Degree Project

THE HUMAN CONNECTION TO INFORMATION SECURITY

A Qualitative Study on Policy Development, Communication and Compliance in Government Agencies

DEN MÄNSKLIGA KOPPLINGEN TILL INFORMATIONSSÄKERHET

En Kvalitativ Studie om Policyutveckling, Kommunikation och Efterlevnad inom Statliga Myndigheter

Bachelor Degree Project in Informatics with a Specialization in Information Systems
G2E, 30 ECTS
Spring term 2023

Osama Abdulhadi

Supervisor: Hanife Rexhepi
Examiner: Eva Söderström

ABSTRACT

The human factor and insider threats play a crucial role in information security. In today's digital age, protecting organizational data requires a deep understanding of human behaviour and its impact on information security. The increasing volume of electronically stored data has led to a rise in cyber threats and breaches, necessitating effective information security policies and regulations.

This study focuses on the experiences and perspectives of employees and top management in government agencies regarding the development, communication, compliance, and attitudes towards information security policies and regulations. Semi-structured interviews were conducted with participants from both top management or information security officers and regular employees, which allowed for an in-depth exploration of their experiences and perspectives.

The findings show that government agencies systematically develop policies by engaging stakeholders, ensuring accessibility, and adhering to legal frameworks. Addressing the human factor involves training, awareness programs, and top management support. Policy development and implementation include risk assessment, stakeholder identification, objective setting, continuous review, and integration into daily operations. Communication channels such as intranets, training, coordinators, and awareness events are utilized, but their effectiveness is not directly measured. Proposed improvements include enhancing accessibility, improving policy document management, and using clearer language.

Employees generally possess a positive attitude towards information security, though their understanding varies, and challenges to their understanding include complex language and unclear instructions. Compliance also varies, with difficulties arising from technical terminology and information overload. Enhanced compliance can be achieved through simplified language, providing better resources, and top management support. Proactive incident management focuses on learning and risk minimization. The human factor and insider threats remain significant concerns, which emphasizes the need for further education, awareness training, and motivation.

Keywords: Communication, Compliance, Development, Effectiveness, Government agencies, Human factor, Information security, Information security awareness, Information security culture, Information security management system, Information security policy, Insider threat

PREFACE

I am deeply grateful for the opportunity to present this thesis, which marks the culmination of my academic journey. I would like to extend my heartfelt gratitude to those who have supported and encouraged me throughout this journey.

First and foremost, I would like to express my profound appreciation and gratitude to my supervisor, Hanife Rexhepi, for your unwavering guidance, patience, and support. Your invaluable insights, expertise, and constructive feedback have significantly contributed to the development and refinement of this thesis. I am honoured to have had the opportunity to learn from such a knowledgeable and inspiring mentor. I would also like to extend my sincere thanks to my examiner, Eva Söderström, for your thorough review and invaluable suggestions for improvement. Your expertise and keen eye for detail have significantly enhanced the quality and rigor of this thesis. I am also immensely grateful to my critical friend, Marcus Sandrén, who has provided me with candid feedback and thought-provoking questions that have given a different perspective on things which in turn have enriched the thesis and sharpened the analysis. Your encouragement and commitment to my progress have been instrumental in shaping the direction of this thesis.

Lastly, I cannot forget to thank all the participants who so generously gave their time and shared their experiences through interviews. Your unique perspectives and insights have been vital in shaping the findings of this research. Without your openness and willingness to share your knowledge, this study would not have been possible.

I am fortunate to have been surrounded by such a supportive and collaborative academic community throughout this endeavour. I am truly grateful for the knowledge, personal growth, and friendships that have emerged from this experience.

Thank you all.

TABLE OF CONTENTS

GLOSSARY

CIA *– Confidentiality, Integrity and Availability*

CISO *– Chief Information Security Officer*

CSF *– Critical Success Factors*

IEC *– International Electrotechnical Commission*

IMY *– Swedish Authority for Privacy Protection*

IS *– Information Security*

ISA *– Information Security Awareness*

ISC *– Information Security Culture*

ISM *– Information Security Management*

ISMS *– Information Security Management System*

ISS *– Information Security Strategy*

ISO *– International Organization for Standardization*

ISP *– Information Security Policy*

MSB *– Swedish Civil Contingencies Agency*

OSL *– Public Access to Information and Secrecy Act*

SÄPO *– Swedish Security Service*

1 INTRODUCTION

Aware, careless, competent, compliant, defiant, greedy, helpful, mischievous, negligent, orderly, overzealous, trusting, vengeful, vigilante. In the day-to-day, these words are traits used to describe people and are important in understanding the behaviour and personality of individuals. These traits shape how individuals interact with the world around them and they can have a significant impact on their personal and professional lives (Caspi, Roberts & Shiner, 2005). In the realm of information security, these traits take on added significance. Protecting sensitive and confidential information requires a combination of technical solutions and a deep understanding of human behaviour and how individuals can impact the security of this information (Mazzarolo & Jurcut, 2019). Protection of information requires not only the implementation of technical measures, but also a comprehensive understanding of human behaviour and the ways in which it affects the security of information (Safa, von Solms & Futcher, 2016).

Today, organizations operate in a global and digitalized information society (van Niekerk & von Solms, 2005) where all types of people, with varying personalities, computer backgrounds and experiences are involved (Thomson & von Solms, 1998). Information security is therefore a critical strategic issue in organizational management, as the handling of sensitive data has become a concern for organizations, government agencies and individuals. The increasing amount of sensitive data being stored and handled electronically has led to a rise in cyber threats and information security breaches, which can have serious consequences for organizations, including financial losses, legal repercussions and damage to reputation (Safa, von Solms & Futcher, 2016; Tu & Yuan, 2014).

The threats to information security can be categorized into two categories, insider and outsider threats. Outsider threats refer to threats posed from outside the organization, such as hackers, while insider threats refer to threats posed from within the organization, mainly the employees (Humaidi & Balakrishnan, 2015). Outsider threats are easier to detect and defend against and organizations have come a long way in developing technological tools to deal with them. Insider threats, on the other hand, can manifest itself in many ways and are harder to address (Colwill, 2009). This has made it imperative for organizations that handle sensitive data to develop information security policies and regulations to not only ensure the protection of sensitive data and prevent information security problems, but also to comply with data protection laws (Colwill, 2009; Höne & Eloff, 2002a).

In order to develop effective information security policies and regulations, organizations must understand the latest threats and vulnerabilities. This requires a comprehensive approach that includes the development of policies and procedures for the protection of sensitive data. Furthermore, it requires the implementation of technical and organizational measures to ensure compliance (Höne & Eloff, 2002b). Once these policies and regulations have been developed, it is equally important for these organizations to communicate them effectively to employees. This requires clear and concise communication that is accessible to all employees, as well as ongoing training and awareness programs to ensure that employees understand the importance of complying with these policies (Tu & Yuan, 2014).

The attitudes of employees towards compliance with information security policies and regulations can have a significant impact on the success of these policies. A positive attitude towards compliance can help create a culture of security that supports the protection of sensitive data, while a negative attitude can undermine the effectiveness of information security policies and regulations (AlKalbani, Deng, Kam & Zhang, 2017; Höne & Eloff, 2002b). Hence, this study investigates how government agencies, that are responsible for handling sensitive data, develop information security policies and regulations, as well as their methods for ensuring employee compliance. Furthermore, the study investigates how these agencies disseminate rules and policies to their employees and explores the attitudes of employees towards complying with these regulations. By investigating these aspects, the study aims to facilitate improvements in the information security practices of government agencies, ultimately leading to enhanced protection of sensitive data and the cultivation of a culture of compliance among employees.

2 BACKGROUND

This chapter will cover the fundamental concepts of information security, such as management, policies, awareness and culture. It will also analyse the internal and external factors that affect information security within organizations, as well as the methods for developing and communicating security policies and regulations to employees. Finally, the chapter will cover employee attitudes towards these policies and regulations.

2.1 Information Security

Information plays a major role in supporting organizations in their business operations and gaining a competitive edge (Tu & Yuan, 2014). In its various forms, information is arguably an organization's most important asset (Gerber & von Solms, 2008). The growing use of information systems in organizations has made their vital information vulnerable to potential cybercrime. To protect this information, organizations must take proactive measures in today's rapidly changing environment (AlKalbani et al., 2017). Organizations are vulnerable to attacks from both inside and outside the organization making information security a major concern for organizational management (Tu & Yuan, 2014). Evidence suggests that malicious forces are active on the internet and many organizations using the infrastructure are susceptible to attacks. Companies providing anti-virus, malware or hacker defence solutions highlight the significance of outsider attacks (Sarkar, 2010). However, it's crucial not to ignore the potential for problems closer to home. Just as there are records of outsider attacks, there is also proof that insiders have been accountable for costly and significant information security incidents (Mazzarolo & Jurcut, 2019; Sarkar, 2010). This is a concerning issue as insiders are authorized users with a high chance of success (Sarkar, 2010).

Information security can be defined in several ways. The traditional industry standard defines information security as preserving the confidentiality, integrity and availability of information, also known as the CIA triad. However, this definition is not fully agreed upon by everyone in the industry (von Solms & van Niekerk, 2013). Elmrabit, Yang & Yang (2015) define information security as the process of safeguarding digital information assets and achieving primary security goals, which include confidentiality, integrity and availability. Confidentiality ensures that information is kept private and is not disclosed to unauthorized individuals or systems. It involves making sure that data assets are not accessible to unapproved users. Integrity guarantees that data cannot be modified by any unauthorized parties and that the data remains the same as when it was originally created. Availability ensures that data assets are accessible to authorized users when requested. It ensures that data assets are always available for legitimate users.

Whitman and Mattord (2021) define information security as protecting information, its critical elements and the systems that use, store and transmit it. They identify confidentiality, integrity and availability of information as critical characteristics, but do not limit the definition to these three. They add accuracy, authenticity, utility and possession to the list. They also note that the CIA triad model is no longer adequate in the constantly changing computer industry and that more characteristics need to be considered and included.

Information security furthermore, refers to a process and not a product or technology. It used to be solely technical but has evolved to include non-technical aspects as computer and network usage have advanced (Whitman & Mattord, 2021). Zinatullin (2016) states that information security is a field that aims to protect a company's confidential information and assets. It is similar to medicine in that there are generalists and specialists who have different levels of expertise in various areas of security. The goal of information security is to identify and protect assets, which help a company generate revenue. The three pillars of information security are confidentiality, availability, and integrity and they need to be linked back to business requirements. The language of the business and the language of information security are different and security professionals must be able to manage this translation effectively. Business and security professionals have common ground in managing risk.

Today, information security is commonly defined in terms of secure information properties or characteristics, including confidentiality, integrity and availability, but may also include additional characteristics (von Solms & van Niekerk, 2013). The definitions of information security described are largely consistent, but there are some nuances in the way the various authors describe and conceptualize the concept. One issue that stands out is the relative emphasis placed on the CIA triad as a defining feature of information security. While some authors view this as a core aspect of the definition, others argue that it is not sufficient to capture the full range of concerns and challenges associated with information security.

Another issue that arises is the question of whether information security should be understood primarily as a technical or non-technical phenomenon. While some authors suggest that it has evolved to encompass a broader set of considerations beyond technical aspects, others may view it more narrowly as a set of technical measures and protocols for safeguarding data and systems.

Given these issues, this thesis will proceed with the definition presented by Whitman and Mattord (2021), as it offers a more comprehensive and nuanced understanding of information security than the other definitions. They emphasize that information security is not limited to the CIA triad, but also includes additional characteristics such as accuracy, authenticity, utility and possession. This broader view of information security acknowledges the complexity and diversity of modern information systems and the need to address a wide range of security concerns beyond just confidentiality, integrity and availability.

Furthermore, Whitman and Mattord's definition recognizes that information security is a process rather than a static product or technology. This perspective aligns with contemporary thinking about information security as an ongoing and adaptive effort to manage risks and threats in a rapidly changing digital landscape. Overall, their definition provides a more nuanced and holistic view of information security that reflects the complex and dynamic nature of this study.

2.1.1 Information Security Management

As the business world becomes more interconnected globally, electronic transactions are becoming more prevalent and leading to an exponential increase in handling and storing

of personal and sensitive data (Sarkar, 2010). Organizations are today more reliant on Information Technology (IT) than ever before, as information technology plays a crucial role in their daily operations and various other essential business processes (Flowerday & Tuyikeze, 2016). They now understand the value of the sensitive data being stored and handled, as it is considered the lifeblood of their operations. However, with the advancement of technology and the breaking down of traditional security boundaries, sensitive data is increasingly accessible to external parties, such as mobile users, business partners and contractors, making it increasingly vulnerable to outsider threats and attacks (Sarkar, 2010). Lack of information security can not only compromise the stability of an organization but also put its survival at risk (Gerber & von Solms, 2008). This has led to an increase in need for proper information security management, where proper information security management is essential for maintaining a high level of information security within organizations (Tu & Yuan, 2014).

Information security management (ISM) is a subset of information security that deals with the interface between an organization and the security mechanisms it employs (Coles-Kemp & Theoharidou, 2010). ISM aims to protect the confidentiality, integrity and availability of information and mitigate its risks and threats. It is a systematic process of implementing physical, technical or operational security controls to secure information assets and achieve organizational goals. ISM covers the strategic, tactical and operational aspects of an organization's information security program and can reduce security threats and help foster secure business information sharing (Tu & Yuan, 2014).

Tu & Yuan (2014) discusses critical success factors (CSFs) that contribute to the success of an organization's ISM. They state that effective organizational information security management encompasses managing people, processes and technology. They propose six constructs of ISM success model: business alignment, organizational support, IT competence, organizational awareness, security controls development and ISM performance evaluation. They suggest that the alignment of information security objectives with business strategy positively affects organizational support, IT competence and organizational awareness, which ultimately leads to an effective information security strategy (ISS). Additionally, they emphasize the importance of security awareness and training programs for all employees in the organization.

2.1.2 Information Security Policy

One of the most important security controls, to manage the implementation and ensure the effectiveness of information security within an organization, is the information security policy (ISP) (Flowerday & Tuyikeze, 2016; Höne & Eloff, 2002a). An information security policy is a document that outlines an organization's goals and objectives for protecting sensitive information and specifies the measures and guidelines to be followed by employees, contractors and other stakeholders to ensure the confidentiality, integrity and availability of information. The ISP sets the standards and expectations for information security and outlines the roles, responsibilities and expectations for all stakeholders to ensure the protection of information assets (Flowerday & Tuyikeze, 2016). Furthermore, it serves as a guiding document, setting the scope of information security and demonstrating management's commitment to information security goals and objectives. The policy outlines the organization's approach to information security and the role it plays in achieving the organization's overall vision and mission. One of its

main goals is to clearly establish the rights and responsibilities of those who handle sensitive information within an organization (Höne & Eloff, 2002b).

An effective information security policy is a crucial component in achieving the information security goals of an organization. The policy must balance the requirements for secure information handling by users with the strategic objectives of the business. To be effective, the information security policy must be a well-defined, practical document that is user-focused and written in a style and tone consistent with the organization's overall communication style and culture. The policy should be presented in a clear and user-friendly manner and be developed in collaboration with representatives from all stakeholders (Höne & Eloff, 2002b). Without understanding their responsibilities, employees may struggle to abide by the policy. A policy that does not align with the goals of the business and does not consider its core mission is likely to be disregarded whenever it hinders productivity or revenue generation (Metalidou et al., 2014). The commitment of top management is critical for the policy's success and the dissemination of the policy throughout the organization. The language of the policy should be unambiguous to prevent misinterpretation. The main document should be concise and presented as a high-quality deliverable and the implementation of the policy should be supported by supplementary policies, standards and guidelines (Höne & Eloff, 2002b).

2.1.3 Effectiveness

An information security policy is considered effective when it communicates the expectations for handling information resources to users in a clear and easily understood manner. The content of the policy is important, but the way it is presented and communicated to the users is crucial for its effectiveness. An effective policy directly contributes to overall information security. (Höne & Eloff, 2002b).

2.1.4 Information Security Awareness

Information security awareness (ISA) is defined as the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organization and their individual security responsibilities and acts accordingly (The European Security Forum, 1993, cited in Metalidou et al., 2014). Information security awareness (ISA) is the most important factor that mitigates the risk of information security breaches in organisations (Safa, von Solms & Futcher, 2016).

Increasing information security awareness is achieved by performing processes that educate individuals within an organization about information security policies, procedures and best practices. The aim of information security awareness is to increase knowledge and understanding of the importance of protecting sensitive information, as well as to equip individuals with the skills and knowledge needed to identify and prevent potential security threats. Information security awareness can take many forms, including training programs, workshops and regular reminders to employees (Chen, Shaw & Yang, 2006). The goal of information security awareness is to build a culture of security within an organization and to ensure that all employees are equipped with the tools they need to protect sensitive information from unauthorized access and breaches (Amankwa, Loock & Kritzinger, 2014).

Information security awareness can be categorized into three categories, awareness of severity, awareness of susceptibility and awareness of benefits of security countermeasures. Awareness of severity refers to a user's understanding of the gravity of information security threats. Awareness of susceptibility pertains to a user's perception of the likelihood of an organization's information being exposed to security threats. Awareness of the benefits of security countermeasures refers to the extent to which users recognize the positive results of engaging in secure behaviours, such as properly using security measures (Humaidi & Balakrishnan, 2015).

Protecting information within an organization is the responsibility of all staff (Colwill, 2009). Information security awareness is a critical aspect in achieving this (Safa, von Solms & Furnell, 2016). By raising awareness about information security, organizations can reduce the risk of security breaches and ensure that sensitive information is properly protected (Elmrabit, Yang & Yang, 2015). This not only helps to prevent security incidents, but it also helps to meet regulatory requirements, maintain customer trust and enhance the overall security culture within the organization (Lopes, Guarda & Oliveira, 2019). Information security awareness training can provide employees with the knowledge and skills they need to identify and avoid potential security threats and it can help to build a culture of security within the organization that encourages all employees to take an active role in protecting sensitive information (van Niekerk & von Solms, 2005).

2.1.5 Information Security Culture

Information security culture is defined as the collective attitudes, assumptions, beliefs, values and knowledge that employees or stakeholders hold, which they use to interact with the organization's systems and procedures. This interaction leads to either acceptable or unacceptable behaviour, which is reflected in the artifacts and practices that become part of the organization's way of protecting its information assets. This information security culture is constantly evolving over time (Da Vega & Eloff, 2010). To carry out information-related tasks securely on a daily basis, users must have the necessary skills and proficiencies, as well as sufficient knowledge of how to perform their tasks securely. Artifacts represent the visible day-to-day actions taken and behaviour in the organization (van Niekerk & von Solms, 2005; Van Niekerk & Von Solms, 2010). These artifacts of information security practices can be seen as a result of the implementation of various components, such as risk management and policies. For example, a bank (a bureaucratic organization), may use public key encryption, while an energy and natural resource company, with a task-based culture, may use passwords to secure files sent via e-mail (Da Veiga & Eloff, 2010).

A strong information security culture is one where employees are knowledgeable about security policies and practices, are vigilant about potential security threats and are committed to protecting sensitive information. The education of personnel is crucial in building a strong culture that prioritizes information security. Employees must be taught to value and prioritize security in their daily operations. This mindset is critical, as it leads to a change in behaviour, turning employees from being a potential risk to instead being an asset for information security and the organization (van Niekerk & von Solms, 2005). In order to achieve this, security cannot be treated as an afterthought, but must be prioritized and fully integrated into the organizational culture. This integration

must start at the top levels of the organization and involve all employees (Corriss, 2010). Leadership from the top management is crucial in achieving a strong security culture. It is often said that good habits are learned from examples and the same is true for security habits. If senior managers are not following security protocols, it sends the message to junior staff that these protocols are not important (Walton & Limited, 2006).

2.2 The Human Factor in Information Security

Technical solutions are continuously being developed and organizations have, in that aspect, come a long way in reducing the number of possible attacks (Aloul, 2012). However, a system is only as strong as its weakest link and information security today has a weak link that remains unexplored and neglected (Georgiadou, Mouzakitis & Askounis, 2022; Metalidou et al., 2014). This weak link in information security is the human factor (Al Zaabi, 2015; Georgiadou, Mouzakitis & Askounis, 2022: Metalidou et al., 2014). Hackers know this and focus have shifted to trying to compromise organizations and users by attacking the people involved, through means such as social engineering, to gain access to the systems or other sensitive data (Al Zaabi, 2015). This has become even more apparent with the recent transition to remote working solutions due to the COVID-19 pandemic, where the most popular attack has become phishing attacks (Škiljić, 2020).

The hackers, however, are not the only threat. Often, organizations focus on the outsider threats and depend on the insiders' morals and ethics to not cause security issues (Carroll, 2006). In organizations, employees have their own attitude towards information security, either positive or negative, which directly influence the information security and implementation of security controls (Tu & Yuan, 2014). This influence underscores the value of cultivating a strong information security culture, as it significantly shapes individual attitudes and the subsequent behaviours towards security measures. Therefore, encouraging users to adhere to information security policies is crucial in order to minimize potential threats (Bauer, Bernroider & Chudzikowski, 2017). In 1995, an Australian company encountered this where employees, due to lack of understanding of why they were in place, tried to circumvent policies and regulations or pushed to have them changed or removed because they were burdensome (Spurling, 1995). This case exemplifies the need for an established security culture and sufficient security awareness within the organization, which fosters an understanding of why such regulations are vital and should be adhered to.

