The second question asked players to "*select how long you have worked in that industry*". The distribution of responses was fairly even, though the 0-2 years and 6-11 years brackets were notably more represented, each accounting for 26.8% of responses.

The final question positioned players within an organisational hierarchy by asking them to "*select the level you work at in that industry (see illustration below)*". The illustration provided was taken from NIST's CSF figure titled "*Notional Information and Decision Flows within an organisation*" [18, p. 12].

The project aimed to garner responses from both the strategic level and the operational level. A significant 53.7% of players identified as belonging to the business category, thus representing the operational level—a favourable outcome. However, the representation of the strategic level was disappointingly low, with only 12.2% of players identifying at this level.

Table 4.2: Player distribution

Question	Alternatives	Frequency	Percentage
1. Select industry	Agriculture, forestry and fishing	1	2,4%
	Wholesale and retail trade	1	2,4%
	Information and communication	15	36,6%
	Finance and insurance	4	9,8%
	Professional, scientific and technical activities	14	34,1%
	Administrative and support services	1	2,4%
	Defense and public administration	2	4,9%
	Education	1	2,4%
	Human health and social work	1	2,4%
	Other service activities	1	2,4%
	Total	41	100%
2. Time in industry	0-2	11	26,8%
	3-5	7	17,1%
	6-10	11	26,8%
	11-20	6	14,6%
	21 or more	6	14,6%
	Total	41	100%
3. Level in industry	Senior Executive	5	12,2%
	Business	22	53,7%
	Implementation	14	34,1%
	Total	41	100%

Seed placement

The random function from code listing 3.2 ended up placing 20 players in seed A_A and 21 in seed A_{TV}.

Table 4.3: Distribution of seeds

Seed	Number of responses
A_A	20
A_{TV}	21
Total	41

4.2.2 Statistical analysis of results

To better understand the result and the data collected, it is analyzed through statistical methods, and organized and presented in tables and graphs. Making it easier to conceptualize and interpret the data.

For this paper, the most interesting relationship is between the independent categorical variable belonging to group R_A and R_B and the dependent variable of the final culture score for S_A and S_{TV}. The paper will therefore study the statistics around the culture score, before divining into the relation between other variables deployed in the game.

Examining the culture score

Firstly, confirming the assumption of the culture score of S_A and S_{TV} to have a normal (Gaussian) distribution. A normal distribution allows for parametric statistics, while if the data is non-normal distributed, a non-parametric statistical approach has to be used. GraphPad Prisma is used to confirm that both S_A and S_{TV} has a normal distribution. Using a *column* sheet in GraphPad Prisma with the culture score of S_A and S_{TV} put into their own columns. Then choosing the "*Normality and Lognormality test*", computing the normal distribution with both *D'Agostino & Pearson omnibus normality test* and *Shapiro-Wilk normality test* with a significance level α of 0.05. As shown on table 4.4 both tests yield a passing value for normality for S_A and S_{TV}. As noted by GraphPad Prism in their guide to choosing the optimal normality test, these tests are not considered scientifically strong [111]. For that reason, two tests are performed, and only to give an indication of the normality of the data. With the data having a reasonable normality as shown in table 4.4, the paper can utilize parametric statistics in the form of an unpaired t-test to evaluate the hypothesis. If not, the paper would have to use a non-parametric method, such as the Mann-Whitney and the Kolmogorov-Smirnov tests [111].

The sample goal of the experimental research was $n => 102$ for the result to yield a statistical power of at least 0.8 with an α of 0.05 and an effect size equal to 0.5. A post hoc calculation of the achieved power with the total sample size of $n = 41$, α of 0.05 and an effect size equal to 0.5 shows an actual power of 0.47 (see table 4.5. Reducing the likelihood of detecting a true effect if there is one. Making it more likely to reject a false negative, also referred to as a type II error.

The primary variables examined is the categorical nominal variable of R_A and R_B, and the quantitative discrete variables of the culture score. Secondarily variables will be categorical variables related to players demographics and quantit-

Table 4.4: Result from the normal distribution test with GraphPad Prism

Type of test	Metric	S_A	S_{TV}
D'Agostino & Pearson test	K2	1,648	2,321
	P value	0,4387	0,3134
	Passed normality test ($\alpha = 0.05$)?	Yes	Yes
	P value summary	Not significant	Not significant
Shapiro-Wilk test	W	0,9352	0,9294
	P value	0,1941	0,1341
	Passed normality test ($\alpha = 0.05$)?	Yes	Yes
	P value summary	Not significant	Not significant

Table 4.5: Post power analyses using G*Power [87, 88]

t tests	Means: Difference between two independent means (two groups)	
Analysis	Post hoc: Compute achieved power	
Input	Tail(s)	= one
	Effect size d	= 0.5
	α err prob	= 0.05
	Sample size group 1	= 20
	Sample size group 2	= 21
Output	Noncentrality parameter δ	= 1.6003048
	Critical t	= 1.6848751
	Df	= 39
	Power ($1 - \beta$ err prob)	= 0.4711490

ative variables related to the different metrics used in the game. In table 4.6 the statistics of the metrics deployed in the game are shown for S_A and S_{TV} in isolation and combined. The mean, median, mode, range max, range min and range width for the culture score, capital left, days left, decipher, develop, deliver and lead.

Table 4.6: The mean, median, mode, range max, range min and range width of the variables used in the game

Variable	**Measure**	S_A	S_{TV}	**Combined**
Culture Score	Mean	63,45	63,24	63,34
	Median	64,5	68	65
	Mode	77	49	78
	Range max	79	83	83
	Range min	36	37	36
	Range width	43	46	47
Capital left	Mean	124 000	88 810	105 976
	Median	122 500	65 000	105 000
	Mode	175 000	175 000	175 000
	Range max	360 000	260 000	360 000
	Range min	-20 000	-70 000	-70 000
	Range width	380 000	330 000	430 000
Days left	Mean	5,15	5	5,07
	Median	5	4	4
	Mode	6	3	3
	Range max	18	21	21
	Range min	-6	-14	-14
	Range width	24	35	35
Decipher	Mean	15,70	15,86	15,78
	Median	16	16	16
	Mode	16	12	16
	Range max	19	21	21
	Range min	9	10	9
	Range width	10	11	12
Develop	Mean	11,10	11,52	11,32
	Median	11	12	12
	Mode	13	10	13
	Range max	16	16	16
	Range min	6	7	6
	Range width	10	9	10
Deliver	Mean	12,30	12,90	12,61
	Median	13	13	13
	Mode	15	14	15
	Range max	15	19	19
	Range min	5	6	5
	Range width	10	13	14
Lead	Mean	13,05	13,38	13,22
	Median	13	14	13
	Mode	12	11	12
	Range max	19	18	19
	Range min	7	8	7
	Range width	12	10	12

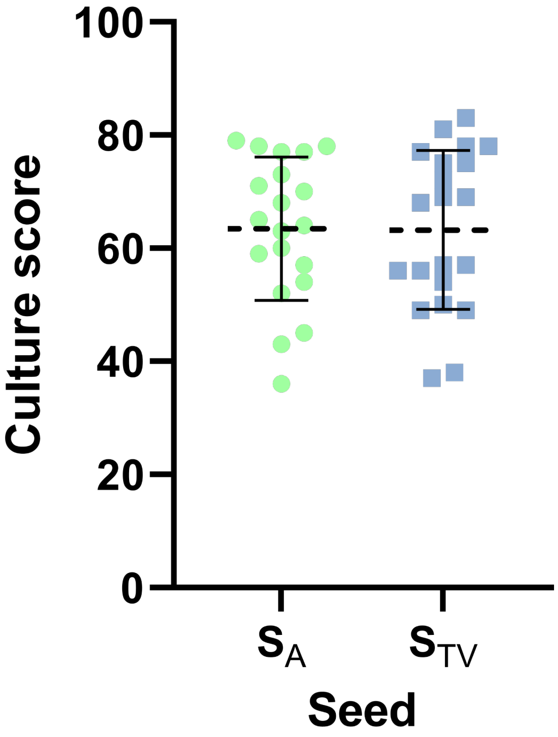


Figure 4.3: Culture score comparison between group R_A and R_B with the mean and the standard deviation for each seed

Statistical significance of culture score

By comparing the culture score mean of $\overline{S_A}$ against $\overline{S_{TV}}$, there is practically no difference. Illustrated in figure 4.3. Both are as close to equal to the average culture score when all players are combined. To confirm that these results are not up to change, a hypothesis test is performed. The hypothesis for the experimental research is that R_A will have a significantly greater culture score than R_B. Making our working alternative hypothesis $H_1 : \overline{S_A} > \overline{S_{TV}}$. Our null hypothesis is therefore that there is no significant difference between the culture scores of $\overline{S_A}$ and $\overline{S_{TV}}$. Making the null hypothesis $H_0 : \overline{S_A} <= \overline{S_{TV}}$. Due to the low sampling, the significance level (α) is set to 5%, implying that the null hypothesis is rejected if there is a 5% change variability difference between the groups. A false rejection of the null hypothesis will lead to a *type I error* and is considered the worst for the integrity of this thesis.

By using an unpaired t-test after confirming a Gaussian distribution and that both populations have close to the same standard deviation. The alternative hypothesis can be investigated. The result is a P value of 0.48. As shown in table 4.7 the result is far from significantly different and the null hypothesis stands. This implies that R_A does not have a significantly greater culture score than R_B, by the data collected. As expected after reviewing table 4.6 and figure 4.3. H_0 is therefore valid. Because the thesis relied on a one-tailed test, mostly because this requires fewer samples. It is not possible to confirm that there is no significant difference or relationship between the two sets of data or variables analyzed. However, the data shows that there is no merit to the hypothesis of R_A outperforming R_B, rather, it shows that R_B preforms the equal to that of R_A or better. The unpaired t-test, therefore, confirms that any observed difference is due to chance and that no underlying causative relationship does exist.

Having a large P value (significantly larger than 0.05) combined with the low R-value the statistics tell that the seed had no effect or impact that would give the group R_A an advantage. The 95% confidence interval however is not reassuring. Implying that most likely the true difference is ± 8 of the mean of the groups. If one group consistently averaged a culture score of 8 or more than the other group. This would be considered to be a notable advantage. This is most likely not the case, but the 95% CI makes it so that we can not make a strong conclusion.

Table 4.7: Results form the unpaired t-test of the culture score of R_A and R_B

Unpaired t test	
P value	0,4799
P value summary	Not significant
Significantly different ($P < 0.05$)?	No
One- or two-tailed P value?	One-tailed
t	t=0,05062
df	df=39
How big is the difference?	
Mean of column S_A	63,45
Mean of column S_{TV}	63,24
Difference between means $(B-A)SEM$	-0,2119 ± 4,186
95% confidence interval	-8,679 to 8,255
R squared (eta squared)	6,570e-005
F test to compare variances	
F	1,228
DFn	20
Dfd	19
P value	0,6573
P value summary	Not significant
Significantly different (P < 0.05)?	No

By changing the hypothesis, it is possible to perform a two-tailed unpaired t-test on the data. Although, the result would have a weak power level. Using G*power, the power level of a t-test between two independent means with an effect size of 0.5, α of 0.05 and sample sizes 1 and 2 of 20 and 21. Shows that the achieved power is 0.35. Consequently, the risk of making a type II error is higher for the two-tailed test than the one-tailed.

The new alternative hypothesis for the two-tailed unpaired t-test is $H_1 : \overline{S_A} \neq \overline{S_{TV}}$ and the null hypothesis $H_0 : \overline{S_A} = \overline{S_{TV}}$. The level of significance α is set to 0.05. The rejection region is therefore $\pm\alpha/2$. Table 4.8 show that there is no significant difference between the culture score of group R_A and R_B, in either direction.

Table 4.8: Results form the two-tailed unpaired t-test of the culture score of R_A and R_B

Unpaired t test	
P value	0,9599
P value summary	Not significant
Significantly different ($P < 0.05$)?	No
One- or two-tailed *P* value?	Two-tailed
t	t=0,05062
df	df=39

Table 4.9: The variance, standard deviation, standard error of mean, coefficient of variation, skewness and kurtosis of the variables used in the game

Variable	**Measure**	S_A	S_{TV}
Culture Score	Variance	160,68	197,39
	Standard deviation	13	14
	Standard Error of Mean	2,8	3,1
	Coefficient of variation	20%	22%
	Skewness	-0,62	-0,35
	Kurtosis	-0,42	-1,0
Capital left	Variance	8 806 842 105	8 987 261 904
	Standard deviation	93845	94801
	Standard Error of Mean	20984	20687
	Coefficient of variation	75,68%	106,7%
	Skewness	0,65	0,068
	Kurtosis	0,63	-0,82
Days left	Variance	23,87	59
	Standard deviation	4,8	7,7
	Standard Error of Mean	1,1	1,7
	Coefficient of variation	93%	154%
	Skewness	0,53	-0,19
	Kurtosis	2,8	1,2
Decipher	Variance	8,12	10,53
	Standard deviation	2,8	3,2
	Standard Error of Mean	0,64	0,71
	Coefficient of variation	18%	20%
	Skewness	-1,2	-0,063
	Kurtosis	0,77	-1,0
Develop	Variance	5,57	7,66
	Standard deviation	2,4	2,8
	Standard Error of Mean	0,53	0,60
	Coefficient of variation	21%	24%
	Skewness	-0,079	-0,15
	Kurtosis	0,064	-1,1
Deliver	Variance	7,06	10,09
	Standard deviation	2,7	3,2
	Standard Error of Mean	0,59	3,2
	Coefficient of variation	22%	25%
	Skewness	-1,2	-0,32
	Kurtosis	1,6	-0,085
Lead	Variance	8,89	9,25
	Standard deviation	3	3
	Standard Error of Mean	0.67	0.66
	Coefficient of variation	23%	23%
	Skewness	-0,054	-0,13
	Kurtosis	0,082	-1,2

The impact of player demographics on cultural score

In order to get a better understanding of the data, all samples *n* were sorted based on the information the players entered and their culture score. This is illustrated in figure 4.4. Figure 4.4a shows the mean and standard deviation of each industry. The result of how many years the player had in that particular industry is illustrated in figure 4.4b. Lastly, the effect on culture score based on what business level the player belongs to is shown in figure 4.4c.

Interpreting the impact on the culture score based on industry serves little purpose, due to most industries only having 1 sample as shown in table 4.2. Only 'Information and communication', 'Finance and insurance' and 'Professional, scientific and technical activities' have 4 or more samples collected. From these 'Finance and insurance' seems to consistently perform the best, however, this is only based on four samples (see figure 4.4a).

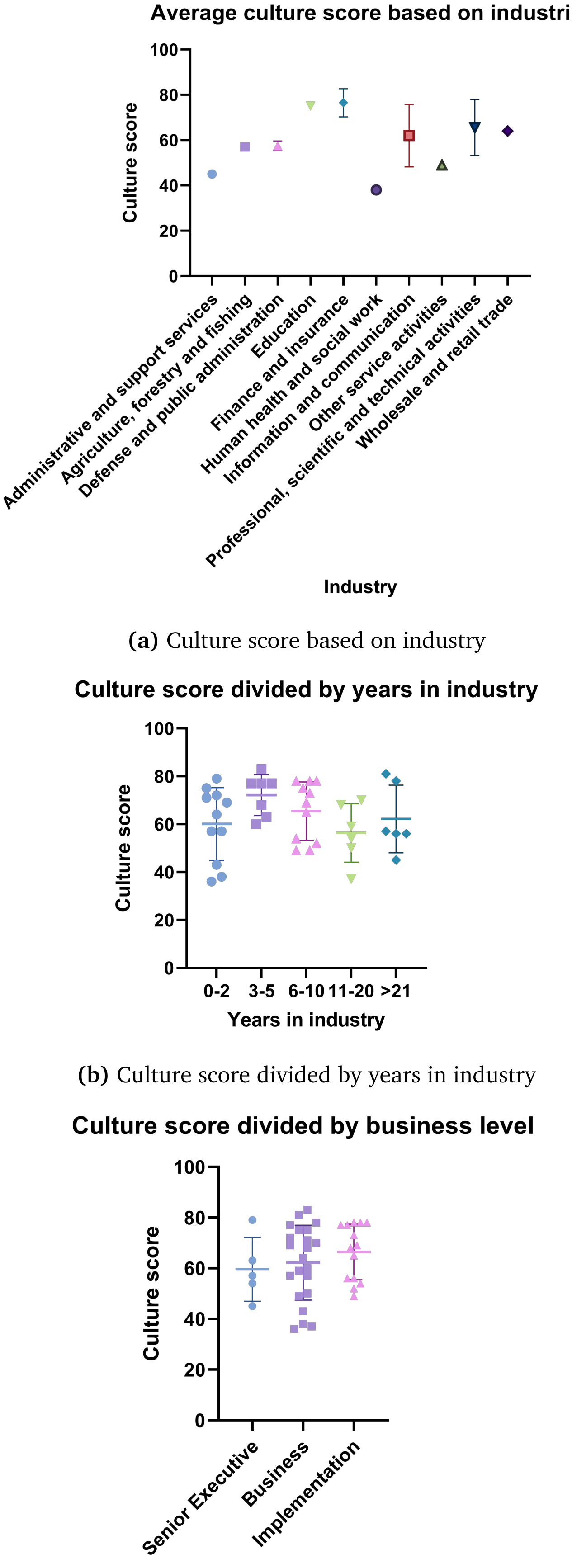
In the years in industry category, the segment that on average has the highest mean is '3-5' (see figure 4.4b). This category is the most consistent, with the lowest standard deviation and error of the mean. '3-5' years in the industry has a culture score with a mean of 72. Ranking second is the '6-10' years segment with a mean of 65. By this data, the segment '3-5' years in the industry will outperform other age groups. Note that years in the industry only indicate how many years that player has been in that specific industry. A senior executive might enter a new industry, and therefore be viewed as a senior but with a low amount of years in that specific industry. Segments '0-2' (60) and '>21' (62) have similar means, and '11-20' (56) have the lowest mean.

The culture score divided by business level is considered similar, as shown in figure 4.4c. The 'implementation level' has on average a 6-point higher score than the 'senior executives' scoring the worst average culture score, while also being more consistent. Due to the few samples, all categories in the game can be skewed by 1 or 2 samples. For that reason non of the figures from 4.4 should be taken on face value.

Statistical significance of remaining variables

The experimental research hypothesis has focused on the significance of the culture score related to what information the player received in their seed group, and how that affect their end result. In addition to the culture score, the player had to manage their resources well. Being their capital and days available. How the player chose to utilize these resources affected the culture score, as well as the variables decipher, develop, deliver and lead. This section examines if the seed had any effect on these variables. Before addressing how the effect of different industries, the length of the time spent in that industry and their level in the organisation had on the end culture score.

From 4.6 and 4.9 the resources stands out in their own way. This is made visual when illustrated on figure 4.5. Figure 4.5a show the difference in means between the amount of capital each group had left at the end of the game. On table



(a) Culture score based on industry

(b) Culture score divided by years in industry

(c) Culture score based on business level

Figure 4.4: Visualisation of the impact on culture score based on demographics

4.10 shows that this variable has the lowest *P* value of all variables deployed in the game. It is still far from statistically significant, but the biggest difference between group R_A and R_B is shown by the amount of capital left. For days left illustrated in figure 4.5b, the mean is similar. But the variance shown on 4.9 and by the *F* test on table 4.10, and illustrated on figure 4.5b, indicates that the spread is significant. The unpaired t-test for days left reports a significant difference between the standard deviation of group R_A and R_B. The variable day therefore fails the assumption of group R_A and R_B having similar standard deviations. Making further analysis of this variable futile.

For the variables decipher, develop, deliver and lead there are no significant findings, leaning in either direction. Implies that H_0 is in effect and that there is no difference between group R_A and R_B, and the seed has no impact on any variable deployed in the game. Table 4.10 list an two-tailed unpaired t-test for all variables belonging to S_A and S_{TV}. Figure 4.6 plots the difference in means between S_A and S_{TV} for the variables decipher (4.6a), develop (4.6b), deliver (4.6c) and lead (4.6d).

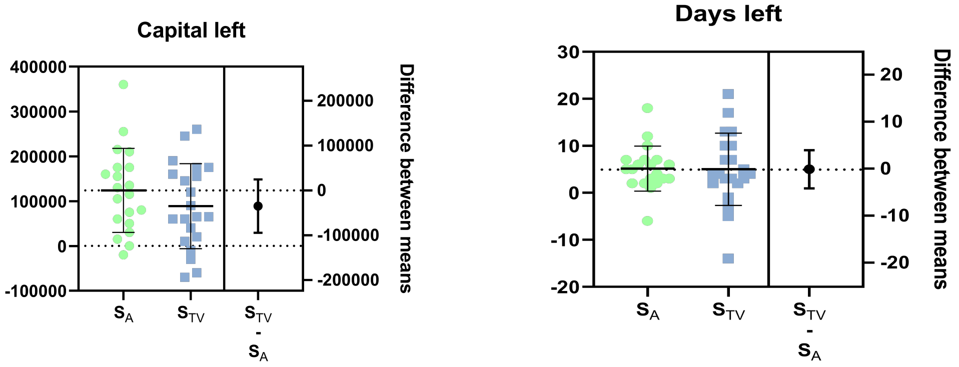
Table 4.10: Results form two-tailed unpaired t-test of deployed variables between S_A and S_{TV}

Unpaired t test	Capital	Day	Decipher	Develop	Deliver	Lead
P value	0,24	0,94	0,87	0,6	0,51	0,73
P sum.	NS	NS	NS	NS	NS	NS
Sig. dif	No	No	No	No	No	No
t	1.19	0,074	0,16	0,53	0,66	0,35
The difference	Capital	Day	Decipher	Develop	Deliver	Lead
$(S_A - S_{TV})$±SEM	-35190 ± 29475	-0,15 ± 2,01	0,16 ± 0,95	0,42 ± 0,81	0,61 ± 0,92	0,33 ± 0,94
95% CI	-94808 to 24427	-4,21 to 3,91	-1,78 to 2,09	-1,2 to 2,05	-1,25 to 2,46	-1,57 to 2,24
R squared	0,035	0,00014	0,0007	0,007	0,011	0,003
F test	Capital	Day	Decipher	Develop	Deliver	Lead
F	1,02	2,58	1,3	1,38	1,4	1,04
P value	0,97	0.04	0,57	0,49	0,44	0,94
P sum.	NS	*	NS	NS	NS	NS
Sig. dif	No	Yes	No	No	No	No

4.2.3 Heatmap

By counting the number of times each option within a scenario was chosen, a heatmap of how players manoeuvred around the game can be built, illustrated in figure 4.7 for all players. Figure 4.8 shows group R_A and figure 4.9 shows group R_B.

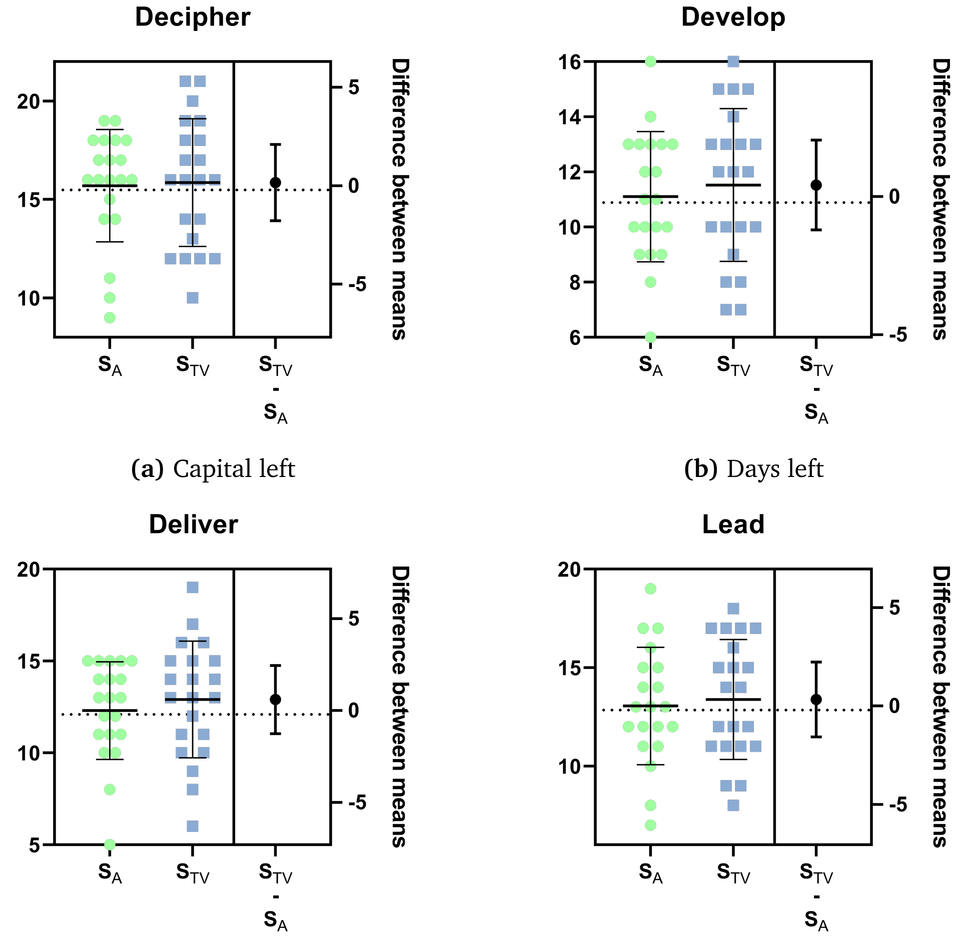
These highlight the similarities and some differences in how R_A manoeuvred around the game, and how R_B did. If the threshold of not reaching a consensus is set to five or more players (25%) in either R_A or R_B choosing a different path. Both groups seem to have reached a consensus on questions Q1, Q2, Q3, Q4, Q6,



(a) Capital left

(b) Days left

Figure 4.5: Resources left



(a) Capital left

(b) Days left

(c) Days left

(d) Days left

Figure 4.6: Dechiper, develop, deliver and lead

Q8 and Q9. Leaving Q5 and Q7 with different consensus. Both for Q5 and Q7 the second most popular answer of one group is the most popular of the other.

If a player would choose to answer the game with the most popular movement from figure 4.7. The player would receive the highest score registered of 83, only accomplished by 1 player. Should the player choose the most popular answers of group R_A, the final culture score would be 70. Taking the path of group R_B, the player would receive a final culture score of 86. Nobody took this path, and the score is 3 points higher than the top scorer of the game.

4.3 Comparing GTS and ER

When triangulating the findings from GTS and ER they are not directly comparable. The GTS has shown that socobertech is an emerging and growing field. The findings with the most synergy between the methodologies are between the ER and the result of the game developed by Frey *et al.* [79]. Both results indicate that balance is key when facilitating strategic decision-making.

There are however no clear overlaps between findings from the GTS and the ER. Further analysis and interpretations of findings will be discussed in the next chapter and section 5.3 due to the fact that there are no obvious connections, similarities or signs of divergence between the methodologies.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
a)	2	5	4	5	12	8	4	9	9
b)	16	17	10	18	6	2	15	7	4
c)	19	8	2	2	15	11	3	3	8
d)	10	11	25	16	8	20	19	22	20

Figure 4.7: How players have moved through the game

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
a)	1	2	1	4	5	2	1	4	3
b)	4	9	6	7	2	2	10	3	3
c)	8	5	1	1	10	5	2	0	3
d)	7	4	12	8	3	11	7	13	11

Figure 4.8: How R_A has moved through the game

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9
a)	1	3	3	1	7	6	3	5	6
b)	6	8	4	11	4	0	5	4	1
c)	11	3	1	1	5	6	1	3	5
d)	3	7	13	8	5	9	12	9	9

Figure 4.9: How R_B has moved through the game

Chapter 5

Discussion

In this chapter, the discussion centres around the analysis findings and their contextualisation. The objective is to elaborate on the implications, explanations, and reasoning behind the results. This entails a comprehensive examination of the nature and causes of the findings, along with an evaluation of the strengths and weaknesses of the methods utilised. The discussion also seeks to derive meaningful insights from the analysis, offering a broader perspective on the research questions.

5.1 Research question 1

What information related to cybersecurity is key for strategic decision-making and management of operations based on ground theory?

The Grounded Theory Study did not offer a set answer, certain aspects, or key information that always needs to be addressed. However, it sheds light on the complexity of the whole and the factors that have or can have a decisive impact that must be considered in a strategic decision.

Cybersecurity has emerged as an indispensable aspect of strategic decision-making, especially in government, industry, and even personal domains. Despite its growing significance, as addressed by the GTS, there is a stark lack of comprehensive research on this subject, making it a fertile ground for future inquiry. Notably, the existent literature often lacks a nuanced understanding of the intricate dynamics between cybersecurity and strategic decision-making processes. This became particularly evident when attempting to determine how beneficial it is to prioritise value assessment over threat and vulnerability evaluations.

Multiple papers in the GTS recognised the considerable challenge in the interface between cybersecurity and strategic decision-making and the challenges of managing a multitude of variables and complex dependencies. Cybersecurity is inherently a multi-faceted domain, encompassing technical, business, human, and organisational elements, to name a few. Furthermore, these variables do not exist in isolation; rather, they interact and influence one another in ways that often exacerbate complexity. For instance, a decision to invest in a new cybersecurity technology might not just have financial implications. Still, it could also impact employee morale, alter workflow processes, and draw regulatory attention. Understanding the consequences of these decisions and how they might play out is challenging. Especially true for the cybersecurity expert that has to present the foundation of which the decision has to be made.

Compounding this complexity is the daunting task of delineating precise information requirements for strategic decision-making in cybersecurity. It is often challenging to pinpoint what information is needed, when it is required, and how it should be interpreted. The pace of change in the Cyber landscape, the overwhelming amount of data, the sophistication of threats, and the lack of standardised information gathering and analysis processes are some factors that contribute to this challenge. Therefore, it isn't easy to compare and link results between papers. Especially since the focus differs and the variables are hard to isolate. Additionally, comparing these papers introduces new biases from the researcher and the risk of faulty interpretation.

Perceptions and decision-making in cybersecurity can significantly differ among individuals. Different stakeholders might prioritise distinct aspects of cybersecurity based on their roles, experiences, and competencies. For example, a CIO may perceive cybersecurity from a technological perspective and favour investment in advanced security solutions. In contrast, a CEO may consider cybersecurity from a risk management perspective, thereby emphasising the establishment of a robust incident response plan. Such variations in perceptions and priorities necessitate a collaborative approach to strategic decision-making in cybersecurity, integrating diverse viewpoints to attain a holistic understanding and response.

Figure 4.2 illustrated in section 4.1.7 introduces a socobertech layer as a result of the GTS. The thought process behind this is for the conveyer to facilitate sound decision-making must concisely think about how to encode the message to the decision-maker(s). Additionally, the sender must be conscious of their perceptions and how different biases can affect the encoding. If done well, the sender can structure the knowledge that will be shared with the receivers to improve the decision-making process significantly. This can be through quantification models, simulations or matrices, but are not restricted to these. Based on their understanding of the different stakeholders, the sender chooses the best medium or channel to send the encoded message to facilitate the decision-making process optimally.

5.1.1 Findings

No substantial evidence in the Grounded Theory Study suggests that focusing on asset assessment is more beneficial to the strategic decision-making process than focusing on threat and vulnerability assessments. This is not because there are papers that conclude this is evident but because no collected research in the Grounded Theory Study addresses the weighting between the three. Most papers are natural to the hypothesis, but some pieces are in support of the focus on asset assessment but do not provide merit to there being a beneficial effect to focus more on asset assessment than threat and vulnerability assessments [40, 43, 46, 80, 81].

The material from the Grounded Theory Study did not have enough coherent results to be able to provide an answer to what essential information is vital for facilitating strategic decision-making. However, it provided evidence for the transdisciplinary nature of strategic decision-making in the Cyber domain. To give an answer or insight into research question **R1**, more studies have to be undertaken, focusing on making multiple variables to get a better grasp of how they interact and affect each other.

5.1.2 Limitation

Collections of material and papers for the GTS have been done through multiple tools, also utilising AI applications such as `https://iris.ai/`. The result of gathering material this way grants a lot of hits on relevant papers. The job then becomes filtering out the work that is not relevant to the problem statement of this thesis. This has been done by adding filters, viewing the title, abstract, and year, and sometimes reading the introduction. Due to the amount of information, multiple relevant papers might have been excluded unintentionally. Only the author could analyse and process Norwegian and English documents, missing pertinent papers from other languages.

The fact that the author has chosen and evaluated papers introduces a risk of bias, not including articles with contradicting titles or abstracts. Only one article in the GTS contradicted the problem description of the paper. This might be because more papers support the hypothesis than oppose it, or the author has not been neutral in selecting documents.

5.2 Research question 2

What cybersecurity factors are important for strategic decision-making and management of operations observed in the game?

During this research, the analysis did not uncover substantial evidence to support the assertion that asset assessment is of greater value than vulnerability and threat assessments in the context of strategic decision-making in cybersecurity. This could be attributed to several factors related to the gaming simulation employed in our study.

One critical factor might lie in the design and development of the game itself. It's plausible that the game did not sufficiently highlight the different strategic values associated with asset, vulnerability, and threat assessments. As a result, players might not have been adequately incentivised or guided to utilise the information at hand, skewing the results towards no significant difference.

Additionally, player engagement and information utilisation may also be contributing factors. The complexity and dynamism of the game could have led some players to not fully utilise the information presented, perhaps due to cognitive overload or a lack of familiarity with cybersecurity concepts. Suppose players overlooked or misunderstood the significance of the information presented. In that case, they may not have effectively integrated it into their decision-making process, which could explain the lack of observed value differences.

A related consideration is the potential for players to rush through the game, perhaps due to time constraints or a desire to achieve a high score quickly. This haste could hinder careful deliberation and strategic decision-making, thereby reducing the discernible impact of different types of assessments.

The limited number of players observed in the study may indicate that the player base was not diverse enough. It could be that players had similar backgrounds or knowledge levels, reducing the variance in their decision-making approaches and thus making it more challenging to identify significant differences in the value of various assessments. The target audience would preferably be in the strategic level category.

In light of these observations, future research might benefit from refining the game design to emphasise the unique value of different assessment types, ensuring players are sufficiently engaged and informed, providing adequate time for thoughtful decision-making, and increasing the player base to enhance the range of strategies employed.

5.2.1 Findings

There is no evidence in the ER and the game's result that an increased focus on asset assessment facilitates and provides improved strategic decision-making compared to threat and vulnerability assessments. The result of the ER indicates that a balance between asset, threat and vulnerability is likely to facilitate most optimally for strategic decision-making.

The paper's result neither provides additional insight into what factors are essential for strategic decision-making. In hindsight, the game should have collected more data points to detect other important factors. The decision not to collect more data points was not to gather more information than necessary, protecting the participants' privacy. The game could, however, collect more data points without increasing the risk regarding participants' privacy or increasing the data's sensitivity.

5.2.2 Limitations

The ER design did not include a third control group (or a placebo group), which could have offered a baseline measure for analysis. The absence of such a group may limit the generalizability of the findings and obscure any effects. Additionally, few data points on the players were gathered because of privacy concerns, making the analysis fall short. In hindsight, more information about the player's demographic, time spent on different questions, and reading background information should have been collected.

A potential limitation involves the Business Impact Analysis (BIA) and risk assessment documents provided to participants. Although these documents are crucial to informed decision-making, whether participants engaged with and comprehended these materials is unclear. Any discrepancies in reading or understanding these documents could impact the results and their interpretation.

The author's role in creating the BIA and risk assessments also warrants consideration. Despite efforts to maintain neutrality, the possibility of unintentional bias influencing these materials cannot be entirely ruled out. Future research might benefit from engaging multiple experts in creating these documents to ensure a balanced and comprehensive representation.

Additionally, the scoring system employed in the study was devised by the author. While every effort was made to ensure objectivity and fairness, any scoring system inherently involves a degree of subjectivity, which might introduce bias into the findings. The scoring systems mainly focus on the security culture as an evaluation of how well the player performs, and after that, analyse what decision and seed granted that security culture score. For that reason, it might be that a focus on asset assessment benefits the strategic decision-making. Still, it is not shown within the security culture score or the other metric employed in the game.

Finally, this study's use of gamification introduces a layer of uncertainty. The artificial nature of the game setting and the competitive aspects inherent to such an environment might influence participants' behaviours in ways that differ from real-world decision-making. As a result, the applicability of findings derived from the game to actual cybersecurity contexts may have some constraints.