Research on the human factor in information security has been largely neglected despite being a crucial aspect of security. Organizations often rely on technology as a quick fix to security problems, but it is the human element that security depends on. Survey results have shown that even those who claim to have security awareness still engage in actions that put the system at risk. Improper training can render even the best software or hardware solution useless and human error, often resulting from lack of awareness or understanding, has been consistently named as the greatest security weakness, outpacing technology as a source of security breaches (Metalidou et al., 2014).

Information security used to rely solely on technology, but as the field has matured, it now recognizes the importance of a holistic approach that encompasses technology, processes, people and organizational factors, including the previously mentioned human

factors of awareness and culture. Technical approaches alone cannot solve information security problems, as it also involves social and organizational issues (Baker & Wallace, 2007).

2.3 Information Security Threats

Information security threats can be broadly classified into two categories, insider and outsider threats. Insider threats are those that originate from within the organization, such as employees, contractors, or other individuals with access to the organization's information systems and resources. Outsider threats are those that originate from outside the organization, such as hackers, cybercriminals, or nation-states (Humaidi & Balakrishnan, 2015). These insider and outsider threats can be further categorized into intentional and accidental types (Cheng, Liu & Yao, 2017).

2.3.1 Outsider Threats

Outsider threats to information security include hacking, denial of service attacks, malware, viruses and phishing attacks through social engineering tactics. Outsider threats are almost always intentional and are often motivated by a desire for personal or organizational gain or a desire to cause harm (Cheng, Liu & Yao, 2017). These threats can lead to data loss, financial loss, damaged reputation and legal repercussions (Tu & Yuan, 2014). Outsider threats are often the primary focus for organizations and is what organizations put most of their information security efforts into. According to Colwill (2009), 90% of security controls and monitoring are focused on outsider threats.

The defining characteristic of outsider attackers is their restricted ability to perform their attacks. They can only achieve entry into the organization's information system by exploiting weaknesses or gaps in its security measures. The motivation behind these attacks is generally beyond the control of the target organization, which calls for strengthening its technical and non-technical protection measures. This includes enhancing its capacity to detect and prevent attacks, limiting the attacker's ability to inflict damage and facilitating recovery in the event of a successful breach of security (Walton & Limited, 2006).

2.3.2 Insider Threats

Insider threats can manifest itself in many ways (Colwill, 2009) and can be categorized into two categories, intentional and unintentional (Cheng, Liu & Yao, 2017; Mazzarolo & Jurcut, 2019). Intentional insider attacks can be driven by a variety of reasons such as corporate espionage, anger towards their employer or financial gain. Unintentional accidental leaks usually occur due to neglect of security measures and procedures, inadequate technology or lack of employee awareness (Cheng, Liu & Yao, 2017). Beyond awareness, users' mistakes can stem from ignorance, negligence, apathy, mischief or resistance (Safa, von Solms & Furnell, 2016).

Intentional insider threats often possess a unique level of ease in execution, as they typically do not require advanced technical skills. Additionally, insiders possess valid authorization and are intimately familiar with the vulnerabilities of the organization, making detection of their malicious activities challenging (Mazzarollo & Jurcut, 2019;

Sarkar, 2010). The potential for malicious insiders to meticulously erase their tracks from log systems and utilize contemporary technologies, such as steganography or wireless technology to steal sensitive information only compounds the difficulty in detecting these threats (Sarkar, 2010).

Insider threats to information security can come in the form of accidental misuse, intentional misuse and misuse due to ignorance. Accidental misuse can occur when employees bypass company security policies to meet business needs, leading to security breaches such as sending confidential information to the wrong recipient or exposing sensitive information on social media. Intentional misuse can come from insiders who use corporate resources for their own purposes or who have malicious intentions such as selling sensitive information or sabotaging the company's infrastructure. Misuse due to ignorance happens when employees are unaware of how to effectively protect data, leading to incidents such as unencrypted data being lost or stolen or the use of proprietary software without realizing it. Additionally, insiders can also cause harm by modifying operating systems, networks, hardware, or applications, either accidentally or intentionally. These modifications can leave the system vulnerable to attacks or data breaches (Sarkar, 2010).

Sharing username and password with co-workers, recording them on sticky notes displayed on desks or monitors, opening unknown emails and attachments, downloading software from the internet and leaving computer systems logged in while unattended are all examples of mistakes employees make and that are an unintentional insider threat to information security (Safa, von Solms & Futcher, 2016). Being lured into opening malicious emails or attachments is an example of being susceptible to a social engineering attack, specifically a phishing attack (Mazzarolo & Jurcut, 2019). Social engineering attacks are usually considered an outsider threat because the source of the attack is an outsider, but the attack is carried out by exploiting the weaknesses or trust of internal entities within an organization (Metalidou et al., 2014). However, social engineering attacks can also be carried out by internal sources too, making it an insider threat (Sarkar, 2010).

Dealing with insider threats can be challenging as insiders often have necessary access to systems and sensitive information to perform their job duties. However, this same access that is crucial to their work can also be used to cause significant harm. This ability to cause harm while having legitimate access makes the insider threat particularly serious and difficult to mitigate (Walton & Limited, 2006).

2.3.3 Probability and Impact of Information Security Threats

In terms of probability, malicious outsider threats are more likely. Those with motives to cause significant harm to a company's information systems, such as theft of confidential information, disruption of capability or wreaking havoc are typically outside the corporation, including rival companies, enemies or criminals (Walton & Limited, 2006). However, insider threats pose a greater risk to organizations as insiders have legitimate access to sensitive information, knowledge of the organization's processes and assets and the ability to cover their tracks (Colwill, 2009). This ease of access and extensive knowledge makes the insider threat particularly serious, even though the vast majority of insiders are trustworthy. The few exceptions to this can be divided into two

categories, the disaffected and the subverted. The subverted refer to those who have deliberately chosen to undermine or attempt to overthrow an established system or organization while the disaffected refer to those who are dissatisfied with the organization or its policies and may act in ways that increase the risk of a security breach (Walton & Limited, 2006). Outsiders typically need to gather intelligence and overcome security barriers, while insiders can target information directly. Outsiders may also exploit insiders by subverting them to steal information, as outsourcing and third-party access can dilute security controls (Colwill, 2009). While technical and other measures may somewhat reduce the damage, the primary focus of defensive measures should be on deterring discontent and countering subversion. To a certain extent, in terms of probability, the insider threat can be managed by the organization, unlike the outsider threat, which is beyond its control (Walton & Limited, 2006).

In terms of impact, no outsider technological attack has ever come close to causing the downfall of a significant corporation or organization. On the other hand, the downfalls of Barings, BCCI, Worldcom, Enron, Societe Generale and the recent cases of Satyam, Stanford and Madoff were caused by shortcomings in internal controls and unethical behaviour by a limited number of authorized employees, often in high-ranking positions, known as trusted insiders (Colwill, 2009).

2.3.4 Investments to Protect Against Information Security Threats

Investment in controls to protect against insider threats is limited. Studies show that 70% of fraud is carried out by insiders rather than outsider criminals, yet 90% of security controls and monitoring are focused on outsider threats. While technical controls for insiders exist, they should not be considered as the sole solution. A greater investment in organizational human factors is necessary to balance the funding in technology. Given the right motivation and time, humans can bypass most technical controls (Colwill, 2009).

Organizations invest heavily in creating robust perimeter defences to safeguard their essential infrastructure and data from outsider threats such as hackers. However, although necessary, these defences do not cover the breaches committed by insiders. According to the Verizon 2009 Data Breach Investigations Report, insider breaches remain significantly more destructive compared to other sources of attack (Verizon, 2009, cited in Sarkar, 2010). Although, outsider threats have a higher probability (Walton & Limited, 2006), Sarkar (2010) states that the Verizon 2009 Data Breach Investigation Report (2009) showed a rise in the number of insider breaches. Despite this, organizations primarily concentrate on averting outsider attacks (Sarkar, 2010). The lack of addressing the insider threat can be due to several factors like organizations not realizing it is happening, fearing bad publicity, being in denial or not knowing how to handle it (Colwill, 2009).

2.4 Development of Information Security Policies and Regulations

Developing the information security policy can be challenging, but it is a vital part of the organization's strategy for achieving a high level of information security (Höne & Eloff, 2002a). The development goes beyond mere policy formulation and just creating and implementing it. Organizations must understand the various steps involved in the policy

development process, otherwise they risk creating an ineffective, deficient, redundant and irrelevant policy that lacks support from users (Flowerday & Tuyikeze, 2016). Although there is a vast amount of research on information security policies there is no consensus or definitive guide on how they should be developed. Rather than relying on a one-size-fits-all approach, the development of an information security policy should put more emphasis on addressing the unique information security needs of each individual organization (Paananen, Lapke & Siponen, 2020). However, there are general steps involved in the policy development process such as conducting a risk assessment, identifying stakeholders, setting security objectives, developing, reviewing, implementing, maintaining and updating the policy. Furthermore, there are common components of what an information security policy should contain, such as scope, roles, responsibilities and security controls (Flowerday & Tuyikeze, 2016; Ismail, Widyarto, Ahmad & Ghani, 2017; Knapp, Franklin Morris, Marshall & Byrd, 2009). The following subsections will elaborate further on the key steps involved in the development of information security policies and outline the essential content that should be included in the policy.

2.4.1 Assessment of Policies and Risks

The process of policy formation begins when the need for addressing an issue arises. This could result in the creation of a new policy or the revision of an existing one. Information analysis plays a vital role in every stage of policy making, starting with identifying the problems and risks (Ismail, Widyarto, Adiyarta, Syafrullah & Tajuddin, 2022). Policy assessment is a process of evaluating existing policies, standards, guidelines and procedures. The categorization of the proposed change as strategic or tactical will influence later steps in the process, but if the organization is implementing the model for the first time, it is considered strategic. The policy assessment step includes four sub-processes: analysing the policy environment, identifying policy gaps and contradictions, summarizing policy assessment results and developing policy recommendations. These sub-steps result in a decision on whether to approve the proposed changes and an assessment of their impact on existing policies (Rees, Bandyopadhyay & Spafford, 2003).

The process of risk assessment must identify, analyse and evaluate the information security risks and controls related to an information system or service in a systematic manner. This provides a comprehensive and organized view of the current IT security risks and the security measures needed to manage them (Ismail et al., 2022). Risk assessment involves evaluating the current state of the organization's information security, including identifying potential threats and their associated risks, as well as determining vulnerabilities and assessing the efficiency of existing security controls (Flowerday & Tuyikeze, 2016; Ismail et al., 2017; Rees, Bandyopadhyay, & Spafford, 2003).

2.4.2 Stakeholder Identification, Engagement and Role Definition

Identifying key stakeholders and ensuring their engagement is an important aspect of the development of an information security policy. Stakeholders can include employees, management, customers, partners, regulators and others who have an interest or are impacted by the organization's information security practices (Ismail et al., 2017).

Once the stakeholders have been identified, it is important to engage with them to gather input on security requirements and priorities, understand their perspectives and needs and to ensure that their voices are heard in the policy development process. This can ensure that the stakeholders are committed to it and that they act as advocates for the policy post-implementation (Paananen, Lapke & Siponen, 2020). Furthermore, it is important to set clear roles and responsibilities for each stakeholder to ensure that everyone understands their obligations and how they fit into the overall information security program (Flowerday & Tuyikeze, 2016). Each individual in an organization must understand their specific role and responsibilities in maintaining information security, as well as the impact of their actions on the overall security of the organization (van Niekerk & von Solms, 2005).

2.4.3 Setting Security Objectives and Determining Security Controls

After conducting a policy and risk assessment, management should perform a security strategy (Flowerday & Tuyikeze, 2016). The security strategy is a comprehensive plan that outlines the future business and security objectives and the necessary security controls to support the organization in reaching these objectives. To develop a security strategy, a session should be held with key management personnel to identify future business initiatives, identify security options, prioritize security initiatives and document the security strategy (Rees, Bandyopadhyay & Spafford, 2003).

2.4.4 Policy Development

Development of the policy itself where it is important to consider industry standards, best practices, legal and regulatory requirements, and other relevant frameworks (Höne & Eloff, 2002b). In light of the growing significance of information security across organizations globally, international laws, regulations, standards and policies have been established to aid organizations in safeguarding their information. There is a growing expectation from stakeholders for organizations to comply with these policies and regulations. These pressures influence the behaviours of organizations in their efforts to protect their information in today's dynamic environment (AlKalbani et al., 2017).

Different standards and regulations exist with varying objectives, requirements and specifications. The International Organization for Standardization (ISO) is an example. It sets international standards for a variety of industries, including information technology and information security (Lopes, Guarda & Oliveira, 2019). The collection of ISO standards that pertain to information security is known as the ISO/IEC 27000 series (International Organization for Standardization [ISO], 2018). ISO standards provide a common framework and set of guidelines for organizations to follow to ensure consistency and quality in their operations (Koza, 2022). Another example is the General Data Protection Regulation (GDPR). GDPR is a regulation by the European Union (EU) that protects the privacy and personal data of EU citizens. It sets standards for how personal data should be collected, processed and stored by organizations operating within the EU. These standards and regulations are designed to promote consistency and best practices in their respective area of focus and require organizations to demonstrate compliance with these standards and regulations through regular audits and assessments (Lopes, Guarda & Oliveira, 2019). GDPR has legal force and carries penalties for non-compliance as it is a regulation, while ISO compliance is voluntary. However,

some countries or industries may require compliance with specific ISO standards as a regulatory requirement (Lopes, Guarda & Oliveira, 2019). ISO standards are used by organizations globally, while GDPR regulations only apply to organizations operating within the EU. In the United States, for example, the Federal Trade Commission (FTC) is the agency responsible for protecting consumer rights and preventing anti-competitive business practices and in the United Kingdom, the Information Commissioner's Office (ICO) acts as the independent regulator for data protection and privacy (Wolff & Atallah, 2021).

These international information security standards, frameworks and regulations offer guidance and requirements for writing an effective policy. Common elements of an information security policy include the need and scope of information security, management's commitment statement and the roles and responsibilities of users (Höne & Eloff, 2002a). These international standards, such as ISO, are designed to be flexible, allowing organizations to adapt them to their specific needs and requirements. They are also designed to be enforceable, so that organizations can be held accountable for non-compliance (Gerber & von Solms, 2008). The standards can provide guidance to organizations on how to develop their policies, but it is important to remember that the policy must reflect the organization's culture and goals and not copy a template or another organization's policy (Höne & Eloff, 2002a; Ismail et al., 2017).

2.4.5 Policy Review and Approval

The policy should be reviewed and approved by key stakeholders, such as executives, legal counsel and information security personnel to ensure that it meets the organization's needs and requirements and that it complies with relevant standards, laws and regulations (Flowerday & Tuyikeze, 2016; Knapp et al., 2009).

After creating the policy document and conducting initial coordination, it should be assessed by an independent party or group, such as a policy evaluation committee before final approval. A policy evaluation committee is established to provide a comprehensive platform for evaluating and assessing the effectiveness of security policies, standards, baselines and guidelines that impact the entire organization. This committee should consist of stakeholders from various parts of the organization, tasked with ensuring that security policies, standards, baselines and guidelines are well-written, clearly understood, properly coordinated and feasible for the people, processes and technologies they affect. An independent review has several benefits, including a sounder policy through scrutiny from different perspectives, increased support from a wider range of stakeholders and improved credibility through input from specialist reviewers. The policy must be presented to the reviewing party and any issues addressed, the objective, context and potential benefits explained and justification provided for the need for the policy. The policy creator must address comments and recommendations for changes, make necessary adjustments and revisions and finalize the policy for management approval (Howard, 2003).

The purpose of the approval process is to gain management support and endorsement of the policy through a signature from a high-level company official. This approval enables and ideally triggers the implementation of the policy. The policy creator must determine the appropriate approval authority, coordinate with them, present the policy review

recommendations and work to secure broader management support. If the approval authority is hesitant to fully approve the policy, the creator must handle issues of interim or temporary approval (Howard, 2003). In the event that a policy proposal is disapproved, the developers may be required to revise the policy or certain portions of it in accordance with the feedback from the reviewing party (Knapp et al., 2009).

2.4.6 Implementation and Communication

Once the policy has been approved, it moves into the implementation phase of its lifecycle and should be implemented across the organization (Ismail et al., 2022). The first step in this phase is communicating the policy. This involves distributing the policy to employees and others affected by it, considering factors such as geography, language, culture, unauthorized disclosure and the role of the supervisory chain in communication. A plan for policy communication, implementation, or rollout can help address these issues and provide details on the resources required, resource dependencies, employee acknowledgment and visibility-enhancing strategies (Howard, 2003). This may involve providing training and education on security procedures and guidelines and establishing a process for regularly monitoring and reviewing the policy to ensure it remains effective and relevant (Ismail et al., 2022).

2.4.7 Evaluation, Maintenance and Updates

The information security policy should be an evolving document that keeps pace with the growth and development of the organization (Höne & Eloff, 2002b). The continuous evaluation of the policy is necessary once implementation has begun. With technology advancements and the rise of internet usage, new security threats are appearing more frequently (Ismail et al., 2022). Regular updates are crucial to ensure the policy supports the organization's vision and mission and remains relevant and up-to-date. The review period should align with the organization's normal business cycles, taking into consideration that certain times may not be suitable for change or new ideas. For example, financial year-end periods can be critical and busy, making users less receptive to change (Höne & Eloff, 2002b). Continuous evaluation, maintenance and updates ensures the current status and validity of a policy. This involves tracking changes that may impact the policy, such as changes in technology, processes, people, organization, or business focus and making recommendations for policy modifications accordingly. It also involves documenting policy changes and maintaining effective version control for policy integrity. When changes to the policy are necessary, key functions such as review, approval, communication and compliance must be revisited (Howard, 2003).

2.5 Communication of Information Security Policies and Regulations

An effective information security policy is dependent on the users knowing about it. The policy should be disseminated across the entire organization in a manner that fits with the organization's traditional methods and can be reinforced through training and awareness sessions with top management support (Höne & Eloff, 2002b). The responsible party for disseminating security procedures should be the proponent, but they should strive to involve the communications department, if there is one, to help carry out this task (Howard, 2003).

2.5.1 Awareness Training

Without ensuring that every person involved understands their roles and responsibilities and has the proper training, it is impossible for organizations to secure the confidentiality, availability and integrity of information in today's highly connected systems. It's crucial for individual users to understand the specific operational controls that depend on their behaviour for effectiveness. Extensive awareness and training programs are necessary to achieve this level of knowledge (van Niekerk & von Solms, 2005). Training, awareness and education serve not only to spread policy but also to establish a security-focused culture, reducing the risk of insider attacks (Coles-Kemp & Theoharidou, 2010).

To ensure that subjects are aware of the information security policy, user training and testing are essential. User participation in activities is crucial for changing security behaviour. Changing formal policies into an informal change in security behaviour requires long-term continuous efforts to institutionalize the changes. This can be a significant challenge, as subjects may have adopted values and behaviours from other sources, such as other organizations or their personal lives, that impact their adoption of the new policy (Paananen, Lapke & Siponen, 2020).

Every organization should have a comprehensive security awareness program where all employees undergo periodic training, with additional smaller briefings as needed. The training should include education of employees on the dangers of social engineering techniques and how to protect sensitive information (Sarkar, 2010). A formal security awareness program sponsored by the organization is a means to raise overall understanding and awareness of information security. Security awareness programs can be carried out through various means such as newsletters, posters, promotional items and web pages (Chen, Shaw & Yang, 2006). The training program is the primary method of communicating security policies, procedures and requirements throughout the organization. This can increase employee knowledge and involvement in security efforts (Tu & Yuan, 2014).

2.5.2 Regular Reminders and Updates

It is important to have regular reminders and updates in communication of information security policies in an organization because employees tend to forget or overlook security protocols over time (Knapp et al., 2009). This is particularly true in organizations where employees are constantly being exposed to new technology and work processes (Mazzarolo & Jurcut, 2019). Regular reminders and updates can help keep security top of mind and ensure that employees remain vigilant in following security policies and procedures (Da Veiga & Eloff, 2010). Additionally, regular reminders and updates can help ensure that security policies remain relevant and up-to-date in light of changing threats and technologies (Amankwa, Loock & Kritzinger, 2014; Ismail et al., 2017). Regular communication further contributes to fostering a culture of security awareness and responsibility, where employees take security seriously and feel empowered to report any potential security risks (Van Niekerk & Von Solms, 2010).

This must also be adhered to when an employee departs from the organization, whether through retirement or a job change. This should involve a farewell interview to remind

the employee of their security obligations and responsibilities, to retrieve any company property such as badges or keys and to provide the opportunity for the employee to voice any security-related concerns or provide feedback (Walton & Limited, 2006).

2.5.3 Monitoring and Enforcement

Monitoring tracks and reports on policy compliance effectiveness. This information is gathered from employee and supervisor observations, formal audits, assessments, inspections, reviews, violation reports and incident response activities. The monitoring function involves ongoing efforts to monitor compliance or noncompliance through both formal and informal methods and reporting any deficiencies to relevant management for action. The duty of monitoring compliance with security policies, standards, baselines and guidelines that apply to the whole organization is shared among employees, managers, the audit function and the information security function. Every employee bound by security requirements should aid in monitoring compliance by reporting any deviations they notice. (Howard, 2003).