5.3 An inquiry into the Nature and Causes of misunderstandings from Cable Ties to Neck Ties

How do key cybersecurity information for strategic decision-making and management of operations overlap with cybersecurity factors from the game?

Unfortunately, the GTS could not collect related data matching the problem description of this thesis. It encountered an emerging science that is growing but with limited quantitative data. The papers included quantitative data but did not isolate variables or manipulated dependencies relevant to this thesis.

The GTS indicates that the answer to the challenges that arise when strategic decisions related to Cyber is the best way to approach this is by gathering and structuring data and limiting the possibility of misunderstandings, and well suited for providing foundations for strategic decision-making. This sounds reasonable and a common approach. However, the GTS does not unveil that it makes for excellent and well-informed decision-making. Although the information can be structured skillfully, information overload and misinterpretation because of technical jargon due to shallow common ground, high levels of uncertainty in the data, and weak links can be real pitfalls even when the data presented is skillfully structured.

This thesis, therefore, introduces the socobertech term. To highlight the transdisciplinary nature of strategic decision-making in the Cyber domain. This thesis hypothesised that asset assessment provides a stronger foundation for strategic decision-making and operation management than a threat or vulnerability assessment. No substantial evidence for this has been observed either in the GTS or the ER. There is evidence when comparing the GTS and the ER for stating that a balanced approach towards the decision-maker benefits the decision-making process. Not leaning toward either, but find a natural approach suited for the receiver. This thesis, therefore, suggests that the sender should mindfully approach the message and encoding for the message to the receiver to facilitate the decision-making process. Understating how the data should be structured to facilitate informed decision-making.

This thesis can not confirm the introduction of the socobertech layer, as illustrated in figure 4.2, will improve the foundation of the strategic decision-making, leading to well-informed decision-making. Based on the findings of this thesis, it is the updated hypothesis that if the cybersecurity expert intentionally considers the socobertech layer and uses this as input in structuring the message to the decision-making, this will likely lead to improved decision-making, that is well informed.

5.3.1 Findings

Research question **R3** aims to assess the validity of the hypothesis by comparing the results obtained from research questions **R1** and **R2**. However, the analysis revealed limited overlap and challenges in finding common data points shared between the two research questions. The complexity lies in isolating and identifying comparable data due to inherent differences in data sources, methodologies, and variables. Consequently, determining the feasibility of comparing the data becomes intricate and requires careful consideration.

Comparing GTS and ER yielded no evidence or significant results to support the hypothesis. The hypothesis is not disproven either but can not be confirmed by the result of this paper.

5.3.2 Limitations

Although both methods were valid in their own right, the GTS and the ER methodologies did not yield directly comparable results. There was a hope that the GTS had more relatable information regarding the game results. The findings derived from comparing these two methodologies should, for that reason, be interpreted with caution.

The study offers valuable insights, but these limitations highlight the need for additional research to further refine our understanding of strategic decision-making in cybersecurity. Future studies should consider these limitations when designing their methodology to ensure the robustness and validity of their findings.

5.3.3 Addressing the problem statement

How can cybersecurity professionals effectively communicate complex cybersecurity issues to non-technical leaders and facilitate their understanding of potential risks and implications, to improve strategic decision-making?

In the finishing phase of this master's thesis, on May 9th, 2023, the The Norwegian National Security Authority published their report 'Security Advisory - A Resilient Norway' (*Sikkerhetsfaglig råd - Et motstandsdyktig Norge*) [112]. In the report, they address the competence shortage of security experts and the lack of national cyber situational awareness mentioned in section 1.1 of this thesis [24, 25]. The report mainly describes six domains that threat actors manipulate to harm Norwegian national security interests [112, p. 15] [113]. These are 'cyber', 'personnel', 'physical', 'economical', 'cognitive' and 'space'. These domains are described in the report as multidisciplinary with some interdisciplinary characteristics. With the old hypothesis of this paper, the security challenges within each of these domains should be addressed to the strategic decision-makers with a focus on the assets found in each domain. This approach is described as a defensive security concept in the report [112, p. 14].

However, the new evidence of this thesis indicates that this does not provide any improvement to the strategic decision-making process, with the receivers of this report being the Norwegian authorities. The result of this thesis suggests that this multidisciplinary is sub-optimal, chiefly due to the shortage of talented resources. Not providing strategic decision-makers on the executive level and the business and management level with the optimal foundation for well-informed decisions for the management of operations and, thereby, national security.

A defensive security concept with a transdisciplinary approach would likely reduce the possibility of misunderstandings and faulty decision-making data. Partially addressing and mitigating the shortage of security professionals. Moreover, the approach would help in facilitating effective communication for complex cybersecurity issues to non-technical leaders, improving cross-sectoral collaboration in building cyber resiliency through a defensive security concept with a truly holistic approach. However, this thesis indicates that this would be a more sustainable approach. It has to be further researched to have any reasonable claim behind it.

Chapter 6

Conclusion

As the exploration of cybersecurity and strategic decision-making concludes, it's imperative to acknowledge that we are only at the threshold of understanding the intricate dynamics of this burgeoning field. As digital technologies become increasingly embedded in our lives and societies, the criticality and complexity of cybersecurity will continue to grow. Consequently, it is of utmost importance that we invest in extensive research to keep pace with these changes and inform effective strategies and decision-making processes.

While the experimental research conducted in this study did not conclusively confirm the initial hypothesis, it nonetheless offered valuable insights. It's essential to recognise that the absence of clear affirmation does not indicate a failure; instead, it underscores the complexity and dynamism inherent in the cybersecurity domain.

Notably, the research contributed to the accumulation of data points in this complex field, providing a foundation for further exploration and understanding. The results prompt us to continually reconsider and refine our theories and assumptions, an integral part of the scientific process.

The game theory simulations and event-response approaches employed in this study facilitated the gathering of diverse data, unveiling interactions and dependencies that might otherwise remain hidden in real-world scenarios. Furthermore, these methods highlighted the limitations and challenges associated with assessing different types of information in decision-making, calling for more nuanced and comprehensive models.

In conclusion, while our understanding of strategic decision-making in cybersecurity is still evolving, this research signifies a step forward in the right direction. As the field continues to grow, so too should our pursuit of knowledge. With each research endeavour, we edge closer to developing strategies that can adeptly navigate the complexities of cybersecurity, safeguarding our digital landscapes for the generations to come.

6.1 Future work

This paper has mainly focused on the continuation of related works, primarily the master's thesis by Tiril Ligaya Tinde and the bachelor's project by Artūrs Umbraško, Kacper Lewandowski, and Danie Dahl [26, 27]. Moreover, the open source development of the cybersecurity game has laid the foundation for collecting more information and improving upon this thesis.

As this master's thesis draws to a close, it opens a multitude of avenues for future research. While the study has offered significant insights into the complexities of strategic decision-making in cybersecurity, it is by no means exhaustive. One notable area ripe for further exploration is the interplay between social and technical aspects of cybersecurity, the sociotechnical perspective and then combined it with behavioural science and decision-making theory where variables are carefully controlled. A transdisciplinary field coined socobertech in this thesis.

The socobertech perspective recognises that cybersecurity and decision-making is not solely a technical issue but is deeply intertwined with social elements. This perspective necessitates a broader lens, one that incorporates human behaviour, organisational culture, policy, and law alongside technical considerations. Unpacking these socobertech dynamics is key to a holistic understanding of cybersecurity and to the development of effective, sustainable strategies for facilitating strategic decision-making.

Future research could thus focus on expanding this inquiry by incorporating more diverse data sources, such as interviews with a broader range of stakeholders, ethnographic studies of cybersecurity practices in organisations, or analyses of policy and regulatory impacts on decision-making. Additionally, employing different methodological approaches, such as mixed methods or interdisciplinary research designs, could enhance our understanding of these socobertech interactions.

Building on the foundation laid by this thesis, such future work has the potential to uncover deeper, richer insights into the socobertech complexities of cybersecurity. Doing so could contribute significantly to our collective efforts to navigate the digital future safely and responsibly. The necessity of research becomes even more paramount considering the accelerated digitisation and ubiquity of cyberattacks, forcing us to reevaluate our assumptions and beliefs regularly. Despite the constraints and challenges, the urgency and importance of this research make it a worthy endeavour, promising to yield valuable dividends for the scholarly community, practitioners, and society at large.

Bibliography

[1] N. I. of Standards and C. s. r. c. Technology. ‘Csrc glossary - best practice.’ (), [Online]. Available: `https://csrc.nist.gov/glossary/term/best_practice` (visited on 09/04/2023).

[2] N. I. of Standards and C. s. r. c. Technology. ‘Csrc glossary - cyber.’ (), [Online]. Available: `https://csrc.nist.gov/glossary/term/cyber` (visited on 07/04/2023).

[3] N. I. of Standards and C. s. r. c. Technology. ‘Csrc glossary - cyber resiliency.’ (), [Online]. Available: `https://csrc.nist.gov/glossary/term/cyber_resiliency` (visited on 07/04/2023).

[4] U. Franke and J. Brynielsson, ‘Cyber situational awareness – a systematic review of the literature,’ eng, *Computers & security*, vol. 46, pp. 18–31, 2014, ISSN: 0167-4048.

[5] C. Brookson, S. Cadzow, R. Eckmaier, J. Eschweiler, B. Gerber, A. Guarino, K. Rannenberg, J. Shamah and S. Górniak, *Definition of cybersecurity: gaps and overlaps in standardisation*, eng. Heraklion: ENISA, 2015, ISBN: 929204155X.

[6] I. T. U. T. S. Sector. ‘Definition of cybersecurity: Gaps and overlaps in standardisation.’ (Dec. 2015), [Online]. Available: `https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx` (visited on 07/04/2023).

[7] N. I. of Standards and C. s. r. c. Technology. ‘Csrc glossary - cyberspace.’ (), [Online]. Available: `https://csrc.nist.gov/glossary/term/cyberspace` (visited on 07/04/2023).

[8] D. Moskowitz, *Fundamentals of adopting the nist cybersecurity framework.* eng, London, 2022.

[9] P. D. Leedy and J. E. Ormrod, *Practical Research: Planning and Design*. Pearson Higher Education, 1992.

[10] Nettskjema. ‘Nettskjema front page.’ (), [Online]. Available: `https://nettskjema.no/`. (accessed: 12.03.2023).

[11] N. I. of Standards and C. s. r. c. Technology. 'Risk management framework for information systems and organizations: A system life cycle approach for security and privacy.' (), [Online]. Available: `https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final` (visited on 25/04/2023).

[12] National Institute of Standards and Technology. 'Managing information security risk: Organization, mission, and information system view.' (Mar. 2011), [Online]. Available: `https://csrc.nist.gov/publications/detail/sp/800-39/final` (visited on 06/12/2022).

[13] N. I. of Standards and C. s. r. c. Technology. 'Security and privacy controls for information systems and organizations.' (), [Online]. Available: `https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final` (visited on 25/04/2023).

[14] Standards Norway, *Krav til risikovurderinger = requirements for risk assessment*, nob, Oslo: Standard Norge, 2021.

[15] A. da Veiga, L. V. Astakhova, A. Botha and M. Herselman, 'Defining organisational information security culture—perspectives from academia and industry,' eng, *Computers & security*, vol. 92, pp. 101 713–23, 2020, ISSN: 0167-4048.

[16] W. Pasmore, S. Winby, S. A. Mohrman and R. Vanasse, 'Reflections: Sociotechnical systems design and organization change,' eng, *Journal of change management*, vol. 19, no. 2, pp. 67–85, 2019, ISSN: 1469-7017.

[17] M. Kyriakidis, V. Kant, S. Amir and V. N. Dang, 'Understanding human performance in sociotechnical systems – steps towards a generic framework,' eng, *Safety science*, vol. 107, pp. 202–215, 2018, ISSN: 0925-7535.

[18] NIST. 'Framework for improving critical infrastructure cybersecurity.' (), [Online]. Available: `https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf` (visited on 08/04/2023).

[19] C. Klimas. 'Twine front page.' (), [Online]. Available: `https://twinery.org/`. (accessed: 12.03.2023).

[20] T. N. Government. 'Nasjonal strategi for digital sikkerhetskompetanse.' (Jan. 2019), [Online]. Available: `https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf` (visited on 06/04/2023).

[21] M. of Justice and P. Security. 'Digital sårbarhet – sikkert samfunn.' (Nov. 2015), [Online]. Available: `https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf` (visited on 06/04/2023).

[22] KPMG. 'Nasjonal strategi for digital sikkerhetskompetanse.' (Jul. 2018), [Online]. Available: `https://assets.kpmg.com/content/dam/kpmg/no/pdf/2018/07/topplederundersokelsen-2018.pdf` (visited on 06/04/2023).

[23] M. S. Mark, C. N. Tømte and T. Terje Røsdal. 'Ikt-sikkerhetskompetanse i arbeidslivet – behov og tilbud.' (Dec. 2017), [Online]. Available: `http://hdl.handle.net/11250/2490041` (visited on 06/04/2023).

[24] T. O. of the Auditor General of Norway. 'Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.' (Feb. 2023), [Online]. Available: `https://www.riksrevisjonen.no/rapporter-mappe/no-2022-2023/undersokelse-av-myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor/` (visited on 06/04/2023).

[25] NSM. 'Risiko 2022.' (Feb. 2022), [Online]. Available: `https://nsm.no/getfile.php/137798-1644424185/NSM/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf` (visited on 06/04/2023).

[26] T. L. Tinde, *Cyber threat information requirements for strategic decision-making*, eng, 2022. [Online]. Available: `https://hdl.handle.net/11250/3014795`.

[27] A. Umbraško, K. Lewandowski and D. Dahl, *Os runner*, eng, 2021. [Online]. Available: `https://hdl.handle.net/11250/2777964`.

[28] SANS. 'Introducing the mgt512 cyber42 security leadership simulation.' (Apr. 2020), [Online]. Available: `https://www.sans.org/blog/introducing-the-mgt512-cyber42-security-leadership-simulation/` (visited on 06/04/2023).

[29] U. S. (10077), 'The benefit of value assessments in strategic security decision-making and management of operations,' eng, 2022.

[30] NIST. 'About nist.' (), [Online]. Available: `https://www.nist.gov/about-nist` (visited on 07/04/2023).

[31] NIST. 'Publications.' (), [Online]. Available: `https://csrc.nist.gov/publications` (visited on 07/04/2023).

[32] NTNU. 'Information security: Experience-based master's degree, 3 years, gjøvik.' (), [Online]. Available: `https://www.ntnu.edu/studies/miseb` (visited on 07/04/2023).

[33] P. Di Toma and S. Ghinoi, 'Overcoming hierarchy in business model innovation: An actor-oriented approach,' eng, *European journal of innovation management*, vol. 24, no. 4, pp. 1057–1081, 2021, ISSN: 1460-1060.

[34] Norwegian National Security Authority. 'Grunnprinsipper for ikt-sikkerhet 2.0.' (Jun. 2020), [Online]. Available: `https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/malgruppe/` (visited on 06/12/2022).

[35] M. Whitman, *Management of information security*, eng, 2017.

[36] I. L. Organization. 'Industries and sectors.' (Dec. 2022), [Online]. Available: `https://www.ilo.org/global/industries-and-sectors/lang--en/index.htm` (visited on 05/12/2022).

[37] F. Kim. 'Mgt514: Security strategic planning, policy, and leadership,' SANS. (Jul. 2022), [Online]. Available: `https://www.sans.org/cyber-security-courses/security-strategic-planning-policy-leadership/` (visited on 21/11/2022).

[38] Karsten Friis and Håkon Bergsjø, *Digitalisering og internasjonal politikk*. Universitetsforlaget, 2022.

[39] I. Lahlou, *Corporate Board of Directors: Structure and Efficiency*, eng. Cham: Springer International Publishing, 2018, ISBN: 3030050173.

[40] Forsvarsbygg. 'Sikringshåndboka.' (2022), [Online]. Available: `https://www.forsvarsbygg.no/sikringshandboka/` (visited on 07/12/2022).

[41] D. Maclean, *The NIST Risk Management Framework: Problems and recommendations.* 2017.

[42] Forsvaret. 'Forsvarets etterretningsdoktrine (2021).' (), [Online]. Available: `https://www.etterretningstjenesten.no/publikasjoner/etterretningsdoktrinen/Etterretningsdoktrine_2021_Web_LoRes_02.pdf/_/attachment/inline/633b7840-43de-42af-bb89-243d81076208:edd1367bd55a434b4489162637336d7d632d42a`
`Etterretningsdoktrine_2021%5C%20-%5C%20Web_LoRes%5C%2002%5C%20(PROD).pdf`. (accessed: 23.04.2023).

[43] ". B. " M. " H. K. " Endregard". 'Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.' (2015), [Online]. Available: `https://www.ffi.no/publikasjoner/arkiv/tilnaerminger-til-risikovurderinger-for-tilsiktede-uonskede-handlinger` (visited on 07/12/2022).

[44] P. Weill, *It governance : How top performers manage it decision rights for superior results*, eng, Boston, 2004.

[45] L. S. Lervik. 'Konsept for utvikling av hæren: Morgendagens hær.' (), [Online]. Available: `https://www.forsvaret.no/om-forsvaret/organisasjon/haeren/morgendagens-haer.pdf/_/attachment/inline/e14ad896-886e-49f7-a99d-ebfc0729a056:0182b3d2c7fcc6459eef5510b2f046e2fdfd367b/Morgendagens%5C%20haer.pdf`. (accessed: 23.04.2023).

[46] V. LeVeque, *Information security : A strategic approach*, eng, Hoboken, New Jersey, 2006.

[47] Norwegian National Security Authority. 'Grunnprinsipper.' (2022), [Online]. Available: `https://nsm.no/regelverk-og-hjelp/grunnprinsipper/` (visited on 07/12/2022).

[48] M. Sas, W. Hardyns, K. van Nunen, G. Reniers and K. Ponnet, 'Measuring the security culture in organizations: A systematic overview of existing tools,' eng, *Security journal*, vol. 34, no. 2, pp. 340–357, 2021, ISSN: 0955-1662.

[49] K. Roer, *Build a security culture*, eng, Cambridgeshire, England, 2015.

[50] ENISA. ‘Cyber security culture in organisations.’ (2018), [Online]. Available: `https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations` (visited on 02/05/2023).

[51] *Cybersecurity awareness*, eng, Cham, Switzerland, 2022.

[52] N. Neshenko, *Smart cities : Cyber situational awareness to support decision making*, eng, Cham, Switzerland, 2022.

[53] P. Emami-Naeini, H. Dixon, Y. Agarwal and L. Cranor, ‘Exploring how privacy and security factor into iot device purchase behavior,’ eng, in *Conference on Human Factors in Computing Systems - Proceedings*, ser. CHI ’19, ACM, 2019, pp. 1–12, ISBN: 1450359701.

[54] M. W. Bailey, ‘Seduction by technology: Why consumers opt out of privacy by buying into the internet of things,’ eng, *Texas law review*, vol. 94, no. 5, pp. 1023–1054, 2016, ISSN: 0040-4411.

[55] M. Williams, J. R. C. Nurse and S. Creese, ‘"privacy is the boring bit": User perceptions and behaviour in the internet-of-things,’ eng, 2018.

[56] F.-J. Sarabia-Sánchez, J.-M. Aguado and I. J. Martínez-Martínez, ‘Privacy paradox in the mobile environment: The influence of the emotions,’ eng ; spa, *El profesional de la informacion*, vol. 28, no. 2, 2019, ISSN: 1386-6710.

[57] *Privacy online : Perspectives on privacy and self-disclosure in the social web*, eng, Berlin, Heidelberg, 2011.

[58] Clayton M. Christensen. ‘How will you measure your life?’ (Jul. 2010), [Online]. Available: `https://hbr.org/2010/07/how-will-you-measure-your-life` (visited on 09/04/2023).

[59] The Norwegian Business and Industry Security Council. ‘Mørketallsundersøkelsen 2022.’ (Oct. 2022), [Online]. Available: `https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen` (visited on 08/12/2022).

[60] M. Christen and B. Gordijn, ‘A review of value-conflicts in cybersecurity : An assessment based on quantitative and qualitative literature analysis,’ 2017.

[61] G. Østby, S. J. Kowalski and B. Katt, ‘Towards a maturity improvement process – systemically closing the socio-technical gap,’ eng, 2020, ISSN: 1613-0073. [Online]. Available: `https://hdl.handle.net/11250/2737120`.

[62] K. Shilton, M. Subramaniam, J. Vitak and S. J. Winter, ‘Qualitative approaches to cybersecurity research,’ 2016.

[63] J. Hughes and G. Cybenko, ‘Quantitative metrics and risk assessment: The three tenets model of cybersecurity,’ eng, *Technology innovation management review*, vol. 3, no. 8, pp. 15–24, 2013, ISSN: 1927-0321.

[64] D. Fujs, A. Mihelič and S. Vrhovec, 'The power of interpretation: Qualitative methods in cybersecurity research,' eng, in *ACM International Conference Proceeding Series*, ser. ARES '19, ACM, 2019, pp. 1–10, ISBN: 9781450371643.

[65] J. K. Jesson, *Doing your literature review : Traditional and systematic techniques*, eng, London, 2011.

[66] N. Oria. 'Databaser.' (), [Online]. Available: `https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/dbsearch?vid=NTNU_UB%5C&lang=en_US`. (accessed: 16.04.2023).

[67] Sikt. 'Oria – fagbibliotekenes søkeportal.' (), [Online]. Available: `https://sikt.no/tjenester/oria-fagbibliotekenes-sokeportal`. (accessed: 16.04.2023).

[68] K. M. Carley, 'Social cybersecurity: An emerging science,' eng, *Computational and mathematical organization theory*, vol. 26, no. 4, pp. 365–381, 2020, ISSN: 1381-298X.

[69] D. W. Straub and R. J. Welke, 'Coping with systems risk: Security planning models for management decision making,' eng, *MIS quarterly*, vol. 22, no. 4, pp. 441–469, 1998, ISSN: 0276-7783.

[70] A. Quaadgras, P. Weill and J. W. Ross, 'Management commitments that maximize business impact from it,' eng, *Journal of information technology*, vol. 29, no. 2, pp. 114–127, 2014, ISSN: 0268-3962.

[71] 'Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective,' eng, *Issues in information systems*, 2015, ISSN: 1529-7314.

[72] L. Keller and J. Ho, 'Decision problem structuring: Generating options,' eng, *IEEE transactions on systems, man, and cybernetics*, vol. 18, no. 5, pp. 715–728, 1988, ISSN: 0018-9472.

[73] A. Moallem, 'Social preferences in decision making under cybersecurity risks and uncertainties,' eng, in *HCI for Cybersecurity, Privacy and Trust*, ser. Lecture Notes in Computer Science, vol. 11594, Switzerland: Springer International Publishing AG, 2019, pp. 149–163, ISBN: 9783030223502.

[74] S. Rass, *Cyber-security in critical infrastructures : A game-theoretic approach*, eng, Cham, 2020.

[75] A. F. Brantly, *The decision to attack : Military and intelligence cyber decision-making*, eng, Athens, Georgia, 2016.

[76] P. Liu, S. Jajodia and C. Wang, *Theory and models for cyber situation awareness*, eng, Cham, 2017.

[77] D. Stepanova, S. E. Parkin and A. v. Moorsel, 'A knowledge base for justified information security decision-making,' eng, 2009. [Online]. Available: `https://citeseerx.ist.psu.edu/doc/10.1.1.149.1260`, (accessed: 09.02.2023).

[78] G. Dhillon and G. Torkzadeh, 'Value-focused assessment of information system security in organizations,' eng, *Information systems journal (Oxford, England)*, vol. 16, no. 3, pp. 293–314, 2006, ISSN: 1350-1917.

[79] S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque and S. A. Naqvi, 'The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game,' eng, *IEEE transactions on software engineering*, vol. 45, no. 5, pp. 521–536, 2019, ISSN: 0098-5589.

[80] A. Ibrahim, C. Valli, I. McAteer and J. Chaudhry, 'A security review of local government using nist csf: A case study,' eng, *The Journal of supercomputing*, vol. 74, no. 10, pp. 5171–5186, 2018, ISSN: 0920-8542.

[81] A. Kohnke, K. Sigler and D. Shoemaker, 'Strategic risk management using the nist risk management framework,' eng, *EDPACS*, vol. 53, no. 5, pp. 1–6, 2016, ISSN: 0736-6981.

[82] M. P. Sallos, A. Garcia-Perez, D. Bedford and B. Orlando, 'Strategy and organisational cybersecurity: A knowledge-problem perspective,' eng, *Journal of intellectual capital*, vol. 20, no. 4, pp. 581–597, 2019, ISSN: 1469-1930.

[83] Z. A. Collier, I. Linkov and J. H. Lambert, 'Four domains of cybersecurity: A risk-based systems approach to cyber decisions,' eng, *Environment systems & decisions*, vol. 33, no. 4, pp. 469–470, 2013, ISSN: 2194-5403.

[84] D. Bojanić, J. Marček, I. Vulić and V. Ristić. 'Designing cybersecurity management bodies in strategic planning: Application of hybrid analysis.' (), [Online]. Available: `https://www.atlantis-press.com/proceedings/senet-19/125925994` (visited on 19/05/2023).

[85] S. Norway. '577 067 virksomheter i norge.' (Jan. 2018), [Online]. Available: `https://www.ssb.no/virksomheter-foretak-og-regnskap/artikler-og-publikasjoner/577-067-virksomheter-i-norge` (visited on 08/12/2022).

[86] G. Prism. 'The ultimate guide to t tests.' (), [Online]. Available: `https://www.graphpad.com/guides/the-ultimate-guide-to-t-tests.` (accessed: 07.05.2023).

[87] GPower. 'G*power.' (), [Online]. Available: `https://www.psychologie.hhu.de/arbeitsgruppen/allgemeine-psychologie-und-arbeitspsychologie/gpower.` (accessed: 07.05.2023).

[88] S. solutions. 'How to determine sample size from g*power.' (), [Online]. Available: `https://www.statisticssolutions.com/how-to-determine-sample-size-from-gpower/.` (accessed: 07.05.2023).

[89] NTNU. 'Data collection.' (), [Online]. Available: `https://i.ntnu.no/wiki/-/wiki/English/Data+collection.` (accessed: 12.03.2023).

[90] NTNU. 'Skjemaverktøy.' (), [Online]. Available: `https://i.ntnu.no/wiki/-/wiki/Norsk/Skjemaverkt%5C%C3%5C%B8y` (visited on 09/04/2023).

[91] Twine. 'Welcome to the twine cookbook.' (), [Online]. Available: https://twinery.org/cookbook/ (visited on 09/04/2023).

[92] Twine. 'Twine manual.' (), [Online]. Available: https://twine2.neocities.org/ (visited on 09/04/2023).

[93] Twine. 'Twine guide.' (), [Online]. Available: https://twinery.org/reference/en/index.html (visited on 09/04/2023).

[94] D. Cox. 'Working with google sheets in twine.' (), [Online]. Available: https://videlais.com/2018/05/16/working-with-google-sheets-in-twine/ (visited on 10/04/2023).

[95] itch.io. 'About itch.io.' (), [Online]. Available: https://itch.io/docs/general/about (visited on 11/04/2023).

[96] OpenAI. 'Introducing chatgpt.' (), [Online]. Available: https://openai.com/blog/chatgpt. (accessed: 28.05.2023).

[97] U. Sagelvmo. 'Trouble-free logistics.' (), [Online]. Available: https://ulrikasa.itch.io/trouble-free-logistics/. (accessed: 29.04.2023).

[98] U. Sagelvmo. 'The benefit of value assessments in strategic security decision-making (gamified survey for everyone).' (), [Online]. Available: https://www.reddit.com/r/takemysurvey/comments/11vn4nk/the_benefit_of_value_assessments_in_strategic/. (accessed: 29.04.2023).

[99] U. Sagelvmo. 'Trouble-free logistics.' (), [Online]. Available: https://www.facebook.com/groups/2682205105123422/user/1551499312. (accessed: 29.04.2023).

[100] U. Sagelvmo. 'Trouble-free logistics.' (), [Online]. Available: https://ulrikasa.itch.io/trouble-free-logistics/. (accessed: 29.04.2023).

[101] BBC. 'Technology.' (), [Online]. Available: https://www.bbc.com/news/technology. (accessed: 29.04.2023).

[102] WIRED. 'Home page.' (), [Online]. Available: https://www.wired.com/. (accessed: 29.04.2023).

[103] 'Hack 5 threat wire series.' (), [Online]. Available: https://www.youtube.com/@hak5/videos. (accessed: 29.04.2023).

[104] NRK. 'Home page.' (), [Online]. Available: https://www.nrk.no/. (accessed: 29.04.2023).

[105] Digi. 'Home page.' (), [Online]. Available: https://www.digi.no/. (accessed: 29.04.2023).

[106] NSM. 'Home page.' (), [Online]. Available: https://nsm.no/. (accessed: 29.04.2023).

[107] T. N. C. S. C. (UK). 'The national cyber security center uk.' (), [Online]. Available: https://www.ncsc.gov.uk/. (accessed: 29.04.2023).

[108] ISO/IEC. 'Iso/iec 27001 information security management systems.' (), [Online]. Available: `https://www.iso.org/standard/27001`. (accessed: 20.05.2023).

[109] L. Rajbhandari and E. Snekkenes, 'Using the conflicting incentives risk analysis method,' eng, in *Security and Privacy Protection in Information Processing Systems*, ser. IFIP Advances in Information and Communication Technology, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 315–329, ISBN: 9783642392177.

[110] L. Milică and D. K. Pearlson. 'Boards are having the wrong conversations about cybersecurity.' (), [Online]. Available: `https://hbr.org/2023/05/boards-are-having-the-wrong-conversations-about-cybersecurity`. (accessed: 21.05.2023).

[111] G. Prism. 'Choosing a normality test.' (), [Online]. Available: `https://www.graphpad.com/guides/prism/latest/statistics/stat_choosing_a_normality_test.htm`. (accessed: 07.05.2023).

[112] NSM, 'Sikkerhetsfaglig råd - et motstandsdyktig norge,' nor, 2023.

[113] ". of Justice and P. Security", *Act relating to national security (Security Act)*, eng. Lovdata, 2018.

[114] NTNU. 'Filling out the master agreement.' (), [Online]. Available: `https://i.ntnu.no/wiki/-/wiki/English/Filling+out+the+master+agreement`. (accessed: 28.05.2023).

[115] NTNU. 'Research project planning.' (), [Online]. Available: `https://www.ntnu.edu/studies/courses/IMT4205#tab=omEmnet` (visited on 09/04/2023).

[116] Sikt. 'Information and consent.' (), [Online]. Available: `https://sikt.no/en/information-and-consent`. (accessed: 12.03.2023).

[117] U. Sagelvmo. 'Trouble-free-logstics.' (), [Online]. Available: `https://github.com/usagelvmo/Trouble-free-logstics.git`. (accessed: 09.04.2023).

[118] K. J. Sund, R. J. Galavan and A. S. Huff, *Uncertainty and Strategic Decision Making*, eng. Bingley: Emerald Publishing Limited, 2016, ISBN: 9781786351708.

Appendix A

Master agreement

This appendix prints the master's agreement for this thesis, a document required by the Norwegian University of Science and Technology (NTNU) [114]. More information on the master's agreement can be found on NTNU web-page `https://i.ntnu.no/wiki/-/wiki/English/Filling+out+the+master+agreement` [114].

Note that the project initially planned to perform a risk assessment and data management plan for the thesis. This field is ticked "Yes". However, in discussions with Sikt, the project was reevaluated and did not require the participants to provide personally identifiable information. For that reason, no risk assessment and data management plan was needed. The thesis did not work out an updated assessment but has followed the risk assessment and data management plan laid out in the preliminary project [29].

Masteravtale/hovedoppgaveavtale

Sist oppdatert 11. november 2020

Fakultet	**Fakultet for informasjonsteknologi og elektroteknikk**
Institutt	**Institutt for informasjonssikkerhet og kommunikasjonsteknologi**
Studieprogram	**MISEB**
Emnekode	**IMT4905**

Studenten

Etternavn, fornavn	**Sagelvmo, Ulrik Andreas**
Fødselsdato	**01.04.1993**
E-postadresse ved NTNU	**ulrikasa@stud.ntnu.no**

Tilknyttede ressurser

Veileder	**Ivar Kjærem**
Eventuelle medveiledere	
Eventuelle medstudenter	

Oppgaven

Oppstartsdato	**02.01.2023**
Leveringsfrist	**01.06.2023**
Oppgavens arbeidstittel	**The benefit of value assessments in strategic security decision-making**
Problembeskrivelse	**Threats in the digital domain poses as a potential existential threat many business. How are business meant to maneuver in this space, building resilience while enabling the business to take risk to achieve competitive advantage, delivering services with high degree of satisfaction and safety? The hypothesis is that to take long-term strategic decisions the organization has to understand its values. This is especially true for the operative level when they communicate with the strategic level. When communicating the need for digital security the operative level has a tendency to focus on threats and vulnerabilities. Though the strategic level have little insight into digital threats and vulnerabilities. They have however, understanding for the business and assets. For that reason, the operative level should communicate how threats and vulnerabilities affects organizational assets. The thesis therefore wants to study the benefits of value assessments in strategic security decision-making and management of operations.**

Risikovurdering og datahåndtering

Skal det gjennomføres risikovurdering? **Dersom «ja», har det blitt gjennomført?**	**Ja** **Nei**
Skal det søkes om godkjenninger? (REK*, NSD)**	**Ja**
Skal det skrives en konfidensialitetsavtale i forbindelse med oppgaven? **Hvis «ja», har det blitt gjort?**	**Nei** **Nei**

* Regionale komiteer for medisinsk og helsefaglig forskningsetikk (https://rekportalen.no)

** Norsk senter for forskningsdata (https://nsd.no/)

Eventuelle emner som skal inngå i mastergraden

Security, Communication system security, digital security, risk management, security management, business communication system operations and management, value assessment, threat assessment, vulnerability assessment

Retningslinjer - rettigheter og plikter

Formål

Avtale om veiledning av masteroppgaven/hovedoppgaven er en samarbeidsavtale mellom student, veileder og institutt. Avtalen regulerer veiledningsforholdet, omfang, art og ansvarsfordeling.

Studieprogrammet og arbeidet med oppgaven er regulert av Universitets- og høgskoleloven, NTNUs studieforskrift og gjeldende studieplan. Informasjon om emnet, som oppgaven inngår i, finner du i emnebeskrivelsen.

Veiledning

Studenten har ansvar for å

- Avtale veiledningstimer med veileder innenfor rammene master-/hovedoppgaveavtalen gir.
- Utarbeide framdriftsplan for arbeidet i samråd med veileder, inkludert veiledningsplan.
- Holde oversikt over antall brukte veiledningstimer sammen med veileder.
- Gi veileder nødvendig skriftlig materiale i rimelig tid før veiledning.
- Holde instituttet og veileder orientert om eventuelle forsinkelser.
- Inkludere eventuell(e) medstudent(er) i avtalen.

Veileder har ansvar for å

- Avklare forventninger om veiledningsforholdet.
- Sørge for at det søkes om eventuelle nødvendige godkjenninger (etikk, personvernhensyn).
- Gi råd om formulering og avgrensning av tema og problemstilling, slik at arbeidet er gjennomførbart innenfor normert eller avtalt studietid.
- Drøfte og vurdere hypoteser og metoder.
- Gi råd vedrørende faglitteratur, kildemateriale, datagrunnlag, dokumentasjon og eventuelt ressursbehov.
- Drøfte framstillingsform (eksempelvis disposisjon og språklig form).
- Drøfte resultater og tolkninger.
- Holde seg orientert om progresjonen i studentens arbeid i henhold til avtalt tids- og arbeidsplan, og følge opp studenten ved behov.
- Sammen med studenten holde oversikt over antall brukte veiledningstimer.

Instituttet har ansvar for å

- Sørge for at avtalen blir inngått.
- Finne og oppnevne veileder(e).
- Inngå avtale med annet institutt/ fakultet/institusjon dersom det er oppnevnt ekstern medveileder.
- I samarbeid med veileder holde oversikt over studentens framdrift, antall brukte veiledningstimer, og følge opp dersom studenten er forsinket i henhold til avtalen.
- Oppnevne ny veileder og sørge for inngåelse av ny avtale dersom:
  - Veileder blir fraværende på grunn av eksempelvis forskningstermin, sykdom, eller reiser.
  - Student eller veileder ber om å få avslutte avtalen fordi en av partene ikke følger den.
  - Andre forhold gjør at partene finner det hensiktsmessig med ny veileder.
- Gi studenten beskjed når veiledningsforholdet opphører.
- Informere veileder(e) om ansvaret for å ivareta forskningsetiske forhold, personvernhensyn og veiledningsetiske forhold.
- Ønsker student, eller veileder, å bli løst fra avtalen må det søkes til instituttet. Instituttet må i et slikt tilfelle oppnevne ny veileder.