The main duty of enforcing security requirements lies with managers of individuals affected by the policy. Enforcement provides the strength behind a policy's compliance. It involves management's response to policy violations with the aim of preventing or deterring repeat incidents. Once a violation is discovered, corrective action must be taken to address the people, processes and technologies involved, in order to reduce the likelihood of future violations. Including information on corrective actions in awareness efforts can be highly effective (Howard, 2003). Top management must demonstrate their support for the desired outcomes by exhibiting the appropriate behaviour and by providing incentives for good behaviour and consequences for negative behaviour. Both incentives and consequences are crucial in shaping employee adherence to information security policies (van Niekerk & von Solms, 2005).

2.6 Employee Attitudes Towards Information Security Policies and Regulations

The attitudes of employees towards compliance with information security policies and regulations are an important factor in ensuring that organizations can reduce the risks associated with insider threats (van Niekerk & von Solms, 2005). Employees who have a positive attitude towards compliance are more likely to adhere to the policies and regulations that they are required to follow (Da Veiga & Eloff, 2010).

Employee attitudes towards information security can vary greatly and are closely related to information security awareness and culture. A strong information security culture is built on the foundation of employee awareness and understanding of the importance of protecting confidential information (Safa, von Solms & Furnell, 2016). Some employees understand the importance of protecting confidential information and take the necessary precautions to maintain the security of that information. When employees understand the significance of their actions, they are more likely to embrace security policies and procedures, making them an integral part of their work (AlKalbani et al., 2017). They understand that their actions can have a significant impact on the company's reputation and financial stability and they take their responsibilities

seriously, thus becoming an asset to information security instead of being a risk (van Niekerk & von Solms, 2005).

On the other hand, a lack of employee awareness and understanding can lead to a weak security culture and a higher likelihood of security breaches (van Niekerk & von Solms, 2005). In this scenario, employees may view security measures as an annoyance or an obstacle to their work and they may be less likely to comply with security policies or take the necessary precautions to protect confidential information (Sarkar, 2010). They may ignore security policies, find ways to bypass security constraints that are in place, use weak passwords, or be careless when handling confidential information (Chen, Shaw & Yang, 2006). These employees may also be more likely to fall for phishing scams or other types of social engineering attacks (Safa, von Solms & Futcher, 2016).

Therefore, it is crucial for organizations to foster a positive information security culture by promoting information security awareness and regularly educating employees about the importance of security (van Niekerk & von Solms, 2005). By creating an environment in which employees understand the impact of their actions on information security and the organization as a whole, organizations can build a stronger, more secure culture and reduce the risk of security breaches.

3 PROBLEM AREA

There has been a marked escalation in the frequency of accidental data breaches caused by insider threats in recent times (Cheng, Liu & Yao, 2017). In 2008, a contractor for the UK Home Office, working for the UK government, lost a USB stick with unencrypted data on all 84,000 prisoners in England and Wales, resulting in the termination of a contract worth £1.5 million (Sarkar, 2010). In 2011, a Texas State server published the personal data of 3.5 million citizens online for an entire year. In 2016, a staff member of the Australian Red Cross accidentally placed documents containing confidential information of over 550,000 blood donors onto an unsecured public-facing website directory on their website. These documents contained birth dates, sexual activity, drug use and medical histories of the blood donors (Cheng, Liu & Yao, 2017).

Alongside these accidental breaches, malicious insider threats have been increasingly reported (Cheng, Liu & Yao, 2017). In 2005, the UK's National Hi-Tech Crime Unit prevented the world's largest attempted bank fraud when thieves, disguised as cleaning staff, attempted to steal £220 million using keystroke loggers installed on computers at a London bank branch of a Japanese bank (Sarkar, 2010). In 2010, confidential documents of US diplomatic cables were leaked to WikiLeaks. This was orchestrated and executed by an insider entity. In 2013, an IT contractor for Vodafone Germany accessed the company's database system, resulting in the theft of personal information and bank account details of up to two million customers (Cheng, Liu & Yao, 2017). In the Capital One data breach in 2019, an insider stole over 100 million customer records, including 140,000 social security numbers and 80,000 linked bank details of customers (Mazzarolo & Jurcut, 2019).

These events highlight the damage that an insider can cause and the importance of protecting valuable and sensitive information and assets. They also highlight both the growing trend of cybercrime and the negligent actions of insiders within organizations.

Information resource protection largely relies on human cooperation. The human aspect is widely acknowledged as a weak aspect of information security (Metalidou et al., 2014; van Niekerk & von Solms, 2005). Insider threats and the human factor pose a significant danger to companies, institutions and organizations (Cheng, Liu & Yao, 2017). Whether intentional or unintentional, staff can cause significant damage to an organization through actions such as stealing intellectual property, sabotaging facilities or disclosing confidential information in various ways. Mainly, this is due to lack of awareness among staff and absence of an information security culture within the organization (van Niekerk & von Solms, 2005).

Although it is impossible to eliminate all risks, they can be reduced and residual risks can be controlled through a combination of administrative, technical and physical controls. Additionally, providing awareness training and ensuring readiness to respond to incidents can further help control these risks (Mazzarolo & Jurcut, 2019). However, this is not an easy task as many parts within an organization have an effect on the information security. Every organization has a diverse mix of intricate infrastructure, employees, consultants, management and partners with their own perspectives, values

and attitudes (Sarkar, 2010). To protect an organization's assets, information security best practices include a comprehensive security policy tailored to the organization, enforceable firm regulations, effective enforcement of these policies and good communication (Mazzarolo & Jurcut, 2019). Despite recognizing their significance however, many organizations still fail to develop information security policies and regulations (Paananen, Lapke & Siponen, 2020). The collected and reviewed literature shows a significant amount of research on information security within organizations, but there is a lack of studies on how this work has been conducted in government agencies.

3.1 Problem/Question

In accordance with the problems described, the aim of this study is to address the existing challenges in government agencies responsible for handling sensitive data by enhancing their information security practices and improving communication strategies. The study investigates how these agencies develop effective information security policies and regulations, as well as how they implement strategies to ensure employee compliance. Additionally, it investigates how these agencies disseminate rules and policies to their employees and explores the attitudes of employees towards complying with these regulations.

By gaining a deeper understanding of the development, communication and employee attitude aspects associated with information security, the study seeks to enable government agencies to improve their information security work, protect sensitive data more effectively, and enhance employee engagement in complying with regulations. To achieve this, this study will answer the following research questions.

1. How do government agencies work to develop information security policies and regulations?
2. How do these government agencies communicate information security policies and regulations to employees?
3. What are the attitudes of these government agencies' employees towards compliance with information security policies and regulations that they must adhere to?

The first question aims to investigate the processes that goes into developing information security policies, taking into consideration the overall attitude of the organization towards information security, what actors are included in the processes and how they make sure the policy adhere to international standards and regulations. The second question aims to investigate how these organizations work to communicate policies and regulations to staff in order to raise awareness and foster an information security culture within the organizations. The third question aims to explore the perception of staff towards communicated policies and regulations, their compliance with these policies, the impact of these policies on their daily work and how that affects their attitudes towards the policies and regulations. Furthermore, the question aims to identify challenges and barriers that these organizations face in ensuring employees' compliance to these policies and regulations.

3.2 Delimitations

This thesis will concentrate on government agencies in the public sector that handle sensitive data, such as personal or classified information. The study will not investigate private sector organizations or organizations in other industries. The focus on government agencies is crucial due to several factors. They manage highly sensitive data, and breaches can lead to severe consequences for both individuals and the nation (Alotaibi & Furnell, 2014). Maintaining public trust is essential for government agencies, and data security plays a critical role in this aspect. Studying these agencies can provide insights into protecting against cybersecurity threats and ensuring national security. It can also help improve information security standards across different sectors by setting an example for the private sector and other organizations (Herold, 2018). Government agencies must comply with strict regulations and legal requirements regarding information security (Kwon & Johnson, 2013). Analysing their work with policies can offer insights into best practices and compliance challenges.

Furthermore, government agencies often face different budgetary and resource constraints than private organizations (Heeks & Stanforth, 2007), making it valuable to investigate their information security policies and practices. Lastly, interagency collaboration can pose unique challenges in maintaining information security (Dawes, 2009). By studying these authorities, the study can explore the impact of collaboration on the development and enforcement of information security policies and regulations.

The study will also focus on the human factor and the insider threat and the method used will be qualitative interviews of top management or information security officers and regular employees. This thesis will therefore not evaluate technical security controls, but instead focus on human factors to show that protecting the organisation from insider threats, whether intentional or unintentional, can only be achieved if a holistic approach is taken.

3.3 Expected results

The expected result of this thesis is a better understanding of the processes and practices used by authorities in the public sector to develop and implement information security policies and regulations as well as the communication and compliance strategies used to ensure adherence to these policies. Additionally, the study aims to identify any challenges or barriers to compliance with information security policies and regulations and to provide recommendations for addressing these issues. The results of this study can contribute to the improvement of information security both in the public sector and the private sector, reducing the risk of data breaches, protecting sensitive information from unauthorized access, and overall improving information security within organizations. Considering the fact that government agencies often are seen as role models for the private sector in how information security work should be conducted (Herold, 2018), the findings of this study can serve as valuable insights and best practices for both sectors.

4 METHOD

This chapter provides an in-depth description of the methodology utilized in the research, including the purpose and process of conducting a literature review. It highlights the rationale for undertaking a comprehensive literature review and how it helped in shaping the research questions and objectives. The chapter goes on to outline the data collection methods employed in the study, including details about the participants, recruitment processes and the instruments used to gather data. Additionally, it presents an overview of the data analysis techniques employed to examine the data, drawing out key insights and findings. The ethical considerations taken into account during the research process are also discussed, highlighting the steps taken to ensure that the study was conducted in an ethical manner and that the participants' rights were safeguarded. Finally, the chapter outlines the measures undertaken to guarantee the validity and reliability of the research findings. It discusses various techniques used, such as triangulation and member checking, to ensure the credibility and dependability of the data and analysis.

4.1 Chosen Method

After formulating a suitable question for investigation, the next step is to select a suitable and structured approach. This is crucial for the project's success. In essence, the implementation of a systematic method is the essence of research. Research methodology refers to an organized approach to problem-solving that is carried out in a logical, orderly and systematic way. It involves a wide range of techniques and procedures that are used to gather and analyse data, test hypotheses and draw conclusions that can be evaluated by others (Berndtsson, Hansson, Olsson & Lundell, 2008). Research methodology is a critical aspect of any research study as it provides a framework for conducting the research and helps ensure that the results obtained are valid and reliable. In order to design a rigorous and effective research study, the research methodology need to be carefully considered and the methods chosen has to be appropriate for the research question. Some of the key elements of research methodology include research design, data collection and analysis, sampling techniques and ethical considerations (Patton, 2015). Research methodology helps ensure that the results obtained are valid, reliable and can be trusted. It is important to understand how and why each step of the methodology is carried out, as the nature of the problem guides the decision on which method to use. Determining the appropriate research method requires understanding the nature of the problem and the desired outcome of the study (Berndtsson et al., 2008).

There are several research methodologies for collecting and analysing data, including quantitative, qualitative and mixed methods (Askarzai & Unhelkar, 2017). Most methods share similar traits, such as the presence of a problem to be defined, goals to be accomplished and a phase of problem examination (Berndtsson et al., 2008). However, these methods have their strength and weaknesses and are better suited for certain research questions and goals (Askarzai & Unhelkar, 2017). It is important to carefully consider the research question, data and the intended outcome when choosing the appropriate method (Berndtsson et al., 2008).

The choice of methodology depends on the specific research question and the goals of the research study (Berndtsson et al., 2008). The purpose of this thesis is to gain knowledge on how government agencies, that handle sensitive data, work to develop information security policies and regulations and ensure compliance to them. Additionally, the study aims to gain knowledge on how these agencies communicate rules and policies to employees and what the attitudes of employees are towards compliance with information security policies and regulations. The central theme of this thesis is the human factor in information security and thus the objectives are achieved by exploring the experiences, behaviours, attitudes, beliefs and values of individuals and the personnel within an organization, ranging from top management down to the employees. Acquiring in-depth knowledge about these experiences is crucial in meeting the established objectives. Hence, it is believed that a qualitative approach is the most appropriate methodology for this study. Berndtsson et al. (2008) states that, unlike the quantitative methodology, qualitative methodology allows for a thorough collection of information through two-way communication between the respondent and the interviewer, which in this study is essential for achieving the set goals.

4.1.1 Chosen Data Collection Method

The method of conducting interviews can vary and serve various purposes. There are several styles of interviews in qualitative research (Berndtsson et al., 2008). These include open interviews (unstructured), closed interviews (pre-structured/structured) and semi-structured interviews (Baumbusch, 2010). When determining the suitable form of interview for the study, various factors must be taken into account. Different interview styles have unique advantages and disadvantages and these are closely associated with the researcher's ability to conduct interviews. If the researcher opts to utilize interviews, there are several aspects to consider in terms of preparation and implementation (Berndtsson et al., 2008).

Structured interviews are a way of conducting an interview where the interviewer follows a pre-determined questionnaire or protocol, asking the same set of questions in the same order to each participant and not allowing for any additions or deletions of questions. These interviews are good for studies that need precise data and the researcher has a clear understanding of the data that is required (Berndtsson et al., 2008). Semi-structured interviews are more flexible, allowing for follow-up questions and a more natural flow of conversation based on the participant's answers. These interviews are suitable for studies that require in-depth data and allow for the discovery of new insights (Baumbusch, 2010). Lastly, unstructured interviews are the least structured and allow the participant to lead the conversation, making them suitable for studies that aim to gain an understanding of a particular phenomenon (Berndtsson et al., 2008).

In this study, semi-structured interviews were selected. As the central theme of the study is to comprehend the underlying attitudes, beliefs and values that influence human behaviour and decision-making in the realm of information security, the semi-structured interview approach allows a more flexible and natural flow of conversation, while still guiding the conversation towards the central themes and objectives of the study. This approach enabled probing deeper into the participants' experiences, gather rich data and uncover new insights (Baumbusch, 2010), which aligns with the set goals.

4.1.2 Chosen Data Analysis Method

The data collected can be analysed using either a deductive or inductive approach. Qualitative deductive analysis involves evaluating the data collected in a study to determine if it supports pre-existing generalizations, explanations, theories, or results. In contrast, qualitative inductive analysis involves the creation of new concepts, explanations, theories or results from the specific data collected in the study (Patton, 2015).

In this study, the qualitative inductive analysis approach was used. The motivation for this is that the method allows generation of new and unique insights and understanding of the data collected. It allows identification of patterns and connections in the data that may not have been previously considered and development of new concepts, explanations, theories or results from the data. The method is particularly useful when studying complex or novel phenomena where pre-existing generalizations or theories may not fully capture the intricacies of the data (Patton, 2015), which is the case here. Furthermore, the inductive approach encourages a deeper exploration of the data, allowing for previously unseen connections and relationships to be uncovered and to gain a more comprehensive understanding of the data (Patton, 2015), which is the goal of this study.

There are several methods that can be used to conduct a qualitative inductive analysis, including grounded theory, thematic analysis, content analysis and more (Patton, 2015). In this study, the thematic analysis method is employed, which is a method for analysing and interpreting qualitative data to identify recurring themes or patterns. Thematic analysis is often used to explore the experiences and perspectives of study participants, uncover underlying patterns and relationships and provide significant insights. Unlike methods like content analysis, for example, which can be more structured and systematic, thematic analysis is typically a more inductive and flexible process that allows for identification of themes as they emerge from the data (Braun & Clarke, 2022).

4.2 Implementation of Study

The study was implemented in three main phases, literature review, data collection and analysis. First, a comprehensive literature review was conducted to provide a strong foundation for the research and to identify gaps in the field that need to be addressed. Next, the data collection process was initiated. Finally, the collected data was subjected to analysis.

4.2.1 Literature Review

A literature review can serve multiple purposes and can be utilized in different ways. It can stand alone as a comprehensive examination of previous studies and literature in a particular field. It can also serve as a preliminary stage in a larger research project, providing the foundation and context for the research to follow. Additionally, it can be a component of a finished research report, serving to summarize and synthesize previous findings and studies relevant to the topic being studied (Knopf, 2006).

In this study, the literature review served as a preliminary stage in the larger research project. The motivation for conducting it in this study was to address several key objectives in the preliminary stage. Firstly, it was conducted to identify a problem area in the field and establish the background context for the research. By reviewing previous research and studies, the aim was to identify any gaps in the existing literature, which could provide opportunities for new and original research. It also served to justify the research by demonstrating its significance and relevance, while helping to define the research question by providing insight into relevant questions in the field. Additionally, it aimed to avoid duplicating previous research and ensure that the study added new and valuable insights to the field. It played a crucial role in providing the foundation for the research and ensuring that it was well-informed, original and made a valuable contribution to the field. Finally, it aided in designing the interview guide, as the questions were based on the information gathered from the literature review.

In order to gather relevant literature for the study, a comprehensive search of academic journals and other sources was conducted using databases such as ACM Digital Library, Google Scholar, IEEE Xplore, Libris, LibSearch, SAGE Journals Online, ScienceDirect, SpringerLink and Taylor & Francis Online. The search process began with the use of broad search terms that are relevant to the study's context, such as "information security", "human factor" and "international standards." This was followed by a refinement of the search strategy to more closely align with the purpose of the study, utilizing more specific search terms such as "insider threats", "information security in government agencies", “information security policy compliance” and "information security awareness" to hone in on the specific areas of the problem. This iterative process of searching and refining was repeated until a sufficient number of relevant sources was located.

4.2.2 Interview Guide

Two interview guides were prepared prior to reaching out to the participants, based on the information gathered in the thesis background section. The questions were categorized into the three research questions that the thesis intends to answer. Participants holding top management positions and information security officers were expected to respond to all three research questions, whereas employees were expected to answer questions only related to research questions two and three.

For top management and information security officers, the interview guide comprised a total of 19 questions, with research question one consisting of four questions, research question two consisting of four questions and research question three consisting of nine questions. Two introductory questions were also asked regarding the respondents’ roles, responsibilities and for how long they have been working in their current role. The interview guide for employees contained a total of 17 questions, with research question two consisting of four questions and research question three consisting of 10 questions. The employees were also asked six introductory questions regarding their roles, responsibilities, for how long they have been working in their current role, their technical skills, their awareness of threats as well as policies and regulations and one question about their understanding of their organization’s policies and regulations.

The decision to prepare two separate interview guides, one for top management or information security officers and the other for employees, was based on the differing roles and responsibilities of these groups. Top management and information security officers are responsible for developing, implementing and communicating information security policies and regulations, while employees are responsible for adhering to these policies and regulations in their day-to-day work.

The interview questions in the guide for top management and information security officers focus on their experiences and expertise in developing policies and regulations, as their methods for communicating these rules and policies to employees as well as their perception of employees' compliance and adherence to these policies and regulations. In contrast, the interview questions in the guide for employees focus on their attitudes towards compliance with information security policies and regulations and their perception of how these rules and policies are communicated to them.

Another reason for preparing separate interview guides is that top management and information security officers may have more experience and knowledge in the development of policies and regulations. Therefore, their interview questions can delve into the details of how policies and regulations are created and implemented. On the other hand, employees can provide more insight into how these policies and regulations affect their work and how they, along with their co-workers, respond to them.

The interview questions in the guide for employees also allow them to share their experiences in adhering to information security policies and regulations. This information can provide valuable insight into the effectiveness of the policies and regulations in achieving their intended goals. Meanwhile, the interview questions in the guide for top management and information security officers can gather information on how to improve these policies and regulations to ensure better compliance and security.

4.2.3 Recruitment of Respondents

Before starting the interviews, a process of participant selection was conducted. The purpose was to identify individuals who were deemed suitable for the study, taking into account the research objectives and questions to be addressed. Participants were selected based on their ability to provide valuable insights into the research questions. For this reason, top management, information security officers and regular employees within different government agencies were included in the sample. The final sample consisted of ten participants, with two from top management, four information security officers and five regular employees being interviewed. The inclusion of top management and information security officers was intended to provide insight into the development and communication of information security policies and regulations. The regular employees were chosen to provide a perspective on the perception and attitudes towards these policies and regulations and their communication.

The initial contact with the participants was initiated through an email which was sent out to representatives of chosen government agencies. The email included a comprehensive description of the study's objectives. The description was based on the background research and aimed to provide a nuanced and brief explanation of the problem being addressed. The modalities of the interview process were presented as a

choice to the participants, with options for either in-person or online interviews through an online platform of their choice. Participants were informed that they had the right to cancel the interview at any point as well as the right to decline to answer a question, regardless of any reason they might have.

In addition, the email specified that the interviews would be recorded in audio format and that the interview would be transcribed and translated. The email further stated that the participants would be sent back the translated data for verification, to ensure that the data was an accurate representation of what was discussed in the interview. The email also stated that the collected data, after verification, would be used in the thesis and then permanently erased once the verification had been received. Furthermore, it was emphasized that no personal information, including information about the respondent or the organization they represent, would be collected.

Finally, the email provided the respondents with an outline of the questions that would be asked during the interview. These questions were categorized into the three central questions driving the research.

In total, 11 individuals were interviewed, six information security officers or top management and five regular employees. To maintain the confidentiality and anonymity of the respondents, their roles are not identified directly. Instead, codes are used to associate the descriptions with the respondents, such as “RM5” for respondent 5. The only differentiation that is made is between respondents from top-level management or information security officer positions and those who are regular employees. The purpose of this is to distinguish between the opinions of regular employees and those responsible for information security work, which is important in order to show the differences and similarities in opinions based on what role the respondent have. The code “RM” (Respondent Management) refers to top management or information security officers, whereas “RE” (Respondent Employee) refers to employees with no information security role.