Avtaleskjemaet skal godkjennes når retningslinjene er gjennomgått.

Godkjent av

Ulrik Andreas Sagelvmo
Student

14.01.2023
Digitalt godkjent

Ivar Kjærem
Veileder

01.02.2023
Digitalt godkjent

Hilde Bakke
Institutt

03.03.2023
Digitalt godkjent

Master`s Agreement / Main Thesis Agreement

Faculty	**Faculty of Information Technology and Electrical Engineering**
Institute	**Department of Information Security and Communication Technology**
Programme Code	**MISEB**
Course Code	**IMT4905**

Personal Information

Surname, First Name	**Sagelvmo, Ulrik Andreas**
Date of Birth	**01.04.1993**
Email	**ulrikasa@stud.ntnu.no**

Supervision and Co-authors

Supervisor	**Ivar Kjærem**
Co-supervisors (if applicable)	
Co-authors (if applicable)	

The Master`s thesis

Starting Date	**02.01.2023**
Submission Deadline	**01.06.2023**
Thesis Working Title	**The benefit of value assessments in strategic security decision-making**
Problem Description	**Threats in the digital domain poses as a potential existential threat many business. How are business meant to maneuver in this space, building resilience while enabling the business to take risk to achieve competitive advantage, delivering services with high degree of satisfaction and safety? The hypothesis is that to take long-term strategic decisions the organization has to understand its values. This is especially true for the operative level when they communicate with the strategic level. When communicating the need for digital security the operative level has a tendency to focus on threats and vulnerabilities. Though the strategic level have little insight into digital threats and vulnerabilities. They have however, understanding for the business and assets. For that reason, the operative level should communicate how threats and vulnerabilities affects organizational assets. The thesis therefore wants to study the**

	benefits of value assessments in strategic security decision-making and management of operations.

Risk Assessment and Data Management

Will you conduct a Risk Assessment? **If "Yes", Is the Risk Assessment Conducted?**	**Yes** **No**
Will you Apply for Data Management? **(REK*, NSD**)**	**Yes**
Will You Write a Confidentiality Agreement? **If "Yes", Is the Confidentiality Agreement Conducted?**	**No** **No**

* REK -- https://rekportalen.no/

** Norwegian Centre for Research Data (https://nsd.no/nsd/english/index.html)

Topics to be included in the Master`s Degree (if applicable)

Security, Communication system security, digital security, risk management, security management, business communication system operations and management, value assessment, threat assessment, vulnerability assessment

Guidelines – Rights and Obligations

Purpose

The Master's Agreement/ Main Thesis Agreement is an agreement between the student, supervisor, and department. The agreement regulates supervision conditions, scope, nature, and responsibilities concerning the thesis.

The study programme and the thesis are regulated by the Universities and University Colleges Act, NTNU's study regulations, and the current curriculum for the study programme.

Supervision

The student is responsible for

- Arranging the supervision within the framework provided by the agreement.
- Preparing a plan of progress in cooperation with the supervisor, including a supervision schedule.
- Keeping track of the counselling hours.
- Providing the supervisor with the necessary written material in a timely manner before the supervision.
- Keeping the institute and supervisor informed of any delays.
- Adding fellow student(s) to the agreement, if the thesis has more than one author.

The supervisor is responsible for

- Clarifying expectations and how the supervision should take place.
- Ensuring that any necessary approvals are acquired (REC, ethics, privacy).
- Advising on the demarcation of the topic and the thesis statement to ensure that the work is feasible within agreed upon time frame.
- Discussing and evaluating hypotheses and methods.
- Advising on literature, source material, data, documentation, and resource requirements.
- Discussing the layout of the thesis with the student (disposition, linguistic form, etcetera).
- Discussing the results and the interpretation of them.
- Staying informed about the work progress and assist the student if necessary.
- Together with the student, keeping track of supervision hours spent.

The institute is responsible for

- Ensuring that the agreement is entered into.
- Find and appoint supervisor(s).
- Enter into an agreement with another department / faculty / institution if there is an external co-supervisor.
- In cooperation with the supervisor, keep an overview of the student's progress, the number of supervision hours. spent, and assist if the student is delayed by appointment.
- Appoint a new supervisor and arrange for a new agreement if:
  - The supervisor will be absent due to research term, illness, travel, etcetera.
  - The student or supervisor requests to terminate the agreement due to lack of adherence from either party.
  - Other circumstances where it is appropriate with a new supervisor.
- Notify the student when the agreement terminates.
- Inform supervisors about the responsibility for safeguarding ethical issues, privacy and guidance ethics
- Should the cooperation between student and supervisor become problematic, either party may apply to the department to be freed from the agreement. In such occurrence, the department must appoint a new supervisor

This Master`s agreement must be signed when the guidelines have been reviewed.

Signatures

Ulrik Andreas Sagelvmo
Student

14.01.2023
Digitally approved

Ivar Kjærem
Supervisor

01.02.2023
Digitally approved

Hilde Bakke
Department

03.03.2023
Digitally approved

Appendix B

Original Thesis Topic

The topic for this master's thesis was chosen as part of the Norwegian University of Science and Technology (NTNU) course 'IMT4205 - Research Project Planning About Timetable Examination' [115]. The subject is designed to serve as a preliminary project for the master's thesis. It involves identifying the topic, finding a supervisor, outlining the problem, providing background information, and presenting relevant theory. This way, when one starts working on the master's thesis, some initial input is begun.

The following document showcases the proposed topic for a master's thesis by Geir Olav Dyrkolbotn, following my (Ulrik Sagelvmo) discussion with Geir Olav Dyrkolbotn about writing a thesis centred around bullet point c) on Cyber Situational Awareness (CSA).

As a result, Geir Olav Dyrkolbotn referred me to Ivar Kjærem, who became the supervisor for both the course IMT4205 and this master's thesis. The focus of the thesis revolves around an idea related to CSA. This master's thesis is the culmination of the work conducted within the scope of IMT4205 subject [29, 115].

NTNU

Norwegian University of Science and Technology

Master Thesis Topics 2022 Autumn

IMT 4205

2022-9-15

45. A Study of Cyber Tactics and Intelligence

Contact details:

Geir Olav Dyrkolbotn, geir.dyrkolbotn@ntnu.no

Background:

Oppgaven bygger på faget IMT 4213 Cyber Tactics og IMT 4214 Cyber Intelligence.

Det er en fordel å ha gjennomført disse fagene. Dette er en oppgave som i utgangspunktet ikke er teknisk av natur, men bygger på god forståelse av og erfaring fra arbeidslivet. Oppgaven er derfor best egnet for studenter på erfaringsbasert master (MISEB) **Tasks:**

Oppgaven bør justeres og formes sammen med veileder teamet, men kan inkludere fokus på følgende områder:

A) Viktig cyberlende: Utforske selve fenomenet. Betydningen av viktig cyberlende i relasjon til egen forretningsdrift. Hvordan identifisere viktig cyberlende?

B) Forming av cyberlende: Utforske selve fenomenet og undersøke den praktiske formbarheten til cyberlendet. Hvordan kan forming av cyberlende understøtte forretningsdriften i ulike trusselsituasjonen?

C) Cyber situasjonsforståelse: Utforske selve fenomenet og undersøke hva en virksomhet bør vite om situasjonen i cyberdomenet for å ha god situasjonsforståelse. Hva er god situasjonsforståelse i cyberdomenet?

D) Taktikk for å forstyrre en motstanders rekognosering: Utforske selve fenomenet og undersøke hvordan cyber-rekognosering kan forstyrres. Hva kan en høyt digitalisert virksomhet gjøre for å forstyrre en avansert motstanders rekognosering og angrepsforberedelser?

E) Taktikker for å avsøke cyberlende (screening): Utforske selve fenomenet og undersøke hvilke type indikasjoner man kan lete etter når man avsøker cyberinfrastruktur på jakt etter fiendtlig aktivitet. Hvordan gjennomføre avsøking av cyberlende for effektivt å avsløre fiendtlig tilstedeværelse?

Reference:

Denne oppgaven er i samarbeid med Cyberforsvaret (CYFOR), som vil veilede oppgaven.

CYFOR ser etter flere kandidater til problemstillingene og vil velge ut studenter basert på relevans i fokus og antall interesserte. Kandidater må levere en kort, egen tolkning av en eller flere av problemstillingene, inkludert egen motivasjon for å jobbe med oppgaven. Dette vil inngå i vurderingen av kandidatene.

Appendix C

Trouble-free Logistics

The following paper is the information seed on Trouble-free Logiositcs. The document combines the A_A seed with the A_{TV}. The document text used in the A_A document is marked blue (light grey in black and white), and the text in A_{TV} is marked red (dark grey in black and white). If not marked, the text is used the same in both documents.

Information about the strategic decision-making game and the fictitious company Trouble-free Logistics

Table of contents

About the game

In this game, you assume the role of the Chief Operating Officer (COO) for the fictitious business named Trouble-free Logistics. The game's events and scenarios are fictitious but based on known digital security challenges and incidents from the past 10 years. The purpose is to simulate real situations that strategic decision-makers may encounter, a practice used exclusively as a pedagogical instrument.

How to play

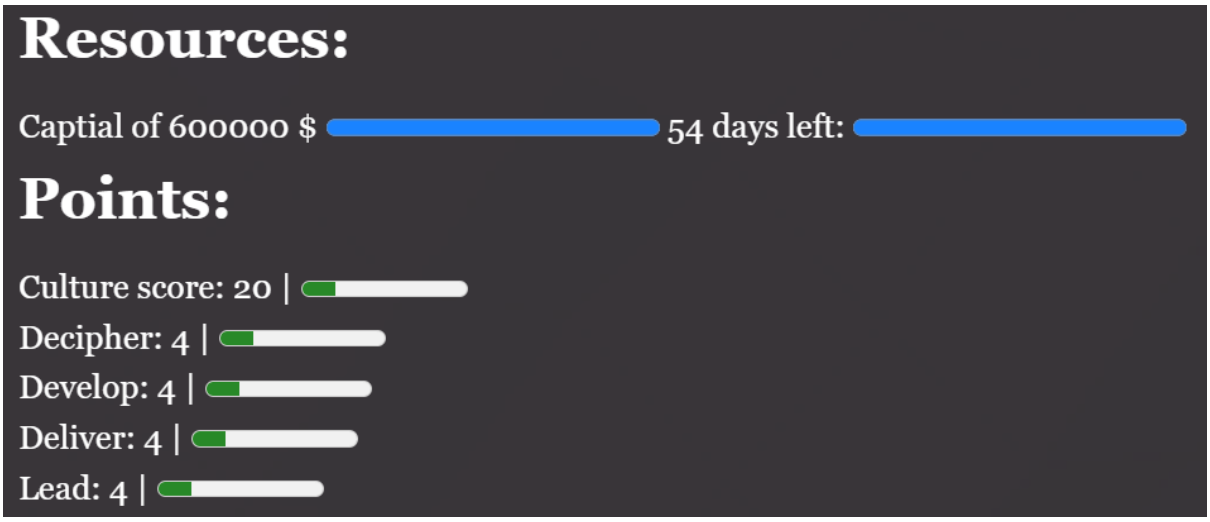
The game consists of nine scenarios, each with four possible actions that you must choose between to achieve the highest security culture score at the end of the game. You will have to answer all nine questions based on the scenarios while managing your limited resources carefully (capital and working days).

Note that sometimes all options may be desirable, while at other times none of them may be optimal. You must base your decisions on what you think will yield the best security culture for Trouble-free Logistics after completing all nine scenarios. It is likely that you will experience uncertainty about upcoming scenarios and resource availability, which you must take into account when making choices.

Game mechanics and resource

In the game, you are given a limited amount of resources, which include a starting capital of $600,000 and 54 days that you must manage throughout the game. Your performance is measured by several metrics, including your culture score, as well as your ability to decipher, develop, deliver, and lead.

Please note that some questions may result in negative points for your culture score, decipher, develop, deliver, and lead measures. Additionally, it is possible to exceed the budget for both capital and days, but doing so will result in a deduction of culture points.



Resources:

Captial of 600000 $ 54 days left:

Points:

Culture score: 20 |

Decipher: 4 |

Develop: 4 |

Deliver: 4 |

Lead: 4 |

Explanation of the metrics:

- **Culture score:** A measure of the overall security culture within Trouble-free Logistics, reflecting the organization's maturity and resilience related to cybersecurity.
- **Decipher:** A measure of how effectively you identify the problem and get to the root of the issue to find a solution. This metric evaluates your ability to think critically and analytically in the face of challenges related to cybersecurity.
- **Develop:** A measure of how well you are able to introduce new functionality to Trouble-free Logistics that improves the organization's security posture. This metric assesses your creativity and innovation in developing new solutions to address cybersecurity challenges.
- **Deliver:** A measure of how well you follow through and maintain the new functionality introduced to Trouble-free Logistics. This metric evaluates your ability to ensure that security improvements are sustained over time and that the organization's security posture continues to improve.
- **Lead:** A measure of how well you are developing the employees within Trouble-free Logistics and inspiring others to embrace and prioritize cybersecurity. This metric evaluates your leadership skills and ability to engage and motivate others to support the organization's security goals.

Note: The game mechanics and point distribution is influenced by the double diamond model and the SANS institute, one of the world's largest cybersecurity research and training organizations and their game Cyber42.

Evaluation criterias

Your evaluation in the game will be based solely on the final culture score, which is influenced by the resources, and points you have accumulated throughout the game. At the end of the game, your culture score will be adjusted according to the following criteria:

- Loose 1 culture point:
    - For each 10000$ spent over budget
    - For each 1 day spent over budget
- Gain 1 culture point:
    - For each 50,000$ saved
    - For each 4th day saved
- Gain 1 culture point for each 1 point you are over 8 for:
    - Decipher
    - Develop
    - Deliver
    - Lead

Trouble-free Logistics

Trouble-free Logistics is a top-tier logistics company that specializes in providing seamless and efficient transportation solutions for businesses of all sizes. They are known for their unparalleled customer service and their ability to handle even the most complex and time-sensitive deliveries with ease. The company was founded by a group of logistics experts with decades of experience in the industry. They recognized the need for a more reliable and customer-focused logistics service, and thus, Trouble-free Logistics was born.

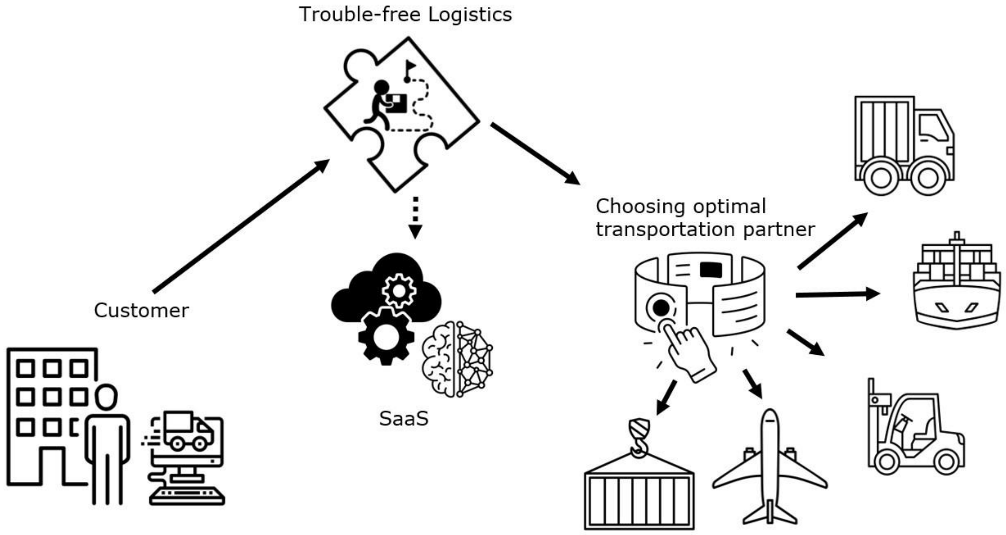
Their state-of-the-art logistics management system allows them to track and monitor shipments in real-time, ensuring that each and every delivery arrives on time and in perfect condition. They have a vast network of transportation partners, including ground, air and sea freight, which allows them to offer a wide range of shipping options to suit the unique needs of each client.

Trouble-free Logistics also prides itself on its commitment to sustainability and environmental responsibility. They work closely with their partners to reduce their carbon footprint and promote sustainable transportation practices.

With their reputation for reliability, efficiency, and outstanding customer service, Trouble-free Logistics is the go-to choice for businesses looking to streamline their logistics operations and ensure smooth and trouble-free deliveries.

Business model

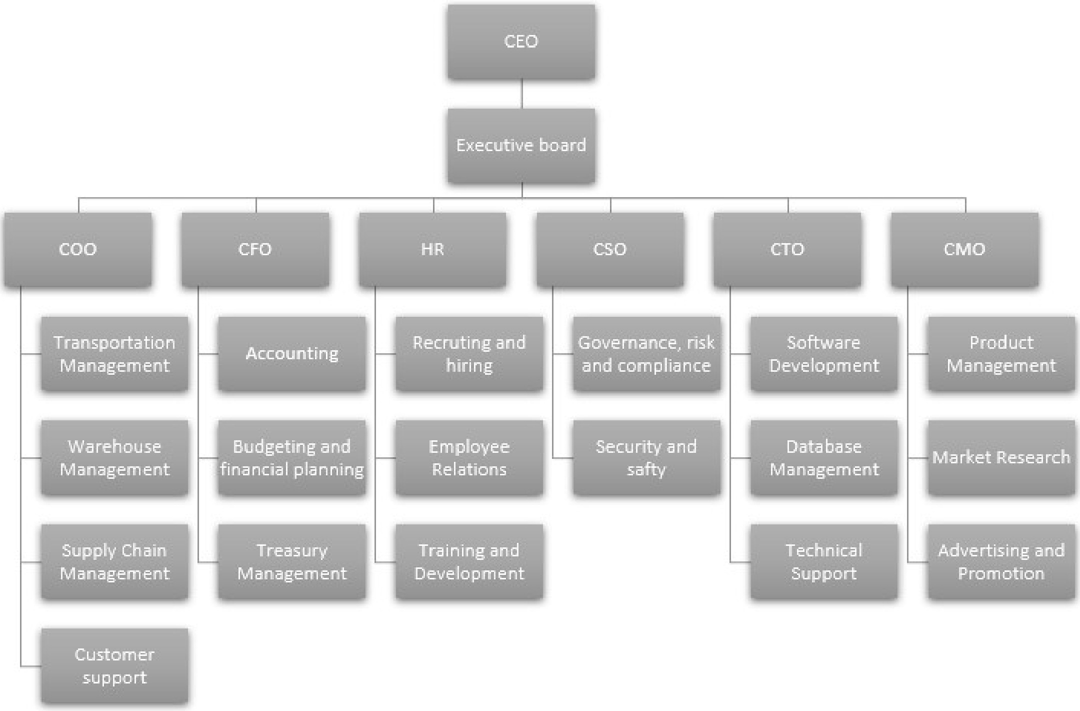
Trouble-free Logistics provides a service that allows businesses and individuals to easily order transportation of small and large deliveries. The service is available as software as a service (SaaS), and customers can access it through their web browser. Once an order is placed, Trouble-free Logistics contacts their network of transportation partners to get the shipment delivered. Trouble-free Logistics acts as an intermediary, except for warehouse services. Their self-developed AI (Artificial Intelligence) is the secret behind their success, as it automatically optimizes transportation, finding the most cost-effective methods and companies for their customers. This benefits customers by removing the burden of having to select the right transportation method. For the transportation partners, they receive a steady stream of customers from Trouble-free Logistics, which often can be added to their existing routes. Recently Trouble-free also relocated all their IT-infrastructure to a cloud provider. They are therefore only maintaining the SaaS platform.