Table 1 – *Respondents*

Respondent	**Interview time**
RM1	51 minutes, 39 seconds
RM2	47 minutes, 41 seconds
RM3	1 hour, 6 minutes, 41 seconds
RM4	45 minutes, 38 seconds
RM5	49 minutes, 29 seconds
RM6	28 minutes, 25 seconds
RE1	29 minutes, 20 seconds
RE2	25 minutes, 47 seconds
RE3	35 minutes, 15 seconds
RE4	41 minutes, 22 seconds
RE5	22 minutes, 50 seconds

4.2.4 Ethical Considerations

In today's society, research holds a prominent place and high expectations are placed on it. This places a significant responsibility on researchers to act with integrity in their work, not only towards the participants in their research, but also towards all those who may be impacted by their results, either directly or indirectly. Researchers are expected to conduct their work with the highest standards of quality, free from outside influence and manipulation and with a commitment to acting in the greater good rather than their own personal or stakeholder interests (Hermerén, 2017).

Researchers must have a strong understanding of the knowledge, methodologies and ethics in their field. Deviation from good research practices can have negative consequences, including damage to the research process, strained relationships between researchers, loss of trust, waste of resources and potential harm to research participants or the environment. Three main forms of research misconduct include deliberate fabrication, falsification and plagiarism, which all distort the research record. Other forms of violation in good research practices can also harm the integrity of the research process and harm the reputation of the researcher (ALLEA, 2017).

The obvious starting point for research ethics consideration is the individual protection requirement, which consists of four main requirements. These are the information requirement, the consent requirement, the confidentiality requirement and the utilization requirement (Swedish Research Council, 2002).

The information requirement states that the researcher is obligated to notify the participants involved in the research about its objective. They should also be made aware of the conditions associated with their involvement and that participation is optional and can be stopped at any time. The information relayed should also include all aspects of the current study that reasonably may affect the respondent’s willingness to participate. Additionally, they should be informed that the information collected during the study will only be used for the purpose of the research and not for any other purposes. The consent requirement states that the participants have the right to make an informed decision about their involvement in the research by being informed about its purpose. Additionally, the requirement states that the participants can stop their participation at any time without facing any negative consequences and must not be subjected to undue pressure or influence. The confidentiality requirement states that the confidentiality of all individuals involved in the study should be given the utmost priority and personal information should be stored in a secure manner to prevent unauthorized access. The utilization requirement states that the information gathered about individuals can only be utilized for research purposes and not for any other objectives (Swedish Research Council, 2002).

Due to the delicate nature of the study, it was essential to ensure that the collected data cannot be linked back to the participants or their associated organization in any way. To achieve this goal and ensure anonymity and confidentiality, several safety measures was implemented. No personal details about the participants or their associated organization was gathered. As a further precautionary measure, each participant was assigned a code to protect their identity and this code was used throughout the research process and reporting of the results to refer to the specific participant. To protect the collected data,

it was stored on a local password-protected computer and when the research was completed, all data was permanently erased.

4.2.5 Conduction of Semi-Structured Interviews

The interviews were conducted through online communication platforms such as Skype or Zoom, with the audio from the interviews being recorded. The interviews were recorded using the software OBS Studio. They lasted between 30 and 60 minutes. Before starting, the participants were informed of the conditions, including their right to cancel the interview at any time, the option to decline answering any question, the recording of the interview, the purpose of the study and the handling of the collected data. After obtaining their consent, the recording and interview began. The questions used in the interview were based on the interview guide provided to the participants via email prior to the interview. To create a relaxed atmosphere, the interviews were semi-structured, taking on a conversational tone. This approach allowed the participants to delve into additional topics they felt were relevant to the research while still ensuring the conversation was guided and kept focused on the primary subject matter.

During the conduct of these interviews, the aforementioned guidelines for ethical considerations, outlined by the Swedish Research Council (2002), were adhered to. To ensure compliance with the four requirements within the individual protection requirement, several precautions were taken.

To meet the information requirement outlined by the Swedish Research Council (2002), the participants were fully informed about the study from the outset. They received an email detailing the purpose of the study and the conditions on initial contact and this information was also provided before the start of the interviews. The consent requirement (Swedish Research Council, 2002) was met by advising the participants of their right to withdraw from the study at any time after being informed of the research purpose and they were asked if they still wanted to participate after being informed of the conditions. They were informed that they were under no obligation to answer any question, regardless of any reason they might have. To ensure confidentiality, all collected data was stored on a local password-protected computer with limited access. No personal or organizational identifying information was recorded or collected during the study. The collected data was permanently deleted after the conclusion of the research and the participants were informed of these measures on initial contact and before the interviews. Finally, to meet the utilization requirement (Swedish Resource Council, 2002), the participants were informed of the intended use of the information collected, both on initial contact and before the interviews and they were assured that the information would only be used for research purposes.

Following the completion of the interviews, the audio recordings were transcribed and then translated from Swedish to English. To ensure accuracy, the translated data was sent back to the participants for verification to confirm that it accurately reflected what was said by the participant in the interview. Upon receiving verification, the process of compiling and analysing the data was initiated.

4.2.6 Conduction of Data Analysis

The first step in the thematic analysis process is to familiarize with the data collected from the interviews (Braun & Clarke, 2022). This was done by reading through the transcripts of the interviews several times, taking notes and marking significant statements, quotes and insights. The transcripts were thoroughly reviewed and re-read multiple times to get a deep understanding of the content. After reviewing the transcripts, codes were assigned to themes that emerged in the data. These codes were used to categorize the data into meaningful themes. The coding process was done manually and involved highlighting and labelling specific segments of text that were relevant to each theme. Each theme was highlighted in a different colour. The selection of the appropriate tool for analysing the collected material was narrowed down to two options, Microsoft Word and Adobe Acrobat Reader. Ultimately, Adobe Acrobat Reader was preferred over Microsoft Word due to its user-friendly features that allow for seamless navigation between multiple documents and effortless navigation to comments via a panel positioned on the right side of the screen.

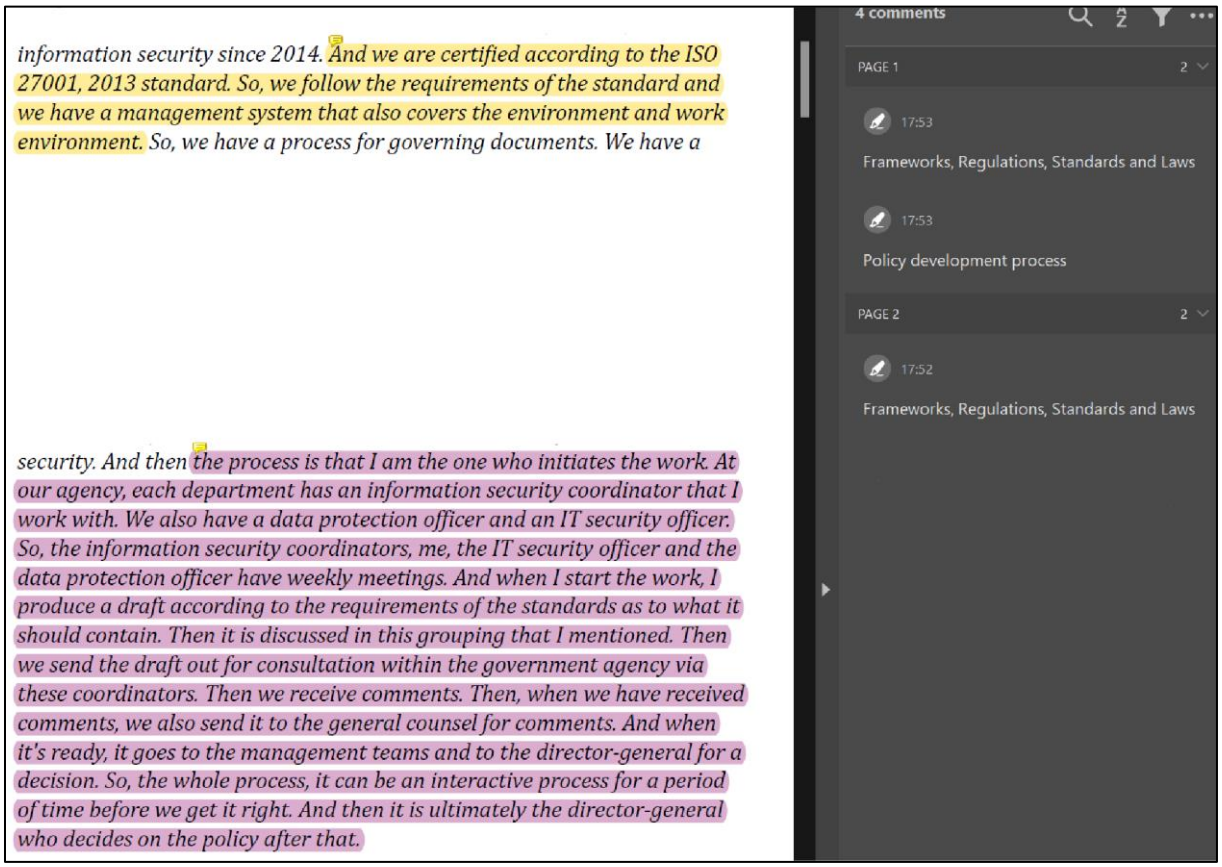

Figure 1 *– Encoding material in Adobe Acrobat Reader*

To ensure easy identification of the themes for the marked data, a colour was assigned to each segment based on a theme-specific colour code. Specifically, the first letter of the coded theme was used to select a corresponding colour. For example, the colour purple was assigned to the theme "policy development process" as both the theme and the colour start with the letter 'p'. This method was adopted to enable quick identification of the theme associated with each segment of data.

The coding process began by breaking down the transcripts into smaller segments and identifying meaningful and relevant themes that emerged from the data. These segments were coded and similar codes were grouped into broader themes. Once the themes had been identified, they were analysed in more detail in order to gain a deeper understanding of the attitudes and perspectives of the participants. This involved looking for patterns and connections between the themes, as well as identifying any discrepancies or outliers that might provide insights into the attitudes and perspectives of the participants. The themes were then grouped together into categories that aligned with the research questions. For the first research question, themes related to how the government agencies work to develop information security policies and regulations were grouped together. For the second research question, themes related to how these agencies communicate the policies and regulations to their employees were grouped together. And for the last research question, themes related to the attitudes of employees towards the policies and regulations were grouped together.

Consideration was taken into removing bias and maintaining credibility of the findings by ensuring that the data was analysed objectively, without making assumptions or preconceptions about the participants or their attitudes. To achieve this, efforts were made to remove any personal bias from the coding and analysis process. This involved continuously reviewing and reflecting on the codes and themes, seeking feedback from fellow students and critical friends and striving to maintain an open-minded and objective perspective.

After the initial coding and theme development, the data was reviewed again to ensure that all relevant themes were captured and accurately represented. This involved comparing and contrasting the themes with the original data and making necessary adjustments to the themes and codes. Finally, the themes and codes were reviewed one last time to verify that they accurately reflected the research questions and provided meaningful answers. This involved a critical evaluation of the themes, codes and data to ensure that they were not oversimplified or misinterpreted and that the findings were robust and reliable.

Overall, the thematic analysis process involved a systematic and rigorous examination of the data in order to identify the themes and patterns that emerged and to gain a deeper understanding of the attitudes and perspectives of the participants. The process was conducted in a methodical and objective manner, with a focus on removing bias and ensuring the validity and reliability of the findings while still accurately answering the research questions.

Table 2 – *Identified Themes*

Identified Themes	
How do government agencies work to develop information security policies and regulations?	*Reasons for Policy and Regulations Development* *Frameworks, Standards and Regulations* *Involvement of Stakeholders* *Human Factor and Insider Threats* *Essential Steps*
How do these government agencies communicate information security policies and regulations to employees?	*Intranet* *Education and Training* *Information Security Coordinators* *Effectiveness* *Improvements*
What are the attitudes of these government agencies' employees towards compliance with information security policies and regulations that they must adhere to?	*General Attitude* *Awareness* *Culture* *Ensuring Compliance* *Challenges in Ensuring Compliance* *Incidents* *Incident Management* *Human Factor and Insider Threats* *Improvements*

4.2.7 Validity and Reliability

Another aspect that needed to be taken into account was the validity and reliability of the research. When studying a problem, the researcher's prior experiences, values and beliefs affect the way the research question is viewed, analysed and reported. To ensure trustworthy results that are independent of personal experiences, research methods are used to address potential threats to validity. It is important to be aware of these threats, as well as the variations in handling them, as they can impact the application of the chosen research method in the project (Berndtsson et al., 2008).

Validity refers to the relationship between what the researcher intends to measure and what is actually measured (Berndtsson et al., 2008) and can be categorized into two categories, internal validity and external validity (Merriam, 1995). Reliability refers to the accuracy and robustness of the research method used. A method can only be considered valid and reliable within a certain range of uses. There are two main threats to validity in qualitative research, the researcher's own biases and the influence of the setting on the research. To address these threats, the researcher should acknowledge their own biases and account for them in the analysis of the findings and be aware of any changes in the setting that may occur during the research. In order to ensure the overall quality of the research project, it is important to consider these threats and address them appropriately (Berndtsson et al., 2008).

Internal validity in research is concerned with the accuracy of observations and measurements made. It is a crucial aspect in both positivist and qualitative research,

with the latter viewing reality as a constantly evolving concept. Strategies to ensure strong internal validity in qualitative research include triangulation, member checks, clear statement of researcher's experiences, assumptions and biases and immersion in the research situation. Reliability in research is concerned with the repeatability of findings. In the natural sciences, it is determined through repeated measurements of a phenomenon using objective methods. However, in social sciences, the study of human behaviour makes it difficult to rely on repeated measures. In qualitative research, the focus is on dependability and consistency, which can be achieved through triangulation, peer examination and audit trails. External validity, also known as generalizability, refers to the ability to apply the findings of a study to other situations. In qualitative research, it is a challenge due to the absence of statistical extrapolation from a sample to a population. Alternative views of generalizability in qualitative research include working hypotheses, concrete universals and reader or user generalizability. Strategies to strengthen the external validity of qualitative research include thick description, multi-site designs, modal comparison, and sampling within (Merriam, 1995).

To ensure the validity of the study, both internal and external validity were considered throughout the research process. In order to achieve this, several concepts were integrated into the study design, including within-sampling, thick descriptions, triangulation, member checking, peer review, collecting rich and detailed data, and reflexivity. Within-sampling was executed by selecting a diverse group of participants from different work roles within the target organizations, providing a comprehensive understanding of information security practices. Thick descriptions were used to provide sufficient information for readers to assess the relevance of the study to their own experiences. To minimize researcher bias, member checking was employed, which involved returning the gathered data to the participants for review and confirmation. The use of multiple sources and methods of data collection, including a literature review and qualitative interviews, served as a means of triangulation. The peer review process was implemented through regular assessments of the study by fellow students and a designated critical friend. Rich and detailed data was obtained through in-depth interviews to enhance both the validity and reliability of the study. The application of reflexivity was achieved through a combination of self-reflection, triangulation and the utilization of multiple research methods such as a literature review and qualitative interviews.

To ensure reliability, an audit trail was also implemented. The audit trail provides a comprehensive record of all actions taken during the study, allowing other researchers to replicate the study and confirm the results, thus ensuring repeatability.

5 ANALYSIS

This chapter presents the analysis of the data collected from the interviews that were conducted with the 11 individuals, including six top-level management or information security officers and five employees without any information security roles. The top-level management or information security officers included a unit manager, a business developer currently acting as an interim information security officer, two information security officers, a chief information security officer (CISO) or information security coordinator, and an information security strategist. The employee respondents consisted of one team coordinator and four caseworkers. The gathered materials have been classified according to the factors and research questions outlined in the background chapter. Themes that correspond to each category are then presented.

The material presented incorporate, at relevant points, direct quotes from the respondents, except for data gathered from RM1, who explicitly requested to not be directly quoted in the thesis. Furthermore, certain words from the quotes have been excluded to avoid identifying the participant or the organization they represent. The identifying words that are removed have been replaced with "[identifying]". If any parts are excluded for other reasons, the explanation will be provided in the same format, using another descriptive word to indicate the reason, such as "[irrelevant]".

5.1 Development of Information Security Policies and Regulations

The participants are first asked introductory questions about their roles and experiences. After the introductory questions, the interview continues with four questions about the development of information security policies and regulations. These questions cover the processes followed by government agencies, the individuals involved, the impact of human behaviour, insider threats and recommended essential steps to be taken. These questions, regarding the development of policies and regulations, were only asked to top management or information security officers and not to the regular employees.

5.1.1 Reasons for Policy and Regulations Development

Policy development begins when an issue arises that necessitates the creation or modification of a policy (Ismail et al., 2022). The process of evaluating a policy involves four sub-steps, collectively known as the policy assessment process. These include examining the policy environment, identifying any gaps or inconsistencies in the policy, summarizing the results of the policy assessment, and developing recommendations for policy improvement. Following these steps, a decision can be made on whether to approve proposed changes and an assessment can be conducted to determine the potential impact on existing policies (Rees, Bandyopadhyay & Spafford, 2003).

RM5 explains that the need for a new policy or regulation often arises due to a new regulatory framework or identified gaps in their information security work. Incidents can also trigger the process of developing procedures to avoid similar occurrences in the future. The approach is scenario-based and can include an independent internal audit to identify and recommend new regulations. RM4 notes that their certification requires the

development of policies, and that they have recently created a policy for information security RM3 cites an example of a challenge they faced during the COVID-19 pandemic which led to them conducting an assessment that resulted in the creation of a policy for online communication.

Similar to the findings of Ismail et al. (2022), the respondents highlight that the need for development of policies is heavily scenario-based and is influenced by their internal events and organizational environment.

5.1.2 Frameworks, Standards and Regulations

Höne and Eloff (2002b) emphasize the importance of taking into account industry standards, best practices, and legal and regulatory requirements when developing policies and regulations. This sentiment is echoed by the respondents, who discuss the significance of adhering to standards, frameworks, regulations, and laws set by the government and other agencies. While their responses have minor differences, they fundamentally align with Höne and Eloff's statement. They emphasize the importance of compliance with data protection laws, archive legislation, and security protection legislation, as well as guidelines from the Swedish Civil Contingencies Agency (MSB). These guidelines are crucial to the policy and regulation development processes carried out by the authorities represented by the respondents.

RM1 states that their organization follows government procedures and external authorities, adhering to laws, regulations, and guidelines provided by these entities. For information security, they rely on MSB guidelines, which are based on the ISO 27000 (ISO, 2018) package. These guidelines govern various aspects of their work, including structure, information handling processes, documentation practices, and distribution of responsibilities. RM2 shares a similar perspective but also includes additional legislations that their organization must follow when creating policies and regulations, such as the security protection legislation, archive legislation, data protection, and ISO:

> *"[...] it's based on the requirements that the government imposes on us as a government agency. Then there are the MSB's regulations, the security protection legislation, the archive legislation, data protection, and of course ISO in this too. Based on the regulatory requirements for the authority, the policies and regulations are drawn up."* – RM2

Although RM3 does not explicitly mention using MSB's guidelines, they underscore the importance of considering the ISO 27001 (ISO, 2013) and 27002 (ISO, 2022) packages. They also mention utilizing the PDCA (Plan, Do, Check, Act) cycle framework in their work, including policy and regulation development:

> *"[...] we have a traditional Plan, Do, Check, Act (PDCA) cycle. We follow it for much of our work. Even when we make policies and regulations around this."* – RM3

RM4 highlights the necessity of complying with MSB's regulations, particularly the 2020:6 (MSBFS 2020:6) and 2020:7 (MSBFS 2020:7) regulations, which align with the ISO standard. They also reference ISO 27001 (ISO, 2013) and 27002 (ISO, 2022)

packages for information security, ISO 14001 (ISO, 2004) for environmental management systems, and regulations established by the Swedish Work Environment Authority. RM4's management system also dictates their use of the PDCA cycle framework.

RM5 cites the GDPR, the Security Protection Act (SFS 2018:585), and the Public Access to Information and Secrecy Act (OSL) (SFS 2009:400) as regulations they must follow:

> *"The authority works to establish systematic information security work in all respects, the ISO 27000 series is used and put in relation to regulations such as GDPR, the Security Protection Act, OSL, etc. Much of an authority's information security work is highly regulated by various types of regulations."* – RM5

RM6 mentions working according to the methodological support from MSB. Interviews reveal that while MSB's guidelines are heavily based on the ISO standard and followed by government agencies, at least two agencies are not ISO certified. RM1 and RM5 share the view that ISO certification is unnecessary and excessively expensive compared to its benefits. Only RM4 explicitly states their organization is ISO certified. It is unclear whether the remaining three agencies that are interviewed have been certified by ISO, as this information is not disclosed. According to Höne and Eloff (2002a), standards like ISO provide instructions and mandates for crafting effective policies. This is primarily how these government agencies utilize them according to the statements that are being provided. As per Lopes, Guarda and Oliveira (2019), standards like ISO lack legal force and do not impose penalties for non-compliance. In these cases, the government agencies are subject to regulations and standards established by the MSB, which are derived from the ISO standard and do impose penalties for non-compliance. This indicates that, while ISO standards themselves do not have penalties for non-compliance, MSB's standards and regulations do.

5.1.3 Involvement of Stakeholders

According to Paananen, Lapke and Siponen (2020), it is crucial to engage with stakeholders to collect their feedback on security requirements and priorities, comprehend their perspectives and needs, and guarantee that their opinions are considered during policy development. This approach can enhance stakeholder commitment and encourage them to support the policy post-implementation. Policy reviews and approval is another crucial step in the process. Key stakeholders, including executives, legal counsel and information security personnel, should review and approve the policy to ensure that it meets the organization's needs and requirements, as well as relevant standards, laws and regulations (Flowerday & Tuyikeze, 2016; Knapp et al., 2009).

RM2 states that policy documents are prepared by a network of professionals such as lawyers, information security coordinators, and data protection experts. These departments work together to create the documents, which are then sent up to the highest decision maker for review and decision. The IT department plays a crucial role in implementing and adapting these policies. The preparation of these documents is an

ongoing process, and the national network ensures that they are constantly updated and adapted.

RM3 states that their policies are written by the security function, which consists of a group of four developers. The policy is then sent out for review to different parts of the organization. RM4 describes a similar process in their organization, where it begins with RM4 initiating the work and producing a draft based on the requirements of the standards. RM4 then discusses the draft with the organization's information security coordinators, IT security officer, and data protection officer in weekly meetings. The draft is then sent out for consultation within the agency, and comments are received from various stakeholders. The draft is also sent to the general counsel for their input. Once the draft is finalized, it goes to the management teams and the director-general for review and a decision. RM4 notes that the process can be an interactive one that takes time to get right, and the final decision on the policy is made by the director-general. Similarly, the organization that RM5 represents involve specialists, the business that the policy or regulation will cover, managers and other decision makers in the process:

> *"Specialists who know security issues, that is specialists in legislation. Also, the business that the regulation will cover. And managers and other decision makers who will approve the policy or regulation."* – RM5

RM6 states that a large number of people are involved in information security in their organization. These include lawyers who specialize in specific types of legislation such as public access, confidentiality, and data protection. Additionally, the head of security, archivists, IT department, administrative organization, controllers, management, and the communication department are all involved. RM6 emphasizes that information security is an organizational issue that cuts across the entire organization and requires collaboration from all departments.

Both the literature and the statements from the respondents emphasize the importance of engaging with stakeholders during the development of security policies. Paananen, Lapke, and Siponen (2020) highlight the necessity of collecting stakeholder feedback, understanding their perspectives, and ensuring their opinions are considered throughout the policy development process. Similarly, RM2, RM3, RM4, RM5, and RM6 describe the involvement of various stakeholders, including legal counsel, information security coordinators, data protection experts, and management, in the creation and review processes of their information security policies and regulations. Key stakeholders, as noted by Flowerday & Tuyikeze (2016) and Knapp et al. (2009), should review and approve the policy to ensure its alignment with organizational needs, legal requirements, and relevant standards. This process is also evident in the statements provided by the respondents and includes policy review and approval by an independent party, usually consisting of key stakeholders. In these cases, the independent party is not outside the organization, but they are an independent party in the sense that they were not involved in drafting the policy. According to Howard (2003), having an independent party or group assess the policy document has several benefits, including the development of a sounder policy through scrutiny from different perspectives, increased support from a wider range of stakeholders and improved credibility through input from specialist reviewers. Although it is evident that these respondents' organizations use

independent parties to review the policies and regulations, they do not mention the benefits of it.

5.1.4 The Human Factor and Insider Threats

The participants are asked how they address the human factor and insider threats when developing information security policies and regulations. The common consensus is that this is not done with policies, but rather through other means such as culture building, incident management, education, training, governance and guidance.

RM1 states that in their organization it is not achieved with policies, but through culture building. A few years back they used to have an approach to information security similar to that of "police officers" where employees were punished for making mistakes. Staff responsible for information security would only deliver negative messages and solely inform employees of their wrongdoings. This led to incidents not being reported out of fear for repercussions and in other ways hindered employees in their daily work. However, RM1's organization have since shifted their focus towards being helpers and supporters instead. This change has proven to be better and more efficient according to RM1, who further notes that many colleagues in the field are making the same transition.

RM2 shares a similar sentiment and states they work towards having an open climate and dealing with it through training. They emphasize the importance of a non-judgmental culture that views mistakes as opportunities for learning rather than opportunities for punishment. Mistakes should instead be handled in a way that contributes to growth and development for the organization

> *"Well, we do a lot of training and we put a lot of effort into having an open climate. It is like, well, making mistakes is nothing, it's also a way for us. So, we can learn from mistakes. So, it is a very, what can I say, non-judgmental culture and it's very important for safety work that it is like that, so to speak."* – RM2

RM3 states that policies have limitations when it comes to dealing with the human factor. They can write rules on what is allowed and what is not, but it is not enough. However, policies are essential in ensuring that the organization communicates clearly and consistently with its employees. To support policies, the organization produces guiding or supporting documents that are communicated in an easily understandable way and they provide training courses that support these documents. RM3 gives an example of how the organization had to tackle the issue of holding sensitive meetings during the pandemic, which led to the development of a policy that specified what types of information.

RM4 highlights that their organization have policies and procedures in place for information classification, security measures and risks, as well as guidance for handling information belonging to any class. RM4 further states that incidents and mistakes still happen despite these measures. In such cases, they have a procedure for incident management and reporting, which involves reporting the incident to a group that analyses it based on its type. The information owners and the department where the incident occurred then propose measures to address the issue and to prevent it from

happening again. RM4 also emphasizes the importance of learning from incidents to avoid similar mistakes in the future. To keep track of incidents, they receive quarterly reports that detail the type of incident, such as personal data incidents, system breakdowns or security breaches. RM4 then reports the incidents to management and other authorities, such as the Swedish Authority for Privacy Protection (IMY) and MSB, if necessary. Finally, RM4 states that the information security coordinators within these departments are responsible for ensuring that employees are aware of the procedures and policies related to information security. They work within the departments to anchor the policies and procedures and to remind employees about them. In addition to training initiatives, the aforementioned incident management procedures govern how incidents are reported. Although not all incidents are reported, RM4 notes that more and more people are reporting incidents that have occurred.

RM5 takes a different approach to the question and claims that the human factor is something that is handled through the use of technology. RM5 also makes a differentiation between intentional and unintentional threats and how they are handled. According to RM5, insider threats can arise from deliberate violations of rules as well as unintentional negligence, and dealing with each type of threat requires different tools. If the threat is unintentional, culture and guidelines are used to prevent and manage it, whereas intentional threats, such as unauthorized behaviour and deliberate risk-taking actions are handled with certain tools such as log management and other types of follow-ups. They also have an internal investigation that deals with incidents. RM5 further mentions that proactive work is important and is something they do, where background checks and verification of qualifications during the recruitment process is conducted. Additionally, RM5 notes that designing working methods in the organization also helps manage unintentional mistakes by building IT systems that make it difficult to make mistakes and easy to do the right thing.

RM6 instead mentions responsibilities within the organization and emphasizes that everyone has their own responsibility to know the internal governance and the laws and regulations that govern the business overall. The organization stresses the importance of keeping oneself updated and each level up the managerial ladder has a regular line responsibility to ensure that issues are dealt with. While their laws may not focus on the human factor, the internal governance of the organization emphasizes that employees must take responsibility for handling the authority's information correctly and in compliance with the governance in place. Van Niekerk and von Solms (2005) state that each individual in an organization must understand their specific role and responsibilities in maintaining information security, as well as the impact of their actions on the overall security of the organization, which falls in line with the statement from RM6:

> *"There is a rule that everyone has their own responsibility. Everyone has their own responsibility to know which... partly our internal governance, but also the laws and regulations that govern the business overall. So, it's something that we emphasize, that it's everyone's responsibility to keep themselves updated. But then at each level up there, like at the managerial level and so on, there is a regular line responsibility, that the manager is responsible for his or her activities. So, you have a slightly greater responsibility to ensure that the issues are dealt with."* – RM6

The literature highlights the human factor as the weakest link in information security and emphasizes the importance of a holistic approach that encompasses technology, processes, people, and organizational factors (Georgiadou, Mouzakitis & Askounis, 2022; Metalidou et al., 2014; Baker & Wallace, 2007). In line with this, respondents similarly recognize that addressing the human factor and insider threats cannot be solely achieved through policies, but also through culture building, incident management, education, training, governance, and guidance. By fostering an open and non-judgmental culture, providing clear guidance and procedures, managing and reporting incidents, and emphasizing individual responsibility, the participants' strategies align with the literature's call for a holistic approach to address the human factor and insider threats in information security (Tu & Yuan, 2014; Van Niekerk & von Solms, 2005).

5.1.5 Essential Steps

The participants are asked what they think are the most important steps to consider when developing policies and regulations. According to Paananen, Lapke and Siponen (2020), there is no established method or definitive guide for developing information security policies and regulations. Therefore, it is crucial for organizations to prioritize tailoring policies and regulations to fit their unique needs. However, authors Flowerday and Tuyikeze (2016), Ismail et al. (2017) and Knapp et al. (2009) agree on a set of essential steps that should be incorporated into the policy development process. These steps include conducting a risk assessment, identifying stakeholders, setting security objectives, developing, reviewing, implementing, maintaining, and updating the policy. There is a shared consensus among these authors on what should be included in an information security policy, specifically scope, roles, responsibilities, and security controls. RM2, RM3, RM4 and RM6 all mention some of these steps and content that they implement in their policies and in their development processes.

RM2 starts by emphasizing the importance of having a basic knowledge of the business and its environment when developing information security policies and regulations. They highlight that different types of organizations have different requirements, and that it is important to adapt the policy to fit the unique needs of the business, which is in line with the view of Paananen, Lapke and Siponen (2020). Additionally, the respondent stresses the importance of creating a policy that can be implemented in practice and is not just a document that sits on a shelf. The policy should be something that everyone in the organization can relate to and adhere to.

RM3 acknowledges that there is no right and wrong, but mention several factors that are important, such as ensuring the scope, sticking to accepted definitions, adhering to constitutional requirements, standards and directions, setting goals, ensuring top management's commitment, and defining roles and responsibilities:

> *"There is no right and wrong here, it's more about how you think you can ensure that you cover everyone."* – RM3

RM4 mentions that developing policies and procedures that are relevant, simple, understandable and easily accessible for those who are going to use them is crucial. RM5 mentions that there is no set process model, but rather a set of guidelines and practices that are typically followed:

> *"There is no process model or equivalent for the procedure, but there is a guideline, checklists and a practice or whatever you want to call it for what is usually done."* – RM5

RM5 further states that when developing information security policies and regulations, the actual implementation, anchoring, and communication are often the challenges, particularly in a large organization with many employees. RM5 continues with noting that it is crucial to have a communication strategy and to take help from business developers. Additionally, there should be a security role that sits far out in the organization, such as an ambassador, with whom there can be regular communication. RM5 further acknowledges that implementation, communication, follow-up, setting security goals, and determining security controls are all crucial aspects of developing effective policies and regulations. However, setting effective security objectives can be complicated, and it is often neglected or left as the last priority.

RM6 states that identifying stakeholders to obtain broad support is crucial when developing information security policies and regulations. This includes considering issues beyond just information security and identifying those who are affected by management policies. Additionally, RM6 emphasizes the importance of implementing policies beyond just having them on paper and integrating them into daily operations:

The varying answers and opinions provided by the respondents align with the findings of Paananen, Lapke, and Siponen (2020), who suggest that there is no universally accepted method or definitive guide on how to approach the topic. RM3 and RM5 explicitly mention this by stating that there is no right or wrong way, but rather that there are guidelines for how it is usually done and that the focus should be on how to ensure that the work is inclusive of everyone in the organization. The respondents' responses are also consistent with the recommendations of Flowerday and Tuyikeze (2016), Ismail et al. (2017), and Knapp et al. (2019) regarding the critical steps involved in developing an information security policy and the essential components that a policy should contain.

5.2 Communication of Information Security Policies and Regulations

According to Höne and Eloff (2002b), an effective information security policy is dependent on the users knowing about it. The policy should be disseminated across the entire organization in a manner that fits with the organization's traditional methods and can be reinforced through training and awareness sessions with top management support. The participants were asked questions regarding their views on the communication of information security policies and regulations. These questions were asked to both top management and information security officers as well as to regular employees.

5.2.1 Intranet

All participants, both from top management and information security officers as well as the regular employees, mention their intranet as a means of communication. This indicates that the intranet is one of the most common and primary means of communication within the organizations. Management speaks of the intranet as a tool to publish news, changes, policies, and procedures and employees also use the intranet to

access this information. This shows that the intranet is a central channel for information dissemination within the organization.

The use of the intranet as a communication channel is supported by Höne and Eloff (2002b), in the sense that they suggest that conventional communication methods should be used to communicate policies and regulations within an organization. This makes the approach of using the intranet logical since employees use the intranet for extended periods in their work and it is a platform that everyone in the organization can access. By using the intranet, the organization ensures that everyone has access to the same information and that it is communicated through a platform that employees are familiar with. The fact that both management and employees use the intranet for communication purposes also suggests that it is an effective method of communication. The intranet provides a centralized location for policies and regulations, making it easier for employees to access them. The intranet can also be updated in real-time, further ensuring that employees have access to the latest information through notifications and newsletters that are published on it.

5.2.2 Education and Training

Höne and Eloff (2002b) emphasise that, while policies and regulations should be communicated through conventional methods, they also need to be reinforced with training and awareness sessions. Sarkar (2010) states that every organization should have a comprehensive security awareness program where all employees undergo periodic training, with additional smaller briefings as needed. According to Tu and Yuan (2014), such training can lead to increasing the knowledge and involvement in security efforts by employees. All respondents indicate that there is a big focus on training and education, where regular and role-specific training is something that these organizations do extensively. RM1 state that they provide training courses for its employees to learn how to do their job effectively, including more specific and targeted training courses aimed at different types of groups. The employees are divided into different groups to increase competencies and handle sensitive cases, with additional special training provided to certain groups for specific areas such as handling sensitive personal data. RM1 recognizes the importance of both practical everyday help and specialized training in educating and training their employees.

RM2 discusses the training packages offered by the organization. They mention that the organization produces their own films about various topics, and these films are made by staff members, which makes them relatable and effective. RM2 further explains that the organization creates their own educational material for information security, data protection, and security protection. The organization offers a variety of training courses that vary in length, from short courses that take five to ten minutes to more solid courses that take upwards of an hour or more. RM2 emphasizes the importance of having different types of training available to employees, as not all employees will respond to the same type of training.

RM4 explains that they have several training programs to raise awareness about information security and safety in their organization. They have developed PowerPoint-presentations for new employees, mandatory training through the DISA training portal, and workplace meeting materials. They also have a presentation about their

management system for information security. The organization is considering a systematic approach to refresh and remind employees about safety issues and management systems, possibly through workplace meetings or departmental coffee breaks:

> *"We have these PowerPoint presentations that the information security coordinators and we have jointly developed, which is, so to speak, an introduction where they sit down with the new employee and go through the basics. Then we have the mandatory training DISA, which is a special training and which is in our training portal that is mandatory for everyone to go through. Then we have also had workplace meeting material on safety work to raise awareness of safety in general."* – RM4

RM5 states that they have an introductory training package for new employees, which includes a predetermined part that all employees receive and a customized part based on the specific role of the employee. RM5's organization also organize theme days and conference days on topics that are relevant to the current security challenges faced by the organization, which is often influenced by what the government and media are discussing. RM6 further continues on the same track as the other respondents and mentions that they provide general training courses for all employees, as well as targeted training for specific employees who work with certain issues or have specific roles and responsibilities.

RE1 state that employees' training start during their first week on the job and includes handling sensitive as well as confidential data, communication protocols, and confidentiality requirements. The basic training lasts for six months, and before starting any tasks, employees must complete it. RE1 continues with reporting that they are happy with the basic training and that it is good. The training is well-structured, starting with the basics and gradually increasing in complexity. The training courses are designed to be taken over time, and after six months, more advanced courses can be taken for those who wish to become experts in the field. Some employees may require advanced training due to the sensitive nature of their work:

> *"The basic training you get at the beginning, the first week you start working, was great. It was very clear and the actual training part is very well structured. It kind of increases gradually. You start with the basics and then you increase your knowledge."* – RE1

RE2, RE3, RE4 and RE5, like RE1, confirm that they have undergone extensive training related to information security and compliance. The training usually starts with an introductory course, which is followed by regular training on specific topics or as new threats emerge. They find that the training is generally clear and effective in building a culture of security and compliance. This supports the findings Sarkar (2010), and Höne and Eloff (2002b) on the benefits of training in building a culture of security and compliance.

All respondents indicate a significant focus on training and education, highlighting regular and role-specific training in their organizations. This is in line with Sarkar's

(2010) findings, which stresses the need for comprehensive security awareness programs, periodic training, and additional briefings as needed. Tu and Yuan (2014) highlight the potential for increased knowledge and employee involvement in security efforts as a result of such training. RM1, RM2, and RM6 discuss the provision of targeted training courses for different types of groups within their organizations, which aligns with Sarkar (2010)'s recommendations. Similarly, RM4 and RM5 mention introductory training packages for new employees and theme days on relevant security challenges, respectively, which is consistent with the literature's emphasis on ongoing training and awareness-raising (Höne & Eloff, 2002b; Tu & Yuan, 2014).

5.2.3 Information Security Coordinators

All respondents notes that departmental information security coordinators are used to communicate information security policies and regulations. RM3 explains that the coordinators are responsible for communicating new guidelines or policies to employees through various channels, such as departmental meetings or emails. RM4 adds that the coordinators also provide training to new employees and ensure that all employees are aware of the organization's management system for information security. They are also responsible for reminding employees of the policies and procedures and making sure they know where to find them. RE4 mentions that they receive information on changes or new threats through workplace meetings with the coordinators, emphasizing that utilizing information security coordinators is effective in informing employees. The use of departmental information security coordinators is not explicitly mentioned in the literature, but plays an important role in communicating information security policies and regulations according to the respondents.

5.2.4 Theme Days

RM3, RM4 and RM5 mention theme days as a way of reaching out, where the organizations have specific days or periods where more emphasis is put on cyber- and information security. RM3, RM5, RE2 and RE4 mention the Information Security Month. The Information Security Month is an annual campaign held in October with the aim of raising awareness and skills in information and cyber security among individuals and companies. It is carried out by the Swedish MSB and the police, with the participation of partners from private, public and non-profit sectors. The campaign is part of the effort to increase the minimum level of information and cyber security in society. October is also the European Cyber Security Month, organized by ENISA, with the same goal of raising awareness of information and cyber security among the public and organizations (Swedish Civil Contingencies Agency [MSB], 2022b). The information security month is something that RM3, RM5, RE2 and RE4's organizations participate in. Theme days and specific days as a means to communicate and reach out to employees is also not mentioned in the literature, but is something that is done in these organizations.

5.2.5 Effectiveness

Höne and Eloff (2002b) claim that an information security policy is considered effective when the content communicates to users the expectations for handling information in a clear and easily understood manner. But although the content is important, the way it is communicated and presented to the users is crucial. Each respondent asserts that they

do not specifically measure the efficacy of their communication channels. Instead, they rely on follow-ups and assessments to gauge effectiveness.

RM1 and RM4 note that completion rates of their training campaigns provide an indication of efficacy, although they clarify that this only measures their success in getting people to participate, not the effectiveness of the training itself. Another tool mentioned by RM4 that can offer insight is MSB's Infosäkkollen. Infosäkkollen is a tool designed to assist municipalities, regions, and government agencies in monitoring and improving their systematic information security work. The tool is an Excel-based form that requires input from various parts of the organization to answer questions about different aspects of information security work. The responses are then endorsed by management and used to provide feedback on the level of work and which areas need improvement. The feedback also includes tips on relevant support and links for further development. Organizations that use Infosäkkollen can report their results to MSB, which provides feedback and recommendations based on the data collected. The Infosäkkollen benchmark allows organizations to compare their results with other responding organizations and collaborate on the results (MSB, 2022a).

RM1 and RM4 highlight that this tool does not provide insight into the effectiveness of their communication or outreach efforts to employees. Instead, it solely indicates the level of their information security work through self-assessment based on questions designed by MSB. RM4 however, mentions that they are currently awaiting an external audit, which they believe will offer a more comprehensive evaluation of their outreach to employees.

RM3 mention that each department does a maturity assessment once a year that provides them with an indication of how well they comply with policies and other parts around it. This is measured using a model called CMMI (Capability Maturity Model Integration). CMMI is a process improvement maturity model for the development of products and services, published by the Software Engineering Institute of Carnegie Mellon University. It can be used to integrate IT Risk Management with any IT process improvement efforts, as it covers activities that guide the implementation of highly mature development and service processes. CMMI is not focused on projects, but on regular business processes that are executed daily, and during the maturity improvement process execution, information about expected operational risks can be gathered and passed to IT Risk Management. Risk treatment measures from IT Risk Management can be included in the process design. Therefore, CMMI has a broad scope and can be applied to various concrete business processes (European Union Agency for Cybersecurity [ENISA], n.d.). RM3 further emphasizes that the CMMI assessment does not provide them with specific numerical data. Instead, it offers a general indication of their performance by presenting them with broad figures that give an idea of the scale of a given situation.

RM2 notes that a strong indication of the effectiveness of their communication is the high level of interest among employees to learn more. According to RM2, the fact that employees request exercises indicates that their outreach is successful. They argue this based on that people are unlikely to request something they have no knowledge of. In addition, RM2 mentions that they conduct follow-ups and surveys on the implementation of policies and regulations, a practice that is also mentioned by RM6:

> *"I wouldn't say effectiveness, but we follow up on implementation. We have made random samples of these general training courses and seen like 'have you understood what it is about? Do you know how to use this?', but also measure the level of knowledge."* – RM6

RM5 acknowledges that the effectiveness of communication is not systematically measured and is often unsatisfactory in many places. They stress that they can identify reasons for communication gaps, but find it challenging to determine how to improve communication for greater impact. They further assert that they lack a tool to measure effectiveness and instead rely on assessments that serve as a basis for devising a new strategy for the next time a policy or regulation is developed, rather than a specific systematic approach.