The business model for Trouble-free Logistics

Organization

The organization of Trouble-free Logistics has naturally developed through the years. Today the company has 127 employees, divided in six divisions, each led by an executive manager. An illustration of the organization is shown below with the divisions and departments. The executive board consists of the Chief Executive Officer (CEO), Chief Operating Officer (COO), Chief Financial Officer (CFO), Chief Human Resources Officer (CHRO), Chief Security Officer (CSO), Chief Technology Officer (CTO), and Chief Marketing Officer (CMO).



Trouble-free Logistics organizational structure

The executive board is led by the CEO and includes all the division's managers. They answer to the Board of Directors, responsible for making strategic decisions for the company and ensuring that it is operating in the best interests of its shareholders. Making the executive board responsible for implementing the strategic decisions made by the board of directors and managing the day-to-day operations of the company.

Operations Division (led by the COO)

The COO has four departments under his supervision.

- Transportation Management: This department is responsible for managing the company's transportation operations, primarily overseeing deliveries that may have been delayed or unsuccessful for some reason.

- Warehouse Management: This department is responsible for managing the company's warehouses, including inventory control, receiving and shipping of goods, and storage management.
- Supply Chain Management: This department is responsible for managing the company's supply chain, with a focus on ensuring the availability of partner transportation. They also engage in demand forecasting to ensure that they meet customer demand.
- Customer Support: This department is responsible for providing support to customers who use Trouble-free Logistics' services. They handle inquiries, complaints, and other issues related to the service, and work to ensure customer satisfaction. In addition, they gather feedback from customers to improve the service and identify areas for improvement. Important distinction is that “Technical support” , the department under the CTO, is only for internal use. However, they are responsible for the uptime of the SaaS service. External inquiries regarding the SaaS service are first handled by the “Customer Support” department, however often pushed to the “Technical support”.

Other Divisions

- Finance (led by the CFO): This division is responsible for managing the company's finances, including budgeting, accounting, and financial reporting.
- Human Resources (led by the CHRO): This division is responsible for recruiting and training new employees, managing employee benefits and compensation, and handling any other personnel issues.
- Security and safety (led by the CSO): This division is responsible for ensuring the overall security and safety of Trouble-free Logistics' operations. This includes overseeing the company's security policies, protocols, and procedures to protect against physical and digital threats. Additionally, the division manages the safety of employees and customers, ensuring compliance with relevant regulations and standards. The CSO works closely with other departments to implement security and safety measures throughout the company's operations.
- Technology (led by the CTO): This division is responsible for the operation and maintenance of Trouble-free Logistics IT-infrastructure. They also develop the AI and update the SaaS application based on user feedback received from customer support. The CTO is overseeing the company's technological strategies and ensuring the development and implementation of effective technology solutions. Leading the technology team and working to align technology goals with business objectives, while staying up to date with emerging technologies.
- Marketing (led by the CMO): This division is responsible for overseeing the company's marketing strategies and ensuring that the company's products and services are effectively promoted and positioned in the market. Identifying target audiences, developing campaigns, and measuring the effectiveness of marketing efforts.

Trouble-free Logistics security maturity assessment

A maturity assessment of Trouble-free Logistics has been carried out by a company named *GuardUp Security*. Together with *GardUp Security*, Trouble-free Logistics has reviewed their business impact analysis, risk assessment, security measures and performed both a web application review and a penetration test. Snippets of the result is provided below divided into sub-chapters, and with a concussion at the end:

Business impact analysis

The crown jewel for Trouble-free Logistics is self-developed AI technology that optimizes transportation and provides cost-effective solutions for customers. This is what sets Trouble-free Logistics apart from its competitors.

However, it is important to note that this is useless if not Trouble-free Logistics has a strong network of transportation partners, ensuring reliable and timely deliveries. Simultaneously as they provide exceptional customer service, providing easy, timely and effective support to customers.

Losing the intellectual property invested in the SaaS and AI development would have a significant impact on Trouble-free Logistics. Competitors could quickly enter the market, making it more competitive and marginal for the company. Therefore, protecting this intellectual property is critical to the success of Trouble-free Logistics. Although Trouble-free Logistics may face new competitors, its established history and relationships may give it an edge in the market. Nonetheless, the company must prioritize maintaining customer satisfaction and keeping its partners happy to remain competitive. Criminal organizations have shown interest in stealing both intellectual property and customer data to sell on the darkweb for huge profits.

The company heavily relies on the uptime of their services, and access to the AI is essential for optimizing transportation orders. Without it, orders would need to be manually followed up, leading to less optimization. Additionally, Trouble-free Logistics has contractual requirements for uptime in their Service Level Agreements (SLAs) with customers, which further underscores the importance of maintaining high levels of uptime.

Risk assessment

The assets of Trouble-free Logistics is closely tied to its ability to maintain customer satisfaction, secure partner availability, and optimize its marketing strategies through its online presence. Any disruption to the platform or a breach of customer data could have significant impacts on the company's assets, reputation, and customer trust. To be able to adapt to the risk landscape it is important to conduct regular risks assessments and ensure that appropriate security measures are in place to protect the platform and customer data. It is also recommended to consider implementing a robust incident response plan to quickly and effectively respond to any potential breaches or disruptions to the service. By effectively managing risks and ensuring the integrity and availability of the platform and data, the assets of Trouble-free Logistics can be protected and enhanced over time.

Criminal organizations, hackers, and malicious insiders pose significant risks to Trouble-free Logistics IT systems and sensitive data. If a cyber attack were to occur, such as a ransomware attack, data theft, or DDoS attack, it could potentially impact the ability to provide services to customers and cause significant financial losses. The assessment points out that Trouble-free Logistics IT systems have several critical vulnerabilities. These vulnerabilities include unpatched software, weak authentication mechanisms, and lack of encryption when storing data.
Attackers could exploit these vulnerabilities to gain access to sensitive data or disrupt the services. It will be important to conduct regular threat and vulnerability assessments to identify potential risks and ensure that appropriate security measures are in place to protect the IT systems and sensitive data. It is also recommended to consider implementing a robust incident response plan to quickly and effectively respond to any potential breaches or disruptions to the service. By effectively managing risks and ensuring the integrity and availability of the IT systems and data, Trouble-free Logistics can mitigate potential losses and maintain customer trust.

Asset assessment

Trouble-free Logistics is a company that offers a transportation service utilizing software as a service (SaaS) and self-developed AI for optimization. The assets of Trouble-free Logistics is primarily in its SaaS platform, which enables customers to easily order transportation services and provides them with optimized routes and cost-effective options. Additionally, the self-developed AI enhances the service and improves its efficiency. The SaaS, the development platform for the AI with the self-developed code and the customer database is separated logically with unique authentication. Meaning that you need specific accounts to access each environment.

The company has a significant customer base, including both businesses and individuals, and relies heavily on the uptime of its services. The assets of Trouble-free Logistics is closely tied to its ability to maintain customer satisfaction, secure partner transportation availability, and optimize transportation through its AI technology. Any disruption to the service or a breach of the SaaS platform could have significant impacts on the company's assets, reputation, and customer trust.

It is important to conduct regular threat assessments and vulnerability assessments to identify potential risks and ensure that appropriate security measures are in place to protect the SaaS platform and customer data. It is also recommended to consider implementing a robust incident response plan to quickly and effectively respond to any potential breaches or disruptions to the service. By effectively managing risks and ensuring the integrity and availability of the SaaS platform and data, the assets of Trouble-free Logistics can be protected and enhanced over time.

Threat assessment

The biggest threats to Trouble-free Logistics are assessed to be supply-chain disruptions, criminal organizations and insider risk. *According to GuardUp Security, criminal organizations pose the biggest threat to Trouble-free Logistics. These organizations are primarily motivated by profit and seek to achieve it with minimal effort. GuardUp Security suspects that customer information is a prime target for these criminal groups, and that they may attempt to exploit vulnerabilities in the company's systems to gain unauthorized access to sensitive data.*

- If a supply chain disruption were to occur, such as due to strikes, natural disasters, or supplier bankruptcy, it could potentially impact Trouble-free Logistics' ability to deliver goods on time. This could result in customer dissatisfaction, potentially leading to a loss of business.
- Criminal organizations may utilize cyber attacks such as ransomware, DDoS, data theft, and phishing attacks. This could lead to Trouble-free Logistics attacks losing sensitive data, intellectual property, and customer trust.
- There could be malicious insiders, including employees in Trouble-free Logistics organization or contractors, and partners that intentionally or unintentionally cause harm to the company's assets and reputation. Strong access controls, monitoring, and background checks can help mitigate the risk of insider threats.

Vulnerability assessment

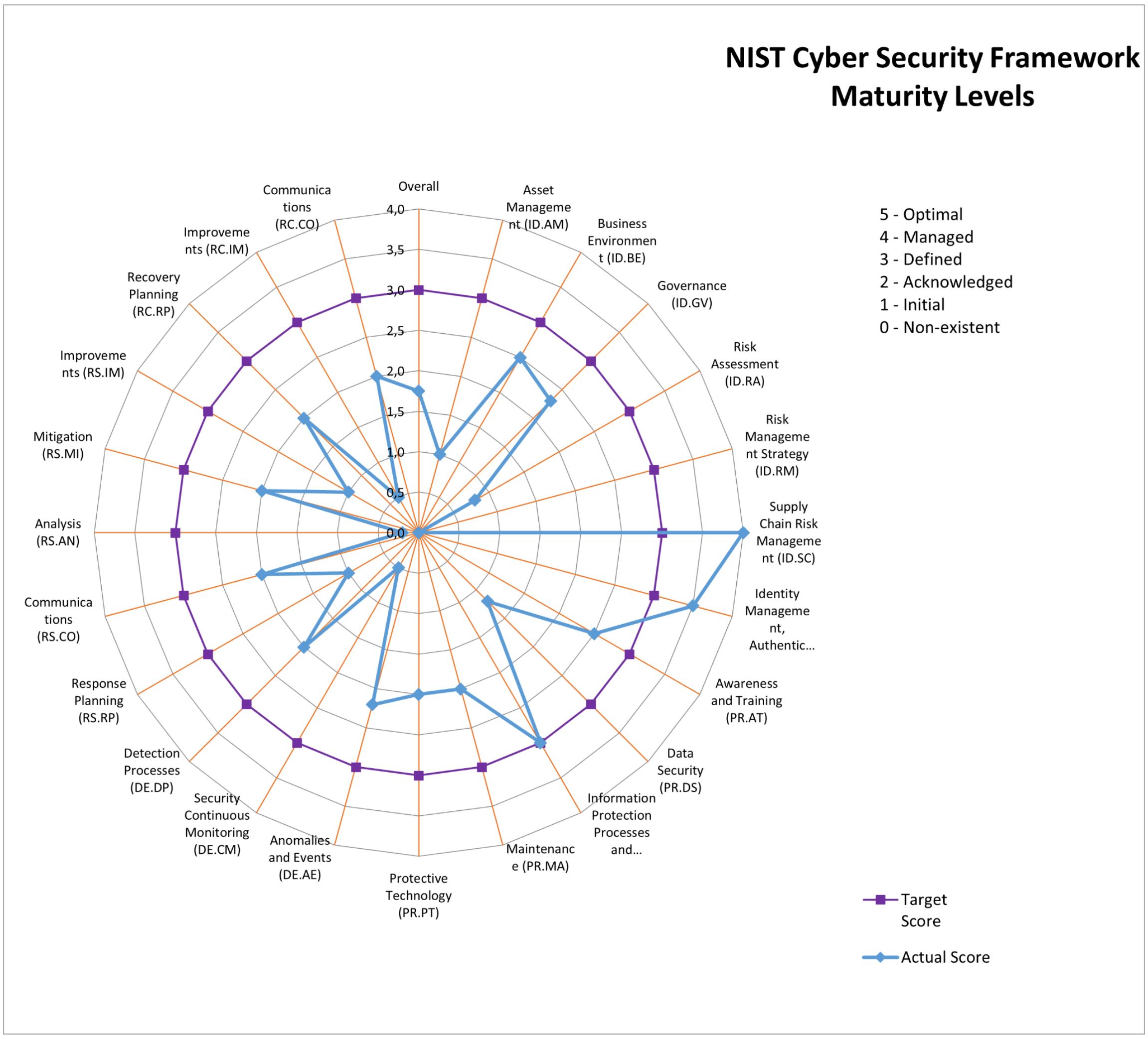
GuardUp Security have focused on SaaS applications, the customer database and the development environment when performing the vulnerability assessment. Trouble-free Logistics has not adjusted their security to adapt to the recent cloud transformation. The infrastructure showing signs of a lift and shift approach to cloud migration.

The assessment points out that Trouble-free Logistics only has one data center with a hot-backup that only can go back four days. The development environment has several critical vulnerabilities. These vulnerabilities include unpatched software, weak authentication mechanisms, and lack of encryption when storing data. Attackers could exploit these vulnerabilities to gain access to sensitive data or disrupt the service. On the SaaS interface they are able to log into customers accounts due to weak passwords, lack of multi-factor authentication, and poor access controls. These vulnerabilities could be exploited by attackers to gain unauthorized access to the system and sensitive data.

Security measures

Trouble-free Logistics had a target score of 3 when accessing their maturity against the NIST Cyber Security Framework Maturity levels. *GuardUp Security* gave Trouble-free Logistics an overall score of 1,75. Pointing to the lack of good routines when it comes to identification of assets, poor risk management and optimization, weak data security and detection and monitoring capabilities. They also suggest Trouble-free Logistics to improve response and recovery measures.

GuardUp Security suggests focusing on measures that address the risk that most heavily affect the assets of Trouble-free Logistics. Recommending Trouble-free Logistics to focus on the SaaS application, integrity of the customer database and the business continuity. threats and vulnerabilities. Recommending to fix vulnerabilities that threats are most likely to exploit, such as weak passwords and unpatched software. They provide the following spider graph to show the result.



Spider graph of the security maturity assessment

Web application review and penetration test

GardUp Security find the following weaknesses and vulnerabilities:

Insecure Authentication and Session Management: The SaaS application uses weak or insecure authentication and session management mechanisms, which can allow attackers to easily bypass authentication and gain unauthorized access to the application or user data.

Outdated Libraries, components, and software: The application uses outdated libraries and components, which can contain known vulnerabilities that can be exploited by attackers.

Lack of Input Validation: The application does not properly validate user input, which can allow attackers to inject malicious code or execute arbitrary commands on the server. This vulnerability was discovered in the file upload feature of the application.

SQL Injection Vulnerability: The application is vulnerable to SQL injection attacks, which can allow attackers to extract sensitive information from the database or even take over the application. This vulnerability was discovered in the login form and the search function of the application.

Conclusion

GuardUp Security assessed Trouble-free Logistics and found that their security maturity level is low. This is primarily due to a mismatch between the identified risks and the security measures in place to mitigate those risks. They advise Trouble-free Logistics to continue on improving their security based on the risk towards the assets and what makes their assets valuable. They advise Trouble-free Logistics to focus on closing known vulnerabilities that have the biggest risk seen from the threat assessment perspective.

Appendix D

Nettskjema form

The following form is the one build in nettskjema to collect consent and ensure informed voluntary participation. The form uses a template provided by *Sikt* named "*Template for information letter and gathering consent (word-format)*" [116].

D.1 Form used in the master-thesis

*Mandatory fields are marked with a star**

Participation in the strategic decision making game

Purpose of the project

You are invited to participate in a research project for a master-thesis, where the main purpose is to investigate what information is of most value for strategic decision-makers in cybersecurity related questions. Trying to answer if it is more valuable to focus on values or threats and vulnerabilities when strategic decisions are made.

Which institution is responsible for the research project?

Norwegian University of Science and Technology: Faculty of Information Technology and Electrical Engineering is responsible for the project (data controller).

Why are you being asked to participate?

The research project has developed a strategic decision-making game and need participants to play the game. For that reason, you are being asked if you want to participate in my research project by playing the game. Which I hope will be a fun and maybe even educational.

What does participation involve for you?

Alongside this document you have or will receive a html file (.html) or an URL to access the game, and a PDF detailing how to play the game and information about the fictitious company Trouble-free Logistics (You will be able to collect all these documents through the game as well). If you chose to participate in the game, it is estimated to take approx. 20 minutes. Your answers will be recorded anonymously after ending the game, and it will not be possible to link the answers back to you.

Participation is voluntary

Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. There will be no negative consequences for you if you chose not to participate or later decide to withdraw. However, it is not possible to delete your submission after the game as it is impossible to link it back to you.

Your personal privacy – how we will store and use your personal data

We will not use or record your personal data and every answare is recorded anonymous.

Recorded data will not be processed or shared outside the database. Your recorded data will not be recognizable in any publications.

What will happen to the recorded data at the end of the research project?

The planned delivery date of the project is 01.06.2023. The database will be deleted as soon as the Norwegian University of Science and Technology confirms that they do not need access to the data for evaluation, but no later than the 31.08.2023.