While the literature highlights the importance of effective communication, the participants reveal that their organizations do not have specific measurements for evaluating communication efficacy. Instead, they rely on indirect indicators such as follow-ups, assessments, and employee interest. These findings suggest that organizations may benefit from developing and implementing more systematic approaches to measure communication effectiveness in the context of information security policies and regulations.

5.2.6 Improvements in Communication

The respondents offer various suggestions for improving communication of information security policies and regulations within their organizations. RM1 discusses their agency's work on developing an ISMS and stresses the importance of making information logically connected and easily searchable. They highlight the challenges in managing complex issues that fall between legal, security, IT, and management, resulting in a large amount of information that is not logically connected, making it difficult to navigate and find answers to specific questions.

RM3, similar to RM1, acknowledges the difficulty of managing interconnected documents within the organization. They focus on the challenge of revising and modifying these documents and suggest the agency function as an internal referral body to ensure accurate referrals and adjustments to policy documents. RM3 emphasizes the importance of ensuring that everyone is updated and referring correctly:

> *"And then you see, well, 'here you are referring to our old policy here'. 'That's not how it applies at all, but this is how it applies' and then you adjust it. So, there are improvements to be made there, I think. I don't know how, but in some way at least ensure that everyone is updated and referring correctly."* – RM3

RM2 emphasizes the need to educate individuals on information security's importance and argues it is a collective responsibility. They recommend that policy documents should be communicated in a way that highlights the significance of information security, making it easy for individuals to understand its importance.

RM4 acknowledges room for improvement in their organization, having conducted a review, developed new procedures, rewritten old ones, and created new guidelines for employees. RM4 notes that procedures and guidelines must be easily accessible and that information security coordinators within departments should effectively reach out with new documents.

Both RM5 and RM6 emphasize the importance of personal contact and interaction with employees for effective communication of information security policies and regulations. They suggest being present in the organization, meeting employees, and addressing concerns. RM5 acknowledges the challenges of reaching out to many employees with limited safety personnel: "Something that is considered to be important and have a great effect is to be present in the organization, meet them, talk to them and let them ask questions. Explain what the purpose of the regulation is, what risks the regulations are intended to manage. However, this is often difficult in a large organization where the number of people working with safety is small in relation to the total number of employees." – RM5

RE1, RE3, and RE4 propose having accessible information security officers or personnel, while RE1 and RE5 suggest using workshops with real-life cases for effective policy communication. RE2 highlights the need for clearer instructions in policies and regulations. RM5, RE2, and RE5 express concerns about the language used in these documents, which can be difficult to understand. RE3 and RE5 mention the challenge of finding specific information within these documents:

> *"Furthermore, the policies and regulations themselves could be easier to understand and easier to search in for specific information."* – RE3

> *"[...] it is not always easy to find among all the content that exists in these documents. Because there is a lot and filtering through it all is a big task in itself. If I search for a specific thing, the search can return several documents, so it can be very tough and frustrating."* – RE5

5.3 Employee Attitudes Towards Information Security Policies and Regulations

The attitude of employees in organizations towards information security can be either positive or negative and this can have a direct impact on the implementation of security controls and overall information security (Tu & Yuan, 2014). Employee attitudes are strongly linked to information security awareness and culture and can vary significantly (Safa, von Solms & Furnell, 2016). It is therefore imperative for users to adhere to information security policies in order to mitigate the risk of information security issues (Bauer, Bernroider & Chudzikowski, 2017).

5.3.1 General Attitude

According to the respondents from top management and information security officers, the overall attitude of employees towards information security policies and regulations is positive, but some respondents lift certain things that require attention.

RM1 observes that employees are generally cooperative and eager to comply with policies once they are aware of what is expected of them, but acknowledges that some may find the regulations cumbersome and hindering to their work. RM2 emphasizes that their organization has a high level of compliance, with employees actively requesting training exercises, indicating an interest and willingness to do the right thing. RM3 believes that most employees are positive and think that clarity is a good thing, but acknowledges that they have not made any direct measurements on it. RM4 notes that there has been a change in the level of acceptance towards information security in recent years, with greater awareness of the threats and a higher willingness to prioritize safety over convenience. RM4 observes that their employees possess knowledge of their ISMS, but acknowledges that they may not always comprehend the expectations placed on them. Additionally, RM4 acknowledges that their authority is composed of passionate experts who sometimes may prioritize their own issues over the goals of the authority, which RM4 means can be a problem. RM4 further notes that their employees are well aware about potential threats and risks but may not always know how to respond to them. RM5 acknowledges that the importance of information security has been increasingly accepted and recognized in recent years, with external factors such as global tensions, media coverage, and the growing prevalence of digitization in daily life being contributing factors to this. RM6 states that their employees grasp the significance of information security and compliance, but may not fully comprehend the need for themselves to change.

The employees are asked about their perspective on the importance of adhering and complying to information security policies and regulations. Their responses further support the notion that employees have a positive attitude towards these policies and regulations. All respondents stress the significance of complying with them. RE1, RE3, RE4 and RE5 further recognize the importance of following them and doing things right because of the importance of representing a government agency specifically, and handling the unique sensitive information that their positions entail.

When employees have a positive attitude towards compliance, they are more likely to follow the policies and regulations that are in place (Da Veiga & Eloff, 2010). The success of information security policies and regulations can be significantly influenced by the attitudes of employees towards compliance. A positive attitude can foster a security culture that prioritizes the protection of sensitive data, whereas a negative attitude can diminish the effectiveness of such policies and regulations (AlKalbani, Deng, Kam & Zhang, 2017; Höne & Eloff, 2002b). The statements and responses from both top management and employees suggest a positive attitude towards compliance with information security policies and regulations. The respondents acknowledge that employees are generally cooperative and willing to comply with policies, but that there can be certain obstacles to overcome. However, it is evident that these obstacles are seldomly related to the attitudes of the employees, but rather to their understanding and knowledge of the content in the documents. The importance of adhering to these policies and regulations is recognized and emphasized by both top management and employees. This positive attitude towards compliance and information security in general is essential in ensuring that the government agency handles sensitive information safely and it is evident that the employees grasp the significance of information security and compliance.

5.3.2 Awareness

Information security awareness is the most important factor that mitigates the risk of information security breaches in organisations (Safa, von Solms & Futcher, 2016). Increasing information security awareness is achieved by performing processes that educate individuals within an organization about information security policies, procedures and best practices. The aim of information security awareness is to increase knowledge and understanding of the importance of protecting sensitive information, as well as to equip individuals with the skills and knowledge needed to identify and prevent potential security threats (Chen, Shaw & Yang, 2006). By raising awareness about information security, organizations can reduce the risk of security breaches and ensure that sensitive information is properly protected (Elmrabit, Yang & Yang, 2015). This not only helps to prevent security incidents, but it also helps to meet regulatory requirements, maintain customer trust and enhance the overall security culture within the organization (Lopes, Guarda & Oliveira, 2019).

In the survey, the employees were asked to rate their level of threat awareness, awareness of policies and regulations, as well as their understanding of them using a scale ranging from one to five. The following tables present the rating scale and descriptions of the rating scales that was employed to evaluate the levels of awareness and understanding:

Table 3 – *Rating Scale of Awareness and Understanding in Relation to Threat Awareness and Policies/Regulations*

Rating	Threat Awareness	Policies and Regulations Awareness	Policies and Regulations Understanding
1	Minimal awareness	Minimal awareness	Inadequate understanding
2	Limited awareness	Limited awareness	Limited understanding
3	Decent awareness	Decent awareness	Basic understanding
4	Extensive awareness	Extensive awareness	Comprehensive understanding
5	Exceptional awareness	Exceptional awareness	Profound understanding

Table 4 – *Rating Scale of Awareness and Understanding in Relation to Threat Awareness and Policies/Regulations – Scale Descriptions*

Threat awareness	Minimal awareness	Lack of understanding of potential threats, with limited knowledge of risks and vulnerabilities.
	Limited awareness	Somewhat restricted understanding of threats, with gaps in knowledge of risks and vulnerabilities.
	Decent awareness	Reasonable level of knowledge and understanding of common threats, risks and vulnerabilities.
	Extensive awareness	Broad-ranging and comprehensive understanding of various threats, risks and vulnerabilities.
	Exceptional awareness	Outstanding level of knowledge and understanding of complex threats, with knowledge about proactive anticipation and mitigation measures.
Policies and Regulations Awareness	Minimal awareness	Basic awareness of policies and regulations, with limited familiarity.
	Limited awareness	Incomplete awareness with gaps in knowledge of relevant policies and regulations.
	Decent awareness	Solid awareness of key policies and regulations relevant to the organization.
	Extensive awareness	Comprehensive knowledge of policies and regulations for effective compliance.
	Exceptional awareness	In-depth knowledge of intricate details of policies and regulations, ensuring full compliance and effective navigation.
Policies and Regulations Understanding	Inadequate understanding	Insufficient knowledge and comprehension, below the desired level.
	Limited understanding	Restricted comprehension with significant gaps in knowledge.
	Basic understanding	Foundational or rudimentary grasp of fundamental principles.
	Comprehensive understanding	Thorough and all-encompassing comprehension of policies and regulations.
	Profound understanding	Exceptional insight into the intricacies and application of policies and regulations.

The employees were also asked to provide a motivation for their rating. The responses indicate that employees have a strong awareness of threats as well as a strong awareness of policies and regulations, but that their understanding of them vary:

Table 5 – *Employee Awareness and Knowledge*

Respondent	Threat Awareness	Policies and Regulations Awareness	Policies and Regulations Understanding
RE1	5	5	5
RE2	4	5	3
RE3	4	5	2
RE4	5	5	5
RE5	4	5	3

All respondents state that their high level of awareness of both threats as well as policies and regulations is a result of the training that they have received. RE1 and RE4 additionally note that information security is integrated into many organizational activities, which has also contributed to their solid understanding of policies and regulations. RE2, RE3, and RE5 attribute their lower understanding of policies and regulations to factors such as the complexity of the language used in them, unclear instructions, and difficulty in finding specific information due to the overwhelming amounts of available documents.

5.3.3 Culture

According to Amankwa, Loock, and Kritzinger (2014), the aim of promoting information security awareness is to foster a culture of security in an organization and to ensure that all staff have the necessary resources to safeguard sensitive information against unauthorized access and data breaches. A robust information security culture involves employees who are knowledgeable about security policies and practices, alert to potential threats, and committed to protecting sensitive information.

RM1 describes a shift in their information security culture where they went from being police officers and enforcers who only delivers negative messages to becoming helpers and supporters who are there to help and something good is happening. This shift has led to a more efficient and effective culture, where the focus is on controlling and managing the right things, not just checking things for the sake of it. RM1 claims that being police officers had a negative impact on the employees. RM1 also mentions that this shift towards a more positive and helpful culture is a trend in the industry, with many colleagues undergoing a similar journey to become trainers or helpers.

RM2 emphasize the importance of having an information security culture in order to create a safe and secure working environment. Technical solutions such as passwords and access controls are important, but they cannot replace the need for a culture of awareness and the sense of personal responsibility among employees which falls in line with Baker and Wallace's (2017) argument that technical approaches alone cannot solve information security issues and that social and organizational measures must also be involved. RM2 further acknowledges that building this culture requires long-term effort and training, as well as a non-judgmental approach to mistakes that allow for learning and improvement:

> *"Well, we do a lot of training and we put a lot of effort into having an open climate. It's like, well, making mistakes is nothing, it's also a way for us... So, we can learn from mistakes. So, it's a very, what can I say, non-judgmental culture and it's very important for safety work that it's like that, so to speak."* – RM2

RE1, RE2, RE3, RE4 and RE5 all recount the same narrative, stating that their organizations have an open climate where colleagues inform each other of mistakes and where management are forgiving and view mistakes as learning opportunities rather than grounds for punishment.

RM2 continues and cites examples of employees politely reminding colleagues to carry their service cards or asking about unfamiliar colleagues who are not wearing their them. RM2 means that when that happens it is a sign that they have succeeded in creating the desired culture. RM2 further states that scenario-based training and a solid introduction scheme can help establish this culture, and that it is important to set the culture early on with new employees, which is something that they work with and try to achieve through introductory training.

RM5 discusses different communication methods used to create and anchor a culture of information security within their organization. They highlight the intranet as an important channel for reaching everyone, along with news feeds and specific pages. However, they note that these methods are not enough to create a strong culture and supplements them with training, such as classroom training and digital meetings. They also hold safety days where lectures are given and further communication is facilitated.

Van Niekerk and von Solms (2005) states that that educating personnel is a critical step in creating a culture that prioritizes information security and that this mindset leads to a behavioural shift, transforming employees from potential risks to assets for information security and the organization. The authorities that have been interviewed share this view. RE1, RE2, RE3, RE4, and RE5 all recount the extensive effort their organizations put into education and awareness training and emphasize how their training have led to them recognizing and prioritizing security in their daily work.

5.3.4 Ensuring Compliance

Respondents discuss various methods to ensure compliance with information security policies and regulations. RM1 shares that their transition from a policing role to a supportive one has positively impacted compliance. This shift allows them to focus on pertinent issues instead of merely going through the motions. Their IT organization employs a well-developed process, governance, and follow-up, ensuring necessary security and compliance activities are performed in processes like development. RM2 recounts a similar approach, incorporating security and information security issues into the development process from the beginning rather than addressing them later. RM2 argues that including security in small increments throughout the development process helps maintain its importance in everyone's minds and ensures it is part of the entire development chain.

RM3 mentions the CMMI model, asserting its effectiveness in evaluating their organization's performance. They view this assessment as a reliable gauge of their compliance level and a basis for taking appropriate measures. Additionally, RM3 acknowledges the incident management process as another means of assessing compliance efforts' efficacy, noting that this approach is more reactive in nature and provides insight into what works and what doesn't. However, they express a preference for avoiding reactive approaches and note that it is not their favored method of addressing compliance issues.

RM4 adopts an approach prioritizing a workplace culture where employees meet compliance requirements through routine job duties without actively considering specific regulations or legislation. RM4's organization aims to achieve this by restricting, simplifying, and clarifying areas within their control. RM4 also mentions using external and internal audits to assess compliance efforts, with external audits crucial for avoiding overconfidence and ensuring objective evaluations.

RM5 and RM6 discuss follow-up surveys and incident statistics collection to identify non-compliance root causes. Targeted measures like communication or training can then be directed to relevant business areas, aiming to prevent future undesirable events. RM5, like RM1 and RM2, includes information security and security considerations throughout the procurement or development process of policies and regulations.

RE1, RE2, RE3, RE4, and RE5 rely on training for compliance and rarely refer to policies and regulations. When encountering issues, employees consult colleagues or managers instead of referring to policies and regulations. Only RE3 and RE5 report consulting governing documents for guidance in addition to colleagues or managers:

> *"I fall back a lot on what I've learned during my training. I only open up and read the policies and regulations in certain situations that require it."* – RE3

> *"But it is usually quickly handled either by looking at our governing documents or asking colleagues or management about instructions on what to do."* – RE5

These approaches to ensuring compliance generally align with Howard (2003), emphasizing enforcement, corrective action, and awareness efforts. However, regular employees' experiences suggest room for improvement in providing accessible resources and guidance to better understand and comply with policies and regulations. Statements from RE1, RE2, RE3, RE4, and RE5 suggest that while Howard (2003) emphasizes enforcement and management's role in policy compliance, employees may benefit from additional support and resources to help them understand and adhere to information security policies and regulations in practice.

5.3.5 Challenges in Ensuring Compliance

To encourage employee compliance with information security policies, top management must exhibit support for desired outcomes by demonstrating appropriate behavior and offering incentives for positive behavior while imposing consequences for negative

actions (van Niekerk & von Solms, 2005). The respondents discuss various challenges in ensuring compliance with information security policies and regulations. RM1 and RM5 highlight the difficulty of implementing effective information security tasks in large, complex organizations. Reaching the right people with the right information becomes challenging due to the organization's size and complexity. RM5 notes that the scarcity of information security specialists relative to the total workforce exacerbates this challenge:

> *"[…] these are large organizations where there can be many different levels of management and if there are also quite few people working with security issues in relation to the number of total employees, this can be a challenge."* – RM5

RM1 and RM3 mention the challenge of managing vast amounts of information, guidelines, and employees, with information security policies and regulations constituting only a small part. Effectively communicating information and preventing information security policies from being overlooked among other documents and tasks is challenging. RE2 shares this sentiment, stating that handling large amounts of information can be overwhelming:

> *"Then I can think that certain information that is communicated is very overwhelming. It's like a lot at once and it can be difficult to take it all in."* – RE2

RM3, RM4, and RM5 emphasize the need to simplify information security policies and regulations, making them less formal and easier to understand. Technical, legal, or safety terminology can hinder employee comprehension and compliance. RE2, RE3, and RE5 express similar concerns about understanding the language or terminology used in policies and regulations:

> *"You have different languages. People working in security use a different language. It may be technical language that comes entirely from the security industry. It may be that it is, it depends a little on what it is, sometimes it can be about legal terms that are incomprehensible to those who do not work with the issues. And it can also involve technical terms. Both law and technology and the technical language associated with these discussions are often very well used in security work. And this can often be a reason why you may not reach the final recipient."* – RM5

Furthermore, RM5 acknowledges the challenge of understanding employees' daily lives, making it difficult to adapt information security measures to their realities. This issue arises when security professionals become too disconnected from employees.

RM2 identifies numerous challenges, including impatience, balancing protection with avoiding shortcuts, dealing with strong-willed individuals, keeping up with rapidly evolving technology, and addressing outsider threats. RM2 also mentions immature management that fails to understand the importance of information security, although they clarify this is based on past experiences and not their current workplace. This

challenge primarily stems from the costs of implementing information security measures without immediate visible impact and the perception that information security can be restrictive.

Addressing these challenges requires simplifying and clarifying language, understanding employees' realities, and balancing security with usability. Coupled with strong support from top management, as suggested by van Niekerk & von Solms (2005), organizations can improve compliance with information security policies and regulations.

To shape employee compliance with information security policies, top management should demonstrate their support for desired outcomes by exhibiting appropriate behaviour and providing incentives for good behaviour and consequences for negative behaviour (van Niekerk & von Solms, 2005).

5.3.6 Incidents

RM3, RM4, RM6, RE1, RE2, RE3, and RE4 mention occurrences of clicking on suspicious links and opening email attachments at their workplaces. RM4, RM5, RM6, RE1, RE2, RE3, and RE5 cite incidents where information was sent to the wrong address or incorrect information was transmitted. RM3 and RE3 report incidents of sensitive information stored in inappropriate locations, while RM5 discusses instances of employees transmitting sensitive information through the wrong channels or ignoring safety measures due to their complexity. RE1, RE2, RE4, and RE5 note cases of sensitive information written on paper and left visible on desks. RE1, RE2, and RE3 recount incidents of leaving computers logged in and unattended, and RE2 and RE4 report incidents of failing to secure hardware before leaving for the day. Additionally, RE2 discusses cases of colleagues forgetting to close designated rooms and granting unauthorized access to restricted areas. RE3 reports visiting websites on their work computer which is not permitted under their regulations.

The main reasons cited for these incidents are convenience, accommodation, and lack of knowledge. While these are generally minor mistakes, RE4 cautions that they can become significant under certain circumstances. RE1 and RE5 recount instances of recording information in the wrong journal, with RE5's case being more severe due to the sensitive nature of the information.

Some respondents mention major incidents, such as RM6's account of an employee mistakenly sending a former employee's final salary to a fraudster. The employee's desire to be helpful led to a failure to adhere to regulations and work in a risk-based manner. RE2 recalls a similar incident of unauthorized access to a restricted room. RE1 and RE4 mention major incidents where colleagues accessed cases involving individuals they were personally acquainted with for personal reasons. RE1 recalls another incident where an employee handled a case involving someone that they had a relationship with:

> *"[…] but a colleague who had a relationship with a client and at the same time handled their case. It's weird, because the thing is that first of all you are biased. So, there were so many things that happened, but that colleague got a reminder and not much more than that."* – RE1

RM3 also notes incidents of employees storing organizational data on personal devices and discussing cases in public areas prior to their employment at the organization.

Metalidou et al. (2014) found that those who claim to have security awareness still engage in actions that jeopardize information security, such as clicking on suspicious links and opening email attachments. Cheng, Liu, and Yao (2017) point out that unintentional leaks often occur due to neglect of security measures, inadequate technology, or lack of employee awareness. The respondents provide examples of such mistakes, including allowing colleagues into restricted areas without service cards, leaving sensitive information visible, and leaving computers logged in while unattended. These findings align with Safa, von Solms, and Futcher (2016), who state that sharing usernames and passwords, recording them on visible sticky notes, opening unknown emails and attachments, downloading software from the internet, and leaving computer systems logged in while unattended are all examples of employee mistakes. Sarkar (2010) states that intentional misuse can come from insiders who use corporate resources for their own purposes, as recounted by RE1 and RE4 in their organizations.

5.3.7 Incident Management

Each of the respondents' organizations have established systematic incident management procedures in place, which may vary to an extent, but the fundamental principle is consistent. In the event of an incident, it must be reported, followed up and dealt with accordingly. The specific steps involved in handling the incident do differ among the organizations. All respondents emphasize the importance of having a non-judgmental approach to handling incidents.