Your rights

So long as you can be identified in the collected data, you have the right to:

- access the personal data that is being processed about you
- request that your personal data is deleted
- request that incorrect personal data about you is corrected/rectified
- receive a copy of your personal data (data portability), and
- send a complaint to the Norwegian Data Protection Authority regarding the processing of your personal data

Where can I find out more?

If you have questions about the project, or want to exercise your rights, contact:

- **Project leader:** Ulrik Sagelvmo
  - Mail: ulrikasa@stud.ntnu.no
  - Phone: +47 93 22 41 19
- **Supervisor from NTNU:** Ivar Kjærem
  - Mail: ivar.kjarem@ntnu.no
- Our Data Protection Officer (NTNU): Thomas Helgesen

Yours sincerely,
Ulrik Sagelvmo
Project Lead

*I agree to the terms and conditions**

- Yes
- No

> If the candidate chose "*Yes*", they would be prompted to enter a five-digit number. If not they would be sent directly to the receipt page.

Please provide a five-digit number that you would like to use as your login for the game.

Once you have entered the five-digit number, please click on "Send." You can then proceed with the game by clicking on "Enter your code".

> The receipt page is then shown after entering the five-digit number or if the candidate had chose "*No*" when asked "*I agree to the terms and conditions**".

Receipt page

Thank you!

You will always be able to go back into the form if you want to refresh the terms and conditions, get a new code for the game or if you have a change of mind.

If you have any questions or feedback you can write me an email at: ulrikasa@stud.ntnu.no

D.2 Settings in the form

Table D.1: The form

The form's opening time	Open
Who may answer the form	Everyone with link
Form URL	https://nettskjema.no/a/327476
Responsible for the form	ulrikasa@stud.ntnu.no
Collection of personal data	No

Table D.2: Layout

Form type	Questionnaire
Form language	English
Hide progress indicator	Yes
Editing of the form after receiving submissions	Yes
Codebook activated	Yes
Form ID for forwarding	Not assigned

Table D.3: Response restriction

Maximum number of submissions	Not assigned
Maximum number of submissions per respondent	Not assigned
Message to respondent when maximum number of submissions has been reached	Not assigned

Table D.4: Permissions

Editing permissions	ulrikasa@ntnu.no
Copying rights	Blank

Table D.5: Processing of submissions

Automatic removal of answers	No
Possible for respondent to store submission	No
Possible for respondent to change or delete submission	No

Table D.6: Receipt

Send receipt to respondent	No
Message on the receipt page after submission	See section D.1

Table D.7: Notifications

Get a notification by e-mail when receiving a submission	No

Table D.8: Storage

Storing answers	Storing submissions in Nettskjema

Appendix E

Game code

The game file and code can be retrieved from GitHub in the repository with the name. Trouble-free Logistics at this URL: `https://github.com/usagelvmo/Trouble-free-logstics.git` [117]. Unfortunately, the code for the game is unfit to be printed as an appendix due to the size of the document.

The repository also contains the code used for the 'Google Apps Script' to collect and push responses into 'Google Sheets'. However, This code can be printed and read in appendix F.

Appendix F

Google setup

The code listing F.1 prints the code used in ’Google Apps Script’ for pushing responses into ’Google Sheets’ for analysis of the data. This code is based on the work of Dan Cox [94].

Code listing F.1: Web-App code [94]

```
//  1. Enter sheet name where data is to be written below
        var SHEET_NAME = "GameData";

//  2. Run &gt; setup
//
//  3. Publish &gt; Deploy as web app
//    - enter Project Version name and click ’Save New Version’
//    - set security level and enable service (most likely execute as ’me’
and access ’anyone,␣even␣anonymously)
//
//␣␣4.␣Copy␣the␣’Current web app URL’␣and␣post␣this␣in␣your␣form/script␣action
//
//␣␣5.␣Insert␣column␣names␣on␣your␣destination␣sheet␣matching␣the␣parameter␣names
of␣the␣data␣you␣are␣passing␣in␣(exactly␣matching␣case)

var␣SCRIPT_PROP␣=␣PropertiesService.getScriptProperties();␣//␣new␣property␣service

//␣If␣you␣don’t want to expose either GET or POST methods you can comment out the
appropriate function
function doGet(e){
  return handleResponse(e);
}

function doPost(e){
  return handleResponse(e);
}

function handleResponse(e) {
  // shortly after my original solution Google announced the LockService[1]
  // this prevents concurrent access overwritting data
  // [1] http://googleappsdeveloper.blogspot.co.uk/2011/10/concurrency-and
  -google-apps-script.html
  // we want a public lock, one that locks for all invocations
  var lock = LockService.getPublicLock();
  lock.waitLock(30000);  // wait 30 seconds before conceding defeat.

  try {
    // next set where we write the data - you could write to multiple/alternate
        destinations
    var doc = SpreadsheetApp.openById(SCRIPT_PROP.getProperty("key"));
    var sheet = doc.getSheetByName(SHEET_NAME);

    // we’ll assume header is in row 1 but you can override with header_row
        in GET/POST data
    //var headRow = e.parameter.header_row || 1; Hawksey’s code parsed
        parameter data
    var postData = e.postData.contents; //my code uses postData instead
    var data = JSON.parse(postData); //parse the postData from JSON
    var headers = sheet.getRange(1, 1, 1, sheet.getLastColumn()).getValues()[0];
    var nextRow = sheet.getLastRow()+1; // get next row
    var row = [];
    // loop through the header columns
    for (i in headers){
      if (headers[i] == "Timestamp"){ // special case if you include a ’Timestamp’
          column
        row.push(new Date());
      } else { // else use header name to get data
        row.push(data[headers[i]]);
      }
    }
    // more efficient to set values as [][] array than individually
    sheet.getRange(nextRow, 1, 1, row.length).setValues([row]);
    // return json success results
    return ContentService
          .createTextOutput(JSON.stringify({"result":"success", "row": nextRow}))
          .setMimeType(ContentService.MimeType.JSON);
  } catch(e){
    // if error return this
    return ContentService
          .createTextOutput(JSON.stringify({"result":"error", "error": e}))
          .setMimeType(ContentService.MimeType.JSON);
  } finally { //release lock
    lock.releaseLock();
  }
}

function setup() {
    var doc = SpreadsheetApp.getActiveSpreadsheet();
    SCRIPT_PROP.setProperty("key", doc.getId());
}
```

Appendix G

Game scenarios and scoring

In this attachment, all the scenarios in the game are listed, including the full text, answer options, and the player's response after selecting an option. A table has also been included, showing how each individual question is evaluated and how it affects the player's values.

Table G.1: Scenario 1: Risk assessment

Scenario

Two years have passed since Trouble-free Logistics conducted a comprehensive review of its risk assessment, which included a value assessment, threat assessment, and vulnerability assessment to identify the organizational risks. During this period, Trouble-free Logistics transitioned from on-premise solutions to relying solely on the cloud. While the CTO believes this shift has not significantly altered the company's risks and may have even improved security, the CSO disagrees. The CSO argues that due to the due diligence process for the cloud provider, which did not include an evaluation of their digital security, the risk assessment and business impact analysis (BIA) should be thoroughly updated.

However, the CSO disagrees with this assessment and believes that the risk assessment and business impact analysis (BIA) should be thoroughly updated. The CSO's belief is due to the due diligence process for the cloud provider, which did not include an evaluation of their digital security.

As the COO you are accountable for the business impact analysis. What should you do?

Alternatives

a) You concur with the CTO's opinion that investing additional time and resources into an extensive reevaluation of the risk assessment, including the business impact analysis, would be a futile exercise. Minor updates to the existing assessments would suffice.

b) You have reached a compromise and opted for a partial revision of the risk assessment. As the company continues to provide the same services as before, there is no immediate need to update the BIA.

c) You concur with the CSO's perspective and decide to conduct a complete revision of the business impact analysis and the risk assessment to gain a deeper understanding of the risk changes.

d) You intend to seek additional information and guidance before arriving at a decision. You plan to consult experts to gain further insights before deciding on revising the risk assessment and business impact analysis.

Respons

The conclusion and key takeaways from various whitepapers on cloud transformation, including "CISO's Guide to Cloud Security Transformation" by Google Cloud, suggest that cloud migration alters a company's ecosystem and risk landscape. Additionally, Paul Gibbons highlights the significance of addressing risk factors during organizational changes, such as migration to the cloud.
Your score reflects how well RESPONSE emphasized the impact of cloud migration on Trouble-free Logistics. However, it is essential to consider the company's current situation and limited resources. While an answer may be considered a best practice, it may not be the most suitable option for Trouble-free Logistics given its context and resource constraints.

Table G.2: Question 1: Risk assessment

Alternative	Culture	Cost	Days	Decipher	Develop	Deliver	Lead
a	-2	$5,000	2	-2	0	1	0
b	1	$15,000	5	0	0	1	1
c	4	$30,000	8	2	1	1	1
d	2	$15,000	6	1	0	0	0

Table G.3: Scenario 2: Global CEO summit

Scenario

The CEO has recently returned from the Global CEO Summit where he gained insights on the latest trends in the field of cybersecurity and how it could provide a competitive edge. He is familiar with the revised Business Impact Analysis (BIA) and Risk Assessment (print:"(See the PDF for more information on BIA and risk)"), but he is eager to learn more about "Threat Intelligence-based Ethical Red Teaming" (TIBER) and how Trouble-Free Logistics can leverage this to attain a competitive advantage. What do you decide to do as the COO?

Alternatives

a) To acquire knowledge and firsthand experience, you develop a pilot program for TIBER. This program will enable Trouble-Free Logistics to identify how TIBER can be utilized.

b) You are aware that the CEO approached you, rather than the CSO, because you could provide an answer on how TIBER could be leveraged to gain a competitive advantage in the market. Nonetheless, you acknowledge that the CSO could offer valuable insights into the technical aspects and the cost-benefit analysis of an implementation of TIBER. Working with the CSO, you convey the message that a TIBER program is not relevant, based on the BIA and risk assessment.

c) This is a golden opportunity to integrate Trouble-Free Logistics' thorough threat assessment into our services. You can use the existing assessments as input values for TIBER, which will not only enhance customer services but also improve future risk assessments and the BIA. You inform the CEO that by acting on these assessments, Trouble-Free Logistics can improve services where it matters the most, as well as improve internal risk assessments and identify cost-saving measures based on the threat intelligence. This will help Trouble-Free Logistics build security in the areas that matter the most.

d) TIBER is just another trend that has caught the CEO's attention, and may not be a viable approach. After careful consideration and evaluation, you explain to the CEO that it is not a reliable or sustainable solution, and therefore not a recommended investment for Trouble-Free Logistics.

Respons

The BIA and risk assessment of Trouble-free Logistics reveal that the company is concerned about security, while having a low level of cyber maturity.
Your score reflects how well OPTION considered the maturity of Trouble-Free Logistics and their risk assessment.

Table G.4: Question 2: Global CEO summit

Alternative	Culture	Cost	Days	Decipher	Develop	Deliver	Lead
a	2	$80,000	9	1	2	1	1
b	2	$10,000	4	2	0	0	2
c	8	$100,000	12	2	2	2	1
d	0	$0	1	1	-1	-1	2

Table G.5: Scenario 3: DDoS

Scenario

You receive a call at 7:30 PM on a Wednesday from a stressed employee in the customer support department. They report receiving numerous calls from irate customers who are unable to access the SaaS website. The employee informs you that they have already contacted the technical support department, who stated that everything appears to be functioning as usual. However, technical support suspects that the website may be under a Distributed denial-of-service (DDoS) attack due to the unprecedented high volume of traffic they have observed. The employee wants to know what they should tell the customers and what the next steps should be. You advise the customer support employee to inform customers that the company is aware of the issue and is currently investigating the cause. Assure them that the technical team is working to resolve the problem as quickly as possible. The following day after the attack you sit down with the CSO and CTO to identify lessons learned and measures against DDoS attacks. What do you as the COO decide to do?

Alternatives

a) The DDoS attack on Trouble-Free Logistics highlighted the need for DDoS prevention mechanisms. One of the reasons for transitioning to the cloud was to leverage the rapid scaling capability. Working with the CSO and CTO, you implement mechanisms for scaling and establish a Content Delivery Network (CDN), which allows for multiple access points.

b) During talks about lessons learned the incident response plan and the contingency plan stands out as clear candidates for revision and improvement. A lot of things went wrong and were not handled as they should according to the policy. You decide with the CTO to improve the incident response plan and the contingency plan, with focus on better collaboration between your customer support department and CTOs technical support department. This way customer support can better respond to irate customers. Additionally, you decide to start exercising the different response plans.

c) This is primarily a concern for the CTO and CSO. You remind them that it is crucial for customers to be able to access the website and that they must ensure its availability. The fact that it was down reflects poorly on the company and can harm customer relations. After highlighting the issue, you leave it to them to find a solution that doesn't impact your budget.

d) You look at the current risk assessment evaluating the document. In dialogue with the CTO and CSO you decide to make a new risk scenario for DDoS attacks to shed light on the risk and identify potential weaknesses with your lessons learned. This will be used to guide the implementation of security measures to prevent or limit the damage of future DDoS attacks.

Respons

According to the UK National Cyber Security Centre (NCSC) it is important to understand your services and environment to develop effective preventative measures against DoS and DDoS attacks. It's also crucial to be able to act quickly in case of an attack, so having a well-planned response and recovery strategy is essential. Your score reflects how well OPTION took into account the prerequisites Trouble-Free Logistics had for effective implementing security measures promptly after the incident.

Table G.6: Question 3: DDoS

Alternative	Culture	Cost	Days	Decipher	Develop	Deliver	Lead
a	1	$80,000	10	0	2	2	1
b	2	$55,000	6	1	2	2	2
c	-2	$0	0	-2	-1	-1	-2
d	4	$20,000	4	2	1	1	1

Table G.7: Scenario 4: Private public services

Scenario

While taking your lunch break, you discover that some employees have stored Trouble-free Logistics data on private public cloud storage platforms like iCloud, Dropbox, OneDrive, or Google Drive. This practice may be more common than you previously believed, and it poses a significant problem if sensitive information is stored outside of the company's platforms and applications. Doing so could potentially compromise the intellectual property of Trouble-free Logistics, which is a serious concern. Additionally, this goes against the acceptable-use policy of the company.

Alternatives

a) Arrange a meeting with the CSO and the employees in question to discuss the significance of information security. This discussion covers the potential risks associated with using public cloud storage solutions, as well as the company's policies regarding the handling of intellectual property. You enforce the sanctions outlined in the policy to ensure that everyone in the company understands that information security, especially as it pertains to intellectual property, is a concern.

b) You begin a project to investigate the root cause of why employees started using private public cloud storage platforms in the first place. Work alongside the CTO to identify potential technical solutions to address the underlying issue, thereby ensuring that employees no longer need to use private public cloud storage platforms. Additionally, you update the company's policies and procedures to reflect the changes made and the lessons learned during the project.

c) Work with the IT department to investigate whether any sensitive information has been compromised as a result of this practice, and take appropriate steps to contain any potential damage.

d) Conduct a company-wide training or awareness campaign to ensure that all employees understand the importance of information security, the risks of using public cloud storage solutions, and the company's policies and procedures for handling sensitive information.

Respons

Your score reflects how well OPTION addressed the employees' use of private public cloud storage platforms and got a change of behavior in the organization.

Table G.8: Question 4: Private public services

Alternative	**Culture**	**Cost**	**Days**	**Decipher**	**Develop**	**Deliver**	**Lead**
a	1	$5000	2	0	0	0	-1
b	4	$95,000	9	2	2	2	2
c	1	$25,000	5	-1	-1	0	0
d	2	$10,000	10	1	1	1	1

Table G.9: Scenario 5: Ransomware

Scenario

It was just another busy day at Trouble-free Logistics, when suddenly, the computer systems started acting strange. The employees noticed that their computers were running slow and several important files were suddenly locked and encrypted. Panic started to spread as it became clear that the company was under a ransomware attack. The IT department tried to quickly contain the spread of the virus, but it was too late. The attackers had successfully infiltrated the company's systems and encrypted all the critical data. A ransom note appeared on the screen, demanding $100,000 in exchange for the decryption key. The ransom will increase by $10,000 every day if no payment is received and if they detect or even suspect the involvement of law enforcement the data will be deleted permanently. Immediately after being informed of the attack, you set up an emergency meeting with the CEO, CSO, CTO and CFO to assess the situation and determine the next steps. What is the following action that you as the COO take?

Alternatives

a) The CTO suggests restoring from backup, but when asked about the timeline for full operational capability, the CTO is unsure and estimates it to take 5 days. The CSO also supports the idea of restoring from backup, but advises against going live until the vulnerability used to install the ransomware has been patched to prevent the threat actor from returning. However, the CSO cannot estimate the time required to uncover and patch the vulnerability. You suggest that the CTO should initiate the restoration process while the CSO begins the forensics work to identify the vulnerability

b) You are aware of how crucial it is for your operations to have 24/7 access to your systems to provide essential services. If these services are down for more than 120 minutes, Trouble-Free Logistics will lose over $80,000 per day and will be unable to serve its customers. Given this, you have concluded that Trouble-Free Logistics has no realistic option other than to pay the ransom, as failing to do so would result in a significant loss of capital.

c) You contact law enforcement and provide them with all the requested information, including log files from various systems and hosts, hoping that it will aid in a thorough investigation of the attack and possibly lead to the apprehension of the attackers. However, the investigation may take some time, and the company may not quickly regain access to their data. Therefore, you suggest that the CTO should begin restoring the backup while the CSO utilizes available resources to support law enforcement.

d) After considering various options, you suggest to the CTO that they only restore a minimal amount of systems to serve the most critical customers. This will allow your team to resume some operations and avoid numerous SLA violations. This approach will also help you support some customers and save costs at the same time. The CTO acknowledges that it is possible, but mentions that most of the time-consuming steps in the restoring process are for the fundamental services on which Trouble-Free Logistics' services are built. As a result, the restoration process will take time. The CSO highlights that the restored services will still be vulnerable to the same attack. However, you emphasize that it is crucial to do this for the customers and ensure that already booked services are processed.

Respons

Thanks to Conti Leaks we have gained insight into how criminal cyber organizations operate. Multiple organizations have also experienced their wrath, and therefore we do have some data on ransomware attacks. Unfortunately, the data indicate that 51% of organizations that pay the ransom demand do not recover their stolen data, of the ones that can restore some data only 19% of organizations are able to fully recover it. If you pay the ransom, some sources say it is a 33% chance to get targeted again by the same group.

Your score reflects how well OPTION ensured that Trouble-Free Logistics would not be exposed to ransomware again by the same group.

Table G.10: Question 5: Ransomware

Alternative	**Culture**	**Cost**	**Days**	**Decipher**	**Develop**	**Deliver**	**Lead**
a	4	$240,000	5	2	1	2	2
b	-6	$100,000	1	-3	-3	-3	-3
c	2	$200,000	8	2	1	2	1
d	2	$160,000	3	1	1	2	2

Table G.11: Scenario 6: Confirmed breach and stolen personal identifiable data

Scenario

Although Trouble-Free Logistics has recovered from the ransomware attack and concluded discussions with affected customers, law enforcement, and supervisory authorities, an internal forensic investigation led by the CSO is still ongoing. During the investigation, one of the forensic analysts discovered that a significant amount of customer data containing personally identifiable information had been exfiltrated three months prior to the ransomware attack by the same threat actor. The CSO has brought this problem to your attention and informed you that it falls under the General Data Protection Regulation (GDPR) as a personal data breach. In response, you quickly look up the latest "Guidelines on Personal Data Breach Notification" from the European Commission.

Alternatives

a) After studying the guidelines, you find that you are still uncertain about whether the notifications made during the prior ransomware attack are sufficient, and what the potential risk to the rights and freedoms of individuals affected by the breach could be. As a result, you decide to reach out to your supervisory authority to request their support and guidance on how to proceed with the incident, based on their guidelines. You conclude to follow their guidance.

b) The data was extracted 3 months ago, and based on this information, neither you nor the CSO see the point of taking any further action. Customers, law enforcement, and supervisory authorities have already been informed about the ransomware incident. Moreover, bringing this to the attention of your customers would only further damage your reputation. Instead, you would rather focus on reviewing and improving the company's data protection policies and procedures, while the CSO wants to patch the systems. So, you both decide to do exactly that.

c) You conclude that the exfiltrated data is unlikely to pose a risk to the rights and freedoms of individuals. Therefore, you instruct the CSO to continue the investigation and identify, if possible, which customer data has been compromised, so that you can notify the affected customers accordingly.

d) You promptly reopen the communication channels with all customers, law enforcement, and supervisory authorities to disclose the new information. However, you are currently unable to provide specifics on which customers are affected and what data. Therefore, you request their cooperation and ask any party with relevant threat intelligence regarding similar incidents to share it with Trouble-Free Logistics.

Respons

The personal data breaches were initially notified to supervisory authorities as an availability breach when Trouble-Free Logistics experienced the ransomware attack. However, it could not be excluded that information was also exposed to unauthorized disclosure or access. Now that it has been confirmed that customer data was breached, it is considered a confidentiality breach as well. On the other hand, since this is related to the same ransomware attack and threat actor, it is considered an update to the existing notification of the attack.

Your score reflects how well OPTION made sure to update supervisory authorities, and how it reflected the values of Trouble-Free Logistics to customers.

Table G.12: Question 6: Confirmed breach and stolen personal identifiable data

Alternative	**Culture**	**Cost**	**Days**	**Decipher**	**Develop**	**Deliver**	**Lead**
a	2	$50,000	6	2	1	2	1
b	-2	$5,000	2	-1	0	0	0
c	1	$30,000	4	1	0	0	1
d	2	$15,000	6	1	2	1	2

Table G.13: Scenario 7: Helping the CSO with metrics

Scenario

The CSO is currently developing a metrics program to ensure that security investments align with Trouble-Free Logistics' business operations and key performance indicators (KPIs). The CTO is also heavily involved, but the CSO is leading the program. As the COO, you are a significant stakeholder in the project. Today, the CSO has scheduled a full day of presentations and workshops with you and your department heads, with the governance, risk, and compliance team and the CSO leading the day.

After listening for two hours about the importance of aligning security metrics with business operations and how crucial your input is for the success of the project. It is time for you and your department heads to share your perspective on business operations and what aspects are essential to you, including what KPIs you consider important. The next session is a workshop where you and your department heads will discuss which security metrics are useful to you and what to report to the CEO. How do you decide to approach this?

Alternatives

a) After listening to the CSO, you have decided that your input may not be as valuable in this context, and you believe your time is better spent on more pressing matters. You trust that your department heads are capable of expressing their views on crucial business operations and identifying the security metrics that are important to them. Therefore, you leave the room after ensuring that the department heads are comfortable continuing without you.

b) You have long felt that the CSO and their team do not have a deep understanding of the business and how Trouble-Free Logistics is run. As a result, you provide them with insights into business management and how operations are run, and assign your department heads to explain their part of the operation. This enables the CSO and their team to gain a better understanding of operations and what metrics would be of value to you. This is then discussed during the workshop session and heavily influences the development of the metrics program.

c) You have evaluated the presentation by the CSO and his department and have come to the conclusion that the metrics program may not be the appropriate way forward for Trouble-Free Logistics, despite having the CEO's approval and being close to entering the development phase from the decipher phase. You feel the need to act quickly and therefore discuss your concerns with the CSO the next day. Following a lengthy discussion involving the CEO and all executive managers, it is decided to abandon the program. As this decision was made early on, before the program entered the development phase, the remaining budget is allocated among the divisions.

d) You have requested the department heads to prepare for this day as you believed that this program could provide significant value to your division and benefit the management of Trouble-Free Logistics. During the presentations, your department heads highlighted what is crucial to them in delivering frictionless services with high customer satisfaction. You then link all the information presented, connecting the operational level to the strategic level, and providing a holistic overview of Trouble-Free Logistics operations, and explain why you operate the way you do. This comprehensive understanding of operations is then discussed during the workshop session, heavily influencing the development of the metrics program.

Respons

Your score reflects how well OPTION laid the foundation for a successful implementation of the metrics program. As a key stakeholder, you are responsible for ensuring that the needs of your division are considered and understood by the CSO, who leads the metrics program. This requires effective communication to convey your division's needs in a manner that is understandable to the program team.

Table G.14: Question 7: Helping the CSO with metrics

Alternative	**Culture**	**Cost**	**Days**	**Decipher**	**Develop**	**Deliver**	**Lead**
a	-2	$5,000	1	-1	-1	-1	-2
b	1	$15,000	4	1	0	0	0
c	-6	+$30,000	+6	2	0	0	2
d	4	$65,000	7	2	2	2	2

Table G.15: Scenario 8: Security awareness training

Scenario

Trouble-free Logistics has identified insider risk, social engineering attacks, and phishing attacks in their risk assessment. The CSO intends to address these risks by providing awareness training to all employees in order to reduce the probability of a successful attack. As the COO, you are responsible for the majority of the workforce at Trouble-free Logistics, and your employees have the most interactions with external individuals. When the CSO asks for your input on how to successfully execute the awareness training, you provide the following recommendations:

Alternatives

a) You suggest starting a rewards program to incentivize good security practices among employees. The program would involve recognizing and rewarding employees who consistently demonstrate good security practices, as well as report potential threats. The aim is to foster a culture of cybersecurity awareness and responsibility within the company.

b) You inform the CSO that you have come across a company that provides cyber exercises, and one exercise is a simulated phishing campaign. The exercise is launched without the knowledge of the employees, but when the campaign is ended the result and performance is shown to the organization. This would be an interactive and engaging exercise that simulates real-life scenarios to help employees recognize and respond appropriately to potential attacks. The exercise can then be run later to see if Trouble-free Logistics has improved their security awareness.

c) You express your skepticism about the effectiveness of security awareness training and suggest that the CSO focus on security measures that address the identified risks for Trouble-free Logistics without placing additional burden on your employees. Although you acknowledge that such measures may increase costs, you propose collaborating with the CSO to develop a more comprehensive solution that effectively addresses both the likelihood and potential impact of these risks while minimizing any additional workload for your employees.

d) You suggest that the CSO should request time from the different departments during their monthly meetings and provide awareness training then. Furthermore, advising the CSO to use recent incidents to highlight the potential breaches and to put it into a relevant context. That way the employees can relate, and the CSO can emphasize the importance of reporting suspicious activity.

Respons

Your score reflects how well "OPTION" addresses all three risks and its impact and likelihood on the organization. It also illustrates how "OPTION" changed the behavior over time and improved the security of Trouble-free Logistics by reducing the risks of insider threats, social engineering attacks, and phishing attacks.

Table G.16: Question 8: Security awareness training

Alternative	**Culture**	**Cost**	**Days**	**Decipher**	**Develop**	**Deliver**	**Lead**
a	1	$10,000	6	1	0	0	1
b	2	$70,000	5	1	1	1	1
c	5	$140,000	2	2	2	1	2
d	1	$20,000	1	0	0	0	0

Table G.17: Scenario 9: Business contingency and continuity

Scenario

You have been concerned about business continuity in Trouble-free Logistics for a long time, even before the ransomware attack. Finally, you have received approval from the CEO to propose a project with the CFO, CTO, and CSO to improve business continuity, and your division will be leading the effort. To ensure that the CEO approves your project, what do you choose to do?

Alternatives

a) Having recently been exposed to the ransomware attack you decide to build a business contingency and continuity plan based on the lessons learned from that incident. You convince the CEO to approve the project by showing how much better the ransomware incident could have been handled if you Trouble-free Logistics invest in measures identified through the lessoned learned process.

b) Since the best business contingency and continuity plan you can have is a rehearsed and tested plan, you choose to suggest a cross division training program. Educating employees on how to respond in the event of a business disruption, as well as how to identify and report potential threats. This will help to build a culture of preparedness and ensure that everyone in the organization understands their role in maintaining business continuity.

c) To obtain approval from the CEO, you realize that you need to present convincing evidence of the benefits of investing in business contingency and continuity. Additionally, you, the CFO, CTO, and CSO are unsure about how to implement an effective business contingency and continuity plan in Trouble-free Logistics. Therefore, you opt to engage a consulting firm to provide advice and support during the planning phase. You share the BIA and risk assessment with them to ensure they have a thorough understanding of your business. This way, when you present the project to the CEO, you have compelling evidence of the benefits that result from improving business contingency and continuity.

d) Trouble-free Logistics has conducted a comprehensive Business Impact Analysis (BIA) and risk assessment. As a result, you choose to use the BIA to identify critical parts and processes of the business and establish contingency and continuity and sustainability requirements based on these. Together with the CFO, CTO, and CSO, you identify measures to meet these requirements. Ensuring the approval from the CEO, you emphasize how investing in these security measures not only reduces risk, but also addresses the findings from the BIA, improving services and increasing Trouble-free Logistics ability to sustain operations during disruptions.

Respons

Your score reflects how well "OPTION" addresses the business's needs and operations to ensure that contingency and continuity plans sustain services and processes during disruptions, emergencies, and crises.

Table G.18: Question 9: Business contingency and continuity

Alternative	Culture	Cost	Days	Decipher	Develop	Deliver	Lead
a	1	$20,000	4	1	1	1	0
b	2	$90,000	14	2	2	1	2
c	2	$115,000	8	3	2	3	1
d	4	$80,000	5	3	1	2	2

Appendix H

GTS results

Table H.1: Literature studied in the project as a result of the GTS

Reference	Resource type	Search term	Tool	Quality	Validation
[68]	Article	Social cybersecurity	Oria	High	Neutral
[46]	Book	Strategic AND Information Security	Oria	Moderate	Supporting
[70]	Article	Referenced by [46]	Oria	Moderate	Neutral
[78]	Journal	Asset assessment OR Threat Assessment OR Vulnerability assessment OR Information security	Oria	Low	Neutral
[69]	Article	Referenced by [78]	Oria	Moderate	Neutral
[26]	Dissertation	Strategic Decision-making AND filtered for last two years	Oria	High	Contradicting
[27]	Dissertation	Cybersecurity game OR Information security game	Oria	High	Neutral
[77]	Publication AND Dataset	A result of providing `iris.ai` with the exact text of the background (1.1) and problem description (1.1.2) of this thesis	Iris	Low	Neutral
[13]	Standards and frameworks	Referenced by multiple sources	Google	Low	Neutral
[11]	Standards and frameworks	Referenced by multiple sources	Google	High	Neutral
[14]	Standards and frameworks	Referenced by multiple sources	Google	High	Neutral

Table H.2: Literature studied in the project as a result of the GTS

Reference	Resource type	Search term	Tool	Quality	Validation
[79]	Journal	A result of providing `iris.ai` with the exact text of the background (1.1) and problem description (1.1.2) of this thesis	Iris	High	Neutral
[12]	Standards and frameworks	Referenced by multiple sources	Google	Moderate	Neutral
[18]	Standards and frameworks	Referenced by multiple sources	Google	High	Neutral
[34]	Standards and frameworks	Referenced by multiple sources	Google	Moderate	Neutral
[47]	Standards and frameworks	Referenced by multiple sources	Google	Low	Neutral
[43]	Report	Risk management AND vulnerability assessment	Google	High	Supporting
[40]	Book	Security management AND Risk management	Google	High	Supporting
[80]	Journal	Security management best practice AND Communication system security AND Risk management	Oria	High	Supporting
[81]	Journal	Security management best practice AND NIST	Oria	Moderate	Supporting
[118]	Book	Strategic Decision Making AND Risk management	Oria	Moderate	Neutral
[83]	Journal	What information related to cybersecurity is key for strategic decision-making and management of operations based on ground theory?	Elicit	Low	Neutral
[71]	Article	What information related to cybersecurity is key for strategic decision-making and management of operations based on ground theory?	Elicit	Low	Neutral
[82]	Journal	What information related to cybersecurity is key for strategic decision-making and management of operations based on ground theory?	Elicit	High	Neutral

Table H.3: Literature studied in the project as a result of the GTS

Reference	**Resource type**	**Search term**	**Tool**	**Quality**	**Validation**
[84]	Publication	What information related to cybersecurity is key for strategic decision-making and management of operations based on ground theory?	Elicit	Low	Neutral
[74]	Book	Cybersecurity AND decision-making	Oria	Low	Neutral
[73]	Book chapter	Cybersecurity AND decision-making	Oria	Moderate	Neutral
[75]	Book chapter	Cyber AND Cognitive	Oria	Moderate	Neutral
[76]	Book chapter	Cyber AND Cognitive	Oria	Moderate	Neutral
[72]	Article	Decision making	Oria	Moderate	Neutral

Appendix I

Original posts for sharing the game

Table I.1: Facebook post [99]

Account	**Forum or group**	**Date**	**Views**
Ulrik Sagelvmo	IT-sikkerhet	19.03.2023	Uknown

Post text
Heisann! I forbindelse med min masteroppgave ved NTNU Gjøvik har jeg utviklet et cybersikkerhet spill og trenger nå noen som kan spille det. Det slo meg at dette forumet passer helt perfekt. Så om du har lyst til å teste ut et spill som omhandler cybersikkerhet og setter dine beslutningsevner på prøve? Så hvorfor ikke gi det en sjanse og prøv "Trouble-Free Logistics" i dag? `https://ulrikasa.itch.io/trouble-free-logistics` Litt mer info her: Spillet er utviklet i forbindelse med min masteroppgave hvor jeg ønsker å kaste lys på hvilken type informasjon som gir mest verdi for en strategisk beslutningstaker. Du vil derfor bli kastet ut i virkelighetsnære problemstillinger som virksomheter kan stå ovenfor, og må ta beslutninger basert på den informasjon du får i spillet. Spillet bygger nemlig på «SANS Cyber42 Security Leadership Simulation», akademisk forskning og erfaringer fra ulike virksomheter. Data fra spillet vil brukes til å hjelpe fremtidens sikkerhetseksperter til å legge frem anvendelige og fornuftige rapporter til ledelsen, slik at vi sammen sikrer gode og effektive beslutninger. Ved å gjennomføre spillet er du med på å gjøre en forskjell! Takk på forhånd for din deltakelse!

Table I.2: LinkedIn posts (1-3) [100]

Account	**Forum or group**	**Date**	**Impressions**
Ulrik Sagelvmo	From personal account	19.03.2023	1848

Post text (1)
Vil du prøve et cybersikkerhet spill? Et spill som setter dine beslutningsevner på prøve? Kanskje lære noe nytt eller bli inspirert? Vel da har du muligheten her: `https://lnkd.in/dUMmkknm` Spillet er utviklet i forbindelse med min masteroppgave hvor jeg ønsker å kaste lys på hvilken type informasjon som gir mest verdi for en strategisk beslutningstaker. Du vil derfor bli kastet ut i virkelighetsnære problemstillinger som virksomheter kan stå ovenfor, og må ta beslutninger basert på den informasjon du får i spillet. Spillet bygger nemlig på «SANS Cyber42 Security Leadership Simulation», akademisk forskning og erfaringer fra ulike virksomheter. Data fra spillet vil brukes til å hjelpe fremtidens sikkerhetseksperter til å legge frem anvendelige og fornuftige rapporter til ledelsen, slik at vi sammen sikrer gode og effektive beslutninger. Ved å gjennomføre spillet er du med på å gjøre en forskjell! Så hvorfor ikke gi det en sjanse og prøve "Trouble-Free Logistics" i dag? Takk på forhånd for din deltakelse!

Account	**Forum or group**	**Date**	**Impressions**
Ulrik Sagelvmo	From personal account	27.03.2023	227

Post text (2)
Ikke fått prøvd cybersikkerhetsspillet enda? 3. april skal jeg begynne å sette sammen data fra spillet for å prøve å si noe om hvilken informasjon som gir mest verdi for en beslutningstaker. For å ha best mulig datagrunnlag ønsker jeg at enda flere får prøvd spillet. Så du har enda mulighet til å teste det, om du ikke har gjort det allerede. Likte du det og kanskje tror det kan være interessant for andre? Så del gjerne spillet videre!

Account	**Forum or group**	**Date**	**Impressions**
Ulrik Sagelvmo	From personal account	28.04.2023	362

Post text (3)
Oppdatering på #cybersikkerhetsspillet Først vil jeg bare takke alle som har deltatt. Håper dere syntes det var litt utfordrende, men samtidig morsomt. Jeg har fått flere henvendelser som går på hva best «Culture score» er. Så ønsker å dele Top 3 listen, den er som følger: **1.** 83, **2.** 81, **3.** 79. Har du ikke fått prøvd spillet, og vil se hvordan du gjør det? Da har du fortsatt muligheten her:

NTNU

Norwegian University of
Science and Technology