RM2 emphasizes the importance of non-accusatory incident management, where the primary goal is to inform rather than blame. This approach aims to create a safe environment where people feel comfortable reporting incidents without fear of being reprimanded. The organization recognizes that everyone is capable of making mistakes and strives to minimize stress caused by incidents:

> *"But it's not an accusatory or suspicious conversation, but more of an information conversation."* – RM2

RM3 outlines their incident detection process, which involves not only reported incidents but also proactive measures such as storage area searches to locate misplaced information. When misplace information is found, they are promptly reported as incidents. The incident is then analysed by specialized groups based on its type before being returned to the information owner for handling. Information security officers also conduct quarterly incident reports, which are then shared with management. Similarly, RM4's organization reports both simple and serious incidents and follows up on them as needed. The incident is analysed by specialized groups before being returned to the information owner for handling. In addition, the organization conducts quarterly incident reports that are shared with management. Depending on the severity of the incident, they may also report to supervisory authorities such as IMY and MSB.

RM5's organization uses surveys as a follow-up measure, compiling incident statistics to gauge the "temperature" of the situation. They then direct measures to the relevant

departments to prevent further incidents. Employees are also required to report phishing emails and spam on a daily basis. Similar to RM4, RM5's organization may also report incidents to supervisory authorities such as IMY, MSB, and the Swedish Security Service (SÄPO) based on the severity of the incident:

RM1, RM2, RM3, RM4, RM5, and RM6 however, all emphasize the importance of having a non-judgmental approach to handling incidents. RE1, RE2, RE3, RE4, and RE5 all share similar views that align with that notion. They emphasize that their organizations prioritize education and development over punishment as a means of managing incidents. These respondents share that their organizations have well-established guidelines and rules for handling incidents, with an emphasis on reporting incidents regardless of how minor they may seem. In addition, they report that their organizations foster a culture of open communication where mistakes are viewed as opportunities for growth and improvement. They highlight that the severity of the incidents determines the measures taken after reporting, but that their organizations always maintain a focus on learning from the incident and taking measures to prevent similar incidents from occurring in the future. The employees further report that their organizations try to proactively approach incident management through training, having guidelines in place and cultivating a supportive culture of learning and improvement that helps minimize the risk of incidents happening.

To shape employee compliance with information security policies, top management should demonstrate their support for desired outcomes by exhibiting appropriate behaviour and providing incentives for good behaviour and consequences for negative behaviour (van Niekerk & von Solms, 2005). In contrast, the respondents' experiences imply that a non-judgmental approach to handling incidents is more effective than punishment in shaping employee compliance with information security policies and regulations. By prioritizing education and development, cultivating a culture of open communication, and proactively approaching incident management instead, the organizations create an environment that encourages compliance and prevents incidents from occurring in the first place.

5.3.8 The Human Factor and Insider Threats

RM2 highlights the importance of having a competent and united team. However, some members may not understand the importance of their work, which can be detrimental to the team's success. It is crucial for the competent members to work with those who need support to ensure everyone is working together and contributing equally to the team's success. Otherwise, even one weak link can affect the entire team's performance:

> *"So yes, I think it's important to get an operation together so that everyone feels that they are working together. Because it's like one person who can, like, even if I do everything, it doesn't matter if the person next to me does everything wrong. Then I will still suffer."* – RM2

RM3 states that having a policy alone does not provide security in terms of the human factor and insider threats, rather it provides a direction. It is essential to work on education and awareness to ensure that people understand the policy and comply with it. Additionally, RM3 believes that the human factor is crucial, and feedback from

employees can help understand and address difficulties in complying with policies. RM3 also points out that being a hot topic in the media helps employees understand the importance of information security and motivates them to find ways to avoid security breaches in the workplace:

> *"So yes, it certainly helps a lot that it is a hot topic in newspapers and the like, I think. I think many people read and follow the news and see websites that are down due to overload attacks, you read about someone who has been fined for not handling personal data properly. So, I think that as an employee you get a pretty good picture of the threats that exist around the information. And that helps us because then people come to us and want to find a way to avoid it happening in the workplace, so to speak."* – RM3

RM4 states that the human factor is always present, but outsider threats may feel more relevant currently due to the rise in hacking incidents. However, RM4 believes that the majority of employees and managers want to do the right thing and that providing them with tools and easy-to-understand explanations can facilitate this. Additionally, mistakes should be viewed as opportunities for learning and improving, and employees should be encouraged to take responsibility for their own education and understanding of information security rather than relying solely on others to provide them with information. RM4 put emphasis on that everyone wants to do the right thing, and it is the organization's responsibility to make it as easy as possible for them to do so:

> *"But the basic attitude is that everyone wants to do the right thing, you just have to provide the tools and conditions to be able to do the right thing. And also pointing out my own responsibility to be able to look up information and know where to find it. It's not just that you should be fed like a baby bird with here you are and here you are. But you should also have a responsibility yourself."* – RM4

RM5 states that the human factor is a major threat from both a corruption as well as an infiltration perspective, and is often underestimated compared to outsider threats. There is a need to be more careful and suspicious, and to work on managing insider threats as well as outsider threats. It is important to keep track of permissions and work with technical solutions to ensure that people are who they claim to be and that logging systems are used in a responsible way. In recent times, there have been examples of infiltration and espionage in Sweden, and these security risks can affect vital operations or Sweden's security in general. Corruption and other types of irregularities are also a constant concern, as they can damage public confidence in authorities and the state as a whole.

RM6 states that understanding and acting in a certain way is a crucial part of security measures, and it cannot be forced upon anyone. It is important to invest as much energy and effort in the human factor as in technology and control, because technical solutions alone are not enough. It is necessary to understand why security measures are in place and how to ensure that people do not take shortcuts or get annoyed:

5.3.9 Improvements to Employee Attitudes

The respondents mention several ideas for improving their employees' attitudes towards information security policies and regulations. RM1, RM3, and RM4 suggest that regulations should be simple and clear, with instructions that are easily comprehensible. They propose developing regulations that are not overly complex and communicating them in a straightforward and easily understood manner. They argue that this would make it easier for employees to comply with information security policies and help them do the right thing. RM3 highlights the use of tabular instructions to explain procedures, while RM4 suggests providing specific guidance and support for various assets and utilizing relatable examples from everyday life:

> *"I think we can, we have seen that something that employees really like. It's simple, like tabular instructions and how to do things. Employees usually want answers to simple things, like 'can I print on my printer at home?'."* – RM3

> *"And simple help and advice and support. And that you make it simple and understandable and use examples from everyday life."* – RM4

RM1 and RM4 emphasize the significance of providing employees with appropriate tools that are functional, relevant, and effective. They suggest that good tools are necessary for successfully improving employees' attitudes.

> *"Instead, employees need access to the tools and information that make it easy for them to do the right thing"* - RM4

RM2, RM3, RM5 and RM6 talks about anchoring and mentions different approaches to achieving it. RM2 suggests getting employees to prioritize the organization's greater good over individual projects through encouraging collaboration:

> *"So, on a [identifying], the average [identifying] thinks that their project is the most important project. Somebody has to say what is most important. And once again, it is a question of priorities, of prioritising activities. What is most important for our activities. If something happens, then we should prioritise this and this should take a back seat."* – RM2

RM3 proposes educating employees about the benefits of governance and information security by demonstrating their advantages, as well as the consequences of non-compliance. RM5 suggests instilling a sense of responsibility in employees by explaining the importance of certain routines and safety measures, highlighting the negative consequences of non-compliance, and emphasizing the benefits of adhering to information security practices:

> *"I think we can always be clearer and demonstrate the benefits of having governance in this area."* – RM3

"You have to assume that the will is there, but in order to achieve desirable attitudes and behaviours, not only the will is required, but also an understanding of why you need to take different routines and safety measures. It can often be a matter of describing the negative consequences that could occur if we do not succeed in doing this in the right way, and then perhaps the people who this is about can then relate to it." – RM5

6 RESULT

This chapters aims to answer the study's three research questions. The chapter is structured according to the order that the research questions has been presented in previous chapters.

6.1 How do government agencies work to develop information security policies and regulations?

This question is answered based on the experiences and recollections of the respondents from top management and information security officers.

6.1.1 Policy Development Process

The analysis shows that government agencies adopt a systematic approach to develop information security policies and regulations, taking into account the unique context and requirements of their organizations. The process is often triggered by various factors, such as legal or regulatory requirements, changes in the threat landscape, technological advancements, or organizational restructuring. The respondents highlight the importance of understanding the organization's operations, risk factors, and stakeholder interests in developing policies and regulations. They collectively emphasize the need to tailor policies and regulations to the specific needs of the organization, considering aspects such as its size, industry, and the nature of the information processed.

Engaging stakeholders from the initial stages of policy development is a key aspect emphasized by the respondents. This ensures that policies and regulations are created with input from those affected by them, leading to more effective and relevant outcomes. Stakeholders include not only employees but also partners, customers, and regulators who have a vested interest in the organization and its information security. Another critical element is the focus on making policies and regulations practical and easily implementable. The respondents note the importance of creating policies that are accessible, easy to understand, and applicable in day-to-day operations. They stress that policies should not merely be documents that sit on a shelf but should serve as living guidelines that everyone in the organization can relate to and adhere to.

The agencies also pay attention to adherence to legal requirements, industry standards, and best practices, ensuring that the developed policies and regulations comply with the relevant legal and regulatory frameworks. This includes taking into account constitutional requirements, international standards, and directions from relevant authorities. The respondents mention standards and regulations, such as MSB's regulations, which are based on the ISO 27000 package (ISO, 2018). The ISO 27000 series, along with other ISO packages like the ISO 14001 (ISO, 2004) for environmental management systems, help guide organizations in creating effective policies. Some respondents mention using the Plan, Do, Check, Act (PDCA) cycle framework in their work when developing policies and regulations. Additionally, GDPR, the Security Protection Act (SFS 2018:585), and OSL (SFS 2009:400) are also cited as essential regulations to comply with.

6.1.2 The Human Factor and Insider Threats

The analysis reveals that the human factor is a significant concern for government agencies when addressing information security. The respondents however, acknowledge that the human factor is not sufficiently addressed through policies alone, as policies cannot fully account for human behaviour and the complexities of human decision-making. To effectively address the human factor, the respondents emphasize the need for a combination of training, awareness programs, and fostering a culture of security awareness. This involves raising employees' understanding of their roles and responsibilities in maintaining information security and ensuring that they have the necessary knowledge and tools to mitigate risks.

The agencies also highlight the importance of clear communication strategies when it comes to information security policies and regulations. This includes disseminating information through various channels, engaging employees in the policy development process, and fostering open lines of communication between different departments and levels of the organization. The role of top management in addressing the human factor is also stressed by the respondents. They point out that top management's commitment and involvement are essential for creating a culture of security awareness and ensuring that employees understand the importance of adhering to policies and regulations.

6.1.3 Essential Steps

The respondents identify several essential steps that should be considered when developing and implementing information security policies and regulations. These steps include conducting a risk assessment, identifying stakeholders, setting security objectives, developing, reviewing, implementing, maintaining, and updating the policy.

Risk assessment is highlighted as a crucial starting point for policy development, as it enables the organization to understand its vulnerabilities and prioritize its efforts in addressing the most pressing risks. This also ensures that the developed policies and regulations are relevant to the organization's specific needs and requirements. Identifying stakeholders and obtaining their support is mentioned as another essential step in policy development. This involves considering the needs and concerns of all parties affected by the policies and regulations, including employees, partners, customers, and regulators. Setting security objectives is also emphasized as a critical aspect of policy development. The respondents note that this can be a complex process, often neglected or left as the last priority. However, clear and measurable security objectives are necessary for guiding the organization's efforts and ensuring that the policies and regulations are effective in achieving the desired outcomes.

Lastly, the respondents highlight the importance of continuous review, implementation, maintenance, and updating of policies and regulations. This involves ensuring that the policies remain relevant and effective in the face of changing threats, technologies, and organizational requirements. The respondents stress that policies should not be static but evolve over time as the organization and its environment change.

Implementing policies and regulations in day-to-day operations is emphasized as a critical factor in their effectiveness. The respondents point out that merely having

policies and regulations on paper is not enough. They must be integrated into the organization's daily activities and procedures. This includes assigning roles and responsibilities, monitoring compliance, and regularly evaluating the policies' effectiveness.

6.2 How do these government agencies communicate information security policies and regulations to employees?

This question is answered based on the experiences and recollections of the respondents from both top management or information security officers and regular employees.

6.2.1 Communication Channels

Various communication channels are employed to convey information security policies and regulations to employees. One of the primary methods identified is the use of the intranet, which serves as a central hub for disseminating news, policy changes, and procedures. Both top management and employees utilize the intranet extensively, ensuring that everyone has access to the same information on a familiar platform. This is in line with Höne and Eloff's (2002b) suggestion that conventional communication methods should be used for policy communication within organizations.

Another important aspect of policy communication is education and training. Respondents from the agencies highlighted a significant focus on providing regular and role-specific training to employees. This approach aligns with the literature, which emphasizes the need for comprehensive security awareness programs and periodic training to increase employee knowledge and involvement in security efforts (Sarkar, 2010; Tu & Yuan, 2014). Examples of such training include introductory packages for new employees, theme days addressing current security challenges, and targeted courses for specific employee groups.

In addition to the intranet and training programs, departmental information security coordinators play a crucial role in policy communication. These coordinators are responsible for sharing new guidelines or policies with employees through various channels such as departmental meetings or emails. They also provide training to new employees, ensure awareness of the organization's management system for information security, and remind employees of policies and procedures. Respondents reported that this method of communication is effective in informing employees, although the literature does not explicitly mention the use of information security coordinators.

Finally, theme days or specific periods where they focus on information security, such as the Information Security Month, are employed by government agencies to place greater emphasis on cyber and information security. This annual campaign, held in October, aims to raise awareness and skills in information and cyber security among individuals and organizations. Participation in such events allows agencies to further communicate policies and regulations to employees and reinforce the importance of information security.

6.2.2 Effectiveness

The respondents state that they do not measure the efficacy of their communication channels directly, but instead relies on follow-ups and assessments instead to get indications. Some respondents note that completion rates of training campaigns can provide an indication of efficacy, but these only measures participation, not the effectiveness of the communication channels themselves. One tool mentioned, Infosäkkollen, is designed to assist organizations in monitoring and improving their systematic information security work. However, it does not provide insight into the effectiveness of communication or outreach efforts to employees. Some respondents are awaiting external audits, which they believe will offer a more comprehensive evaluation of their outreach. A model called CMMI (Capability Maturity Model Integration) can be used to assess compliance with policies and other aspects of information security. However, this assessment does not provide specific numerical data, but rather a general indication of performance.

A strong indication of communication effectiveness is the high level of interest among employees to learn more, as well as the use of follow-ups and surveys on policy implementation. However, respondents acknowledge that effectiveness is not systematically measured, and they lack a tool for this purpose. They rely on assessments as a basis for devising new strategies for policy or regulation development.

6.2.3 Improvements in Communication

In order to enhance the communication of information security policies and regulations within government agencies, respondents suggest various improvements. One area of focus is the need for a well-connected, consistent, and easily accessible ISMS. This is essential because the current state of documentation is often vast and difficult to navigate, leading to confusion among employees. Agencies should ensure that the ISMS is logically connected and searchable, enabling employees to find the information they need more easily.

Another suggestion is to improve the management system for maintaining the coherence and relevance of policy documents. Agencies could function as internal referral bodies to ensure accurate referrals and adjustments to policy documents, which would help keep everyone updated and referring correctly. This would help tackle the challenge of managing numerous interconnected documents and streamline the process of revising and modifying them.

Educating employees who do not work directly with information security about its importance is also crucial. Information security is a collective responsibility and not solely the task of the IT department. Policy documents should be communicated in a way that emphasizes the significance of information security and makes it easy for employees to understand its importance. Agencies should also work on improving accessibility and the presentation of their procedures and guidelines. Ensuring that information security coordinators within each department make efforts to reach out effectively with new documents can further help bridge the communication gap.

Personal contact and interaction with employees are other important aspects of communicating information security policies and regulations. Establishing relationships with employees, understanding their reality, and addressing their questions and concerns can lead to more effective communication. However, this may be challenging in large organizations where the number of people working with safety is small compared to the total number of employees. Some employees propose having information security officers or personnel that are easily accessible, as well as utilizing workshops to communicate policies and regulations more effectively. Incorporating real-life cases into these workshops can further help employees better understand and apply the information presented to them.

Clearer instructions and more comprehensible language in policy documents can also lead to better understanding and application of information security policies and regulations. Security experts should consider their target audience and ensure that the language used in these documents is accessible and easy to understand. Lastly, making it easier for employees to search for specific information in policies and regulations is a crucial improvement. Filtering through extensive documents can be time-consuming and frustrating, so streamlining the search process can greatly enhance the overall communication of information security policies and regulations within government agencies.

6.3 What are the attitudes of these government agencies' employees towards compliance with information security policies and regulations that they must adhere to?

This question is answered based on the experiences and recollections of the respondents from both top management or information security officers and regular employees.

6.3.1 General Attitude, Awareness and Culture

The overall attitude of employees towards information security policies and regulations is positive. Both top management and information security officers confirm that employees are generally cooperative and eager to comply with the policies once they understand the expectations. Some respondents also note that employees may find the regulations cumbersome and hindering to their work. However, the willingness to prioritize safety over convenience has increased in recent years, as the importance of information security has become more recognized.

Employee perspectives support these findings, with respondents emphasizing the importance of adhering to and complying with information security policies and regulations. Many employees understand the significance of their role within a government agency and the sensitive nature of the information they handle, further reinforcing their commitment to compliance.

Employees have a strong awareness of threats and policies, but their understanding of the policies and regulations varies. High levels of awareness can be attributed to the training employees have received, with some respondents also citing the integration of information security into many organizational activities. However, some employees

reported lower understanding of policies and regulations due to factors such as complex language, unclear instructions, and difficulty finding specific information amidst the large volume of available documents.

The data highlights a shift in information security culture from enforcement and negative messaging to support, assistance, and fostering a positive environment. This shift has led to a more efficient and effective culture, focused on managing and controlling the right aspects of security. Employees also report an open climate within their organizations, where mistakes are viewed as learning opportunities instead of grounds for punishment. Various communication methods, training, and safety days are used to create and anchor a culture of information security within these organizations. The interviewed authorities emphasize the importance of educating personnel in developing a culture that prioritizes information security and aids in transforming employees from being potential risks to being assets instead for the organization.

6.3.2 Compliance

The attitudes of government agencies' employees towards compliance with information security policies and regulations vary, but generally, they appear to be aware of their responsibilities and recognize the importance of adhering to these policies. However, employees face certain challenges in ensuring compliance, which may affect their attitudes towards these policies and regulations.

Employees rely on their training to ensure compliance and rarely refer to policies and regulations directly. They consult with colleagues or managers for guidance when facing issues rather than examining the policies and regulations themselves. This suggests that while employees may have a basic understanding of their responsibilities, there may be room for improvement in providing accessible resources and guidance to help them better understand and comply with these policies and regulations.

Challenges in understanding the language or terminology used in policies and regulations also affect employees' attitudes towards compliance. Several respondents express that the difficulty in comprehending the technical, legal, or safety terminology used in these documents poses a challenge to their own compliance with information security measures. This reinforces the need for simplifying and clarifying the language used in policies and regulations to make them more comprehensible and accessible to employees. Furthermore, employees may be overwhelmed by the amount of information they need to process, as mentioned by RE2, who finds certain information to be overwhelming and difficult to take in. This indicates that employees might struggle to maintain a comprehensive understanding of their responsibilities related to information security compliance.

To improve employee attitudes towards compliance, it is essential to address these challenges. This can be done by simplifying and clarifying the language used in policies and regulations, providing better resources and guidance, and understanding the realities of employees' day-to-day work. Additionally, strong support from top management can help to foster a positive attitude towards compliance, as they can demonstrate their commitment to information security by exhibiting appropriate

behaviour and providing incentives for good behaviour while enforcing consequences for negative behaviour.

6.3.3 Incidents and Incident Management

The attitudes of employees in government agencies towards compliance with information security policies and regulations appear to be mixed. While they acknowledge the importance of these policies and regulations, employees still perform actions that deviate from them. In the incidents reported, employees have made mistakes like clicking on suspicious links, opening email attachments, sending information to the wrong address, or storing sensitive information in inappropriate places. The reasons behind these mistakes include a desire for convenience, trying to be helpful, and lack of awareness. Although these mistakes are often minor, the respondents recognize that they can lead to severe consequences depending on the context. Major incidents have also occurred, including fraudsters obtaining sensitive information and employees accessing information for personal reasons. These incidents emphasize the need for vigilance and strict adherence to information security policies and regulations.

Regarding incident management, the organizations have systematic procedures in place that prioritize reporting, follow-up, and handling of incidents. They also encourage a non-judgmental approach, creating a safe environment where employees feel comfortable reporting incidents without fear of repercussions. This approach recognizes that everyone is capable of making mistakes and aims to minimize the stress caused by incidents. The organizations promote a culture of open communication, with mistakes being viewed as opportunities for growth and improvement. They proactively approach incident management through training, guidelines, and a supportive culture that minimizes the risk of incidents happening. This focus on learning and development, instead of punishment, encourages employees to comply with information security policies and regulations, ultimately reducing the likelihood of incidents occurring in the first place.

6.3.4 The Human Factor and Insider Threats

The attitudes of employees in these government agencies towards compliance with information security policies and regulations appear to be a mix of understanding, willingness, and occasional confusion or reluctance. The human factor and insider threats are significant concerns for the respondents, who emphasize the importance of a competent and united team. They recognize that even one weak link can affect the team's performance, and that providing education, awareness, and motivation is crucial for ensuring that employees understand and comply with information security policies and regulations.

Respondents also acknowledge that while external threats, such as hacking incidents, are on the rise, the human factor and insider threats should not be underestimated. They believe that most employees and managers want to do the right thing, but providing them with the tools and easy-to-understand explanations is essential for ensuring compliance. They also stress the importance of viewing mistakes as opportunities for learning and improvement as well as encouraging employees to take responsibility for their own education and understanding of information security.

6.3.5 Improvements

The respondents emphasize the importance of simplicity and clarity in regulations and instructions. By developing straightforward and easily comprehensible regulations, employees are more likely to comply and do the right thing. Examples of this approach include using tabular instructions to explain procedures and providing specific guidance and support for various assets, while also utilizing relatable examples from everyday life. The significance of providing employees with appropriate tools that are functional, relevant, and effective is also emphasized. Having the right tools in place is crucial for successfully improving employees' attitudes towards compliance.

Another approach to improving attitudes involves anchoring the importance of compliance within the organization. This can be achieved by encouraging collaboration and prioritizing the organization's greater good over individual projects. Educating employees about the benefits of governance and information security, as well as the consequences of non-compliance, can further help create a sense of responsibility. Employees need to understand why routines and safety measures are important, and by highlighting the negative consequences of non-compliance and the benefits of adhering to information security practices, they may be more likely to relate to the importance of compliance and adopt the desired attitudes and behaviours.

6.4 Summary

Government agencies develop information security policies and regulations through a systematic approach that accounts for their organizations' unique context and requirements. This process may be triggered by legal or regulatory requirements, changes in the threat landscape, technological advancements, or organizational restructuring. Key aspects of this approach include stakeholder engagement, adherence to legal requirements, and addressing the human factor. The development and implementation of information security policies involve risk assessment, stakeholder identification, setting security objectives, and continuous review, implementation, and maintenance of policies. Policies must be integrated into daily activities and procedures, and prioritizing employee awareness and training is crucial to effectively mitigate risks.

These government agencies communicate information security policies and regulations to employees using various channels, such as the intranet, through education and training, departmental information security coordinators, and theme days. However, the effectiveness of these channels is not systematically measured, and improvements are needed. Enhanced communication can be achieved by improving the ISMS for better accessibility, streamlining the policy document revision and modification process, emphasizing the importance of information security for all employees, and personalizing contact with employees. Additionally, providing clearer instructions, using comprehensible language, and streamlining the search process for specific information can enhance communication.

Employees of government agencies generally have a positive attitude towards compliance with information security policies and regulations. They understand the importance of their role in handling sensitive information and possess a strong awareness of threats and policies. However, their understanding of the policies varies,

with some employees facing challenges related to complex language and unclear instructions. The information security culture has shifted towards support and positive reinforcement, leading to a more effective culture focused on managing the right aspects of security.

The employees are generally aware of their responsibilities. They however, rely on their training and consult with colleagues or managers for guidance instead of referring directly to policies and regulations. Challenges in understanding the language and terminology used in policies affect employees' attitudes and compliance. To foster a positive attitude towards compliance, simplifying and clarifying language in policies, providing better resources and guidance, and ensuring strong support from top management are necessary. Incidents of non-compliance still occur, often due to mistakes or lack of awareness. Incident management focuses on reporting, follow-up, and handling incidents while fostering a non-judgmental and open environment, encouraging employees to report incidents without fear of repercussions. Addressing the human factor and insider threats are significant concerns, and providing education, awareness, and motivation is essential for compliance. Improvements can be made by simplifying regulations and instructions, offering functional and relevant tools, anchoring the importance of compliance within the organization, and educating employees about the benefits of compliance and consequences of non-compliance.

The purpose of this thesis was to enable government agencies improve their information security work, protect data more effectively, and enhance employee engagement in complying with regulations. This was achieved by answering the three aforementioned research questions (read chapter 3.1). By addressing each question, the answers provide results that give valuable insights into the processes involved in policy development, the strategies used for communicating these policies, and how employee compliance with information security policies and regulations is currently. The results also highlight potential improvements in the communication and compliance of information security policies and regulations within government agencies, which can enhance the effectiveness of their information security practices. The insights into possible improvements, combined with the findings from the research questions, contribute to a more comprehensive understanding of the factors influencing the effectiveness of information security policies and practices within government agencies. This knowledge can inform future research and help develop strategies to enhance information security in these societally critical organizations.

7 DISCUSSION

This chapter reflects on and discusses the study's research methodology, results, societal, scientific and ethical aspects, as well as provides suggestions for future research in the field.

7.1 Method

One of the key strengths of the qualitative method used in this study is its ability to provide rich, detailed, and contextualized information about the experiences and perspectives of participants (Berndtsson et al., 2008). By conducting semi-structured interviews with both top management or information security officers and regular employees, a wide range of perspectives and experiences on the development, communication, and compliance with information security policies and regulations was captured. This allowed for a more nuanced understanding of the challenges and successes faced by the government agencies in managing information security, which would not have been possible through quantitative methods. Another strength of the qualitative approach, particularly the use of semi-structured interviews, is its flexibility (Berndtsson et al., 2008). This format allowed for the exploration of topics that emerged during the interviews, which may not have been anticipated in the initial literature review.

However, the qualitative method also has some limitations that should be considered when interpreting the findings. One limitation is the potential for researcher bias to influence the data collection and analysis process. Although steps were taken to mitigate this risk, such as basing interview questions on the literature review, member checking, and using a systematic approach to the thematic analysis, it is important to acknowledge that personal biases could still impact the interpretation of the results. Another limitation of the study is the relatively small number of participants, which may limit the generalizability of the findings. Although the qualitative method is not focused on producing statistically representative data, the insights gained from this study may not necessarily apply to all government agencies or organizations and their employees. In this thesis, this limitation was mitigated through conducting long interviews, which allowed for the collection of rich data from the respondents. Future research could further address this limitation by conducting interviews with a larger and more diverse sample of participants, potentially including individuals from various government agencies, organizations and countries.

The respondents were also informed before the interviews of what questions would be asked. Providing the interview guide beforehand can potentially lead to rehearsed or overly polished answers, which can negatively impact the results. Participants may also be less likely to raise topics that are relevant to the research question but were not covered in the interview guide. In a sensitive topic like information security, employees may also feel pressured to provide answers that align with the views of their organization or superiors, which can be due to fear of repercussion for expressing their honest opinions.

7.2 Result

The findings reveal that government agencies primarily work systematically and collaboratively to develop these policies, involving multiple stakeholders to ensure the effectiveness and comprehensiveness of the regulations. The process is dynamic, with continuous improvement, adaptation, and evaluation being critical aspects that help agencies stay up to date with the ever-evolving threat landscape. Communication plays a vital role in disseminating information security policies and regulations to employees. The results highlight the use of intranets, training programs, education programs, and departmental information security coordinators as primary communication channels. These methods have proven effective in raising awareness and improving employees' knowledge about information security. However, the research also identifies the need for systematic measurement of communication effectiveness and suggests various improvements, such as simplifying language, tailoring messages, and prioritizing personal contact with employees.

The attitudes of employees towards compliance with information security policies and regulations are predominantly positive, with most employees recognizing the importance of adhering to these guidelines. Despite this positive outlook however, employees' understanding and knowledge of policies and regulations vary, presenting obstacles to successful compliance. To fully capitalize on the positive attitude and ensure effective compliance, the research suggests that the organizations should address these challenges and focus on improving employees' understanding of the policies. Employee awareness and understanding of threats, policies, and regulations are key to fostering a strong information security culture. The findings suggest that although employees have a high level of threat and policy awareness, their understanding of regulations varies due to factors such as language complexity and unclear instructions. Therefore, simplifying regulations and providing clearer instructions are essential to improve employees' understanding and compliance.

The results also highlight a shift towards a more supportive and positive information security culture, moving away from a strictly punitive approach. This change encourages open communication, learning from mistakes, and fostering personal responsibility. To further develop this culture, a combination of training, communication methods, and early integration of information security principles for new employees is recommended. Various approaches are employed by organizations to ensure compliance with information security policies and regulations. Some respondents mentioned shifting from being enforcers to helpers and supporters, allowing them to focus on pertinent issues. Others emphasized incorporating security measures throughout the development process or evaluating the organization's performance using models like CMMI. Workplace culture, follow-up surveys, and incident statistics also play a role in maintaining compliance.

The results further acknowledge the human factor as a significant threat and emphasizes the importance of managing insider threats through monitoring permissions, implementing technical solutions, and ensuring responsible use of logging systems. Furthermore, the results suggest that investment in the human factor is as important as investing in technology and control.

While the study offers valuable insights, it is essential to acknowledge the limitations of the results. One limitation is the variability in employee responses due to the qualitative nature of the interviews. This could lead to potential biases or inconsistencies in the data. Furthermore, the results are based on employees' self-reported attitudes and experiences, which may not accurately reflect their actual behaviour or the organization's reality. This self-reporting bias might have led to an overemphasis on positive attitudes or an underreporting of negative experiences. Another limitation is the small sample size, which might not have captured the full range of perspectives across different government agencies, job roles, and levels of seniority. As a result, and as previously mentioned, the study's findings may not be generalizable to all government agency employees. Additionally, the results might be influenced by factors such as the specific organizational culture, leadership styles, and environmental differences in information security regulations.

Another important aspect of the results and a possible limitation to take into consideration is the concept of effectiveness in relation to information security policies and communication, which is multifaceted and somewhat elusive. In this research, effectiveness is specifically defined according to Höne and Eloff's (2002b) definition, which states that effectiveness is achieved when an information security policy communicates expectations for handling information resources in a clear and easily understood manner, with emphasis being on the content and its communication. However, this definition cannot be applied to all research and all organizations, as its determination is often contingent on the context and criteria set by the entity making the assessment. Effectiveness could be interpreted in numerous ways, from policy adherence, reduction in security incidents, to improved awareness among users. This plurality of interpretation introduces a subjectivity that is inherent in the definition and assessment of effectiveness. It is also important to acknowledge that what is deemed effective from the viewpoint of top management or information security officers may not be perceived as such by an employee or from the perspective of an external auditor (Siponen, Mahmood & Pahnila, 2014). The subjective and context-dependent nature of effectiveness means that results drawn under one specific definition or set of circumstances might not be applicable or provide the same insights in a different setting.

Effectiveness is also usually not a binary state, but rather it exists on a continuum. It can, for example, be a spectrum ranging from wholly ineffective to highly effective, with many nuances in between. There is no clear line dividing effective and ineffective, but rather a sliding scale that depends on specific metrics and performance indicators. It's also vital to note that effectiveness might be contextual and temporal, where a policy or communication strategy is effective in one context or time period but less effective in another (Ifinedo, 2012). Findings may therefore vary significantly when different indicators are used to measure effectiveness. This should be taken into consideration when extrapolating these results to different contexts or when comparing them to studies using different definitions or measures of effectiveness.

7.3 Societal Aspects

As government agencies handle a vast amount of sensitive and confidential data, ensuring the security and protection of this information is crucial to maintain public trust and safeguard the interests of citizens. In this digital age, information security has

become a primary concern for societies across the globe. Cyber threats are constantly evolving, making it increasingly important for government agencies to adopt robust information security measures. By implementing comprehensive policies and regulations, these authorities can prevent unauthorized access to sensitive data and mitigate the risks associated not only with cyberattacks, but also threats posed by insiders. In turn, this enhances the overall security of nations and contributes to a safer digital environment for all citizens.

One key societal implication is the importance of fostering a strong information security culture within government agencies. The results show that employees' attitudes towards compliance with information security policies and regulations are predominantly positive, which can contribute to the establishment of a security culture that prioritizes the protection of sensitive information. However, to fully capitalize on this positive attitude, agencies should address challenges related to employees' understanding and knowledge of policies and regulations. By doing so, government agencies can ensure that employees are well-equipped to safeguard sensitive information and contribute to a secure digital society. Another significant aspect is the need for effective communication and collaboration between various stakeholders, including government agencies, employees, and the general public. Communication plays a vital role in disseminating information security policies and regulations to employees, raising awareness, and improving knowledge about information security. By enhancing communication methods and tailoring messages to make them more relevant and meaningful, government agencies can ensure that employees understand the importance of their role in maintaining information security and fostering a secure digital environment.

The results also emphasize the importance of balancing security with usability, especially in the context of compliance with information security policies and regulations. Simplifying policies, adapting them to employees' realities, and addressing language barriers can help overcome some of the challenges faced by employees in understanding and complying with these regulations. By striking this balance, government agencies can set examples for other sectors and create an environment that encourages compliance and prevents incidents from occurring in the first place.

7.4 Scientific Aspects

Research on the development, communication, and compliance with information security policies and regulations within government agencies offers valuable insights into the scientific aspects of information security. These findings contribute to an expanding body of knowledge on best practices for devising, conveying, and implementing information security measures across organizations. Since government agencies often serve as models in the field, understanding their methods can inform other organizations and promote the study of information security.

However, research specifically focusing on information security within government agencies is limited. This study involved interviews with 11 respondents, which may not provide a sufficient foundation. The participants came from different government agencies operating in various areas, potentially reducing the generalizability of the results. While respondents shared similar approaches, such as a systematic method for developing information security policies, involving many organizational components in

the process, and using comparable communication channels to disseminate governing documents, there were notable differences in some responses. This study can therefore be supplemented with research on a larger and more diverse sample of government agencies, focusing on specific sectors or domains, to enhance the generalizability and applicability of the findings.

7.5 Ethical Aspects

In order to address the research questions, interviews were conducted with government agency employees holding various roles. Given the sensitive nature of the study, adherence to the four research ethics aspects (read chapter 4.2.4) was crucial. This had multiple positive outcomes. Trust was established with the respondents, leading to more reliable and valid responses. Obtaining informed consent ensured that participants felt comfortable sharing their genuine opinions without experiencing pressure or coercion. Additionally, by informing participants about the confidential handling of their data and guaranteeing their anonymity, they were more inclined to disclose sensitive information. Adhering to these research ethics aspects not only yielded credible results but also enhanced the overall credibility of the study. However, one drawback of adhering to the research ethics aspects was the time-consuming and resource-intensive nature of the process, which consequently limited the scope of the study and lead to potentially important information not being collected during the interviews.

As for the study results, the ethical aspects of information security policies and regulations in government agencies are crucial to consider, as they impact not only the organizations themselves but also the wider society that they serve. This study provides an opportunity to examine the ethical implications of government agencies' practices and the potential consequences of non-compliance. One key ethical aspect is the responsibility of government agencies to protect sensitive and confidential information. As organizations that handle a vast amount of personal data, government agencies have an ethical obligation to ensure that the information they manage is secure and safeguarded against potential breaches. Failure to do so could result in significant harm to individuals whose data is compromised, as well as to the reputation and trustworthiness of the government agency involved.

The results highlight the importance of fostering a culture of compliance and personal responsibility within the government agencies to meet this ethical obligation. By promoting a positive attitude towards information security and ensuring that employees understand the importance of adhering to policies and regulations, organizations can create an environment that prioritizes the protection of sensitive information. This focus on culture and personal responsibility helps to minimize the risk of data breaches and supports the ethical duty of government agencies to protect the information they hold.

Another ethical aspect is the transparency and openness of government agencies in their information security practices. The research reveals a shift towards a more supportive and positive information security culture, moving away from a strictly punitive approach. This encourages open communication, learning from mistakes, and fostering personal responsibility. By adopting a non-judgmental approach to handling incidents and emphasizing education and development over punishment, government agencies can create a culture that values transparency and continuous improvement. This

ethically sound approach allows employees to learn from their mistakes and contribute to a more secure environment. The results also underscore the need for accessible, coherent, and understandable information security policies and regulations. Government agencies have an ethical obligation to ensure that employees can easily comprehend and navigate these policies, as this directly impacts their ability to comply with them. By simplifying language, providing clear instructions, and making policies easier to navigate through, government agencies can support their employees in understanding and adhering to information security requirements.

Finally, the results highlight the importance of addressing the human factor in information security. Ethically, it is essential to invest in education and awareness to ensure that employees fully understand the implications of their actions and the potential consequences of non-compliance.

7.6 Future Research

This thesis provides valuable insights into current practices and challenges in information security. However, there is always room for further exploration and understanding, particularly as technology and the threat landscape continue to evolve. Future research in this area could focus on several key areas to help government agencies improve their information security practices and better protect sensitive information.

One potential area of research is the creation of innovative and more efficient methods for conveying information security policies and regulations to employees. Existing communication channels sometimes fall short in ensuring comprehensive understanding and compliance with information security requirements. Exploring new approaches, such as the use of gamification, interactive learning modules, or personalized training programs, could enable government agencies to engage employees more effectively and heighten information security awareness.

Assessing the efficacy of various information security practices, policies, and regulations also warrants further exploration. Many government agencies do not directly measure the effectiveness of their communication channels, often relying on follow-ups and assessments for mere indications. Establishing more accurate and robust evaluation methods for gauging the impact of information security policies and practices on employee behaviour and overall security posture could help organizations pinpoint areas requiring improvement and apply targeted interventions.

The results highlight the use of models and assessment tools like the CMMI. While these instruments aid organizations in evaluating their information security practices and identifying areas needing improvement, there is a notable absence of tools for assessing communication channels and outreach efforts. This gap suggests an opportunity for advancing research and development of evaluation methods in this area. Developing and validating new tools and models for assessing information security communication effectiveness could substantially progress the field and offer organizations valuable insights to refine their practices.

Delving deeper into the factors that contribute to a positive information security culture within government agencies is also essential. The results reveal that a supportive and non-judgmental approach to incident handling can be more effective than punishment in encouraging employee compliance with information security policies and regulations. A more thorough understanding of specific contributing factors to a robust information security culture, such as leadership styles, employee engagement, and organizational values, could enable government agencies to devise targeted interventions to bolster their security culture.

One of the important steps in the communication of policies, according to the literature, is the monitoring of compliance. This is not particularly mentioned by the respondents. However, monitoring can give rise to several problems, such as potential impacts on employee trust and morale. While monitoring can enhance policy compliance and promote security, it may also give rise to feelings of distrust if not properly implemented, thereby potentially affecting productivity and the work environment negatively. This dual nature of monitoring presents a compelling case for future research. The concept of trust, a significant aspect in organizational settings, can be a standalone research area, particularly in relation to its impact on information security. Future studies could delve into how different monitoring strategies influence employees' trust levels, perception, and behaviour, and how these factors subsequently shape their attitude towards information security and overall job satisfaction. Such understanding could assist organizations in establishing monitoring practices that ensure policy compliance while also fostering a trustful and positively engaged workforce.

Lastly, future research should investigate the long-term influence of enhanced information security practices on overall trust and confidence in government agencies to emphasize the benefits of operating securely. As government agencies manage sensitive data and provide crucial services, maintaining public trust is vital. Studying the relationship between information security practices, employee behaviour, and public trust could yield valuable insights for government agencies striving to improve their reputation and retain the confidence of the citizens they serve.

REFERENCES

Books

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2008). *Thesis Projects: A Guide for Students in Computer Science and Information System,* Second Edition, London: Springer.

Braun, V. & Clarke, V. (2022). *Thematic analysis: a practical guide*. SAGE Publications.

Hermerén, G. (2017). *Good research practice*. Stockholm: The Swedish Research Council.

Herold, R. & Hertzog, C. (2015). Data Privacy for the Smart Grid. Auerbach Publications.

Howard, P. (2003). The security policy life cycle: functions and responsibilities. In: Tipton, H., Krause, M. (Eds.), Information Security Management Handbook, 4th edition. 999CRC Press, LLC, Boca Raton.

Patton, M. Q. (2015). *Qualitative research & evaluation methods: integrating theory and practice: the definitive text of qualitative inquiry frameworks and options*. 4th ed., SAGE Publications Inc.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. 7th edition., Cengage learning.

Zinatullin, L. (2016). *The Psychology of Information Security: Resolving Conflicts Between Security Compliance and Human Behaviour*. IT Governance Ltd.

Scientific Papers

Al Zaabi, K. & Tubaishat, A. (2015). Security Awareness Program for Customers Using Online Banking. *GSTF Journal on Computing (JOC)*, 4(3), pp. 80-89. doi:10.7603/s40601-014-0019-3

AlKalbani, A., Deng, H., Kam, B. & Zhang, X. (2017). Information Security Compliance in Organizations: An Institutional Perspective. *Data & Information Management*, 1(2), pp. 104–114. doi:10.1515/dim-2017-0006

Alotaibi, M., Furnell, S. & Clarke, N. (2016). Information Security Policies: A Review of Challenges and Influencing Factors. *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST),* pp. 352-358. doi:10.1109/ICITST.2016.7856729

Aloul F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology*, 3(3), pp. 176-183. doi:10.4304/jait.3.3.176-183

Amankwa, E., Loock, M. & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference For*, pp. 248–252. doi:10.1109/ICITST.2014.7038814

Askarzai, W. & Unhelkar, B. (2017). Research Methodologies: An Extensive Overview, *International Journal of Science and Research Methodology,* 6(4), p. 21-42.

Baker, W. H. & Wallace, L. (2007). Is Information Security Under Control?: Investigating Quality in Information Security Management. *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Secur. Privacy*, 5(1), pp. 36–44. doi:10.1109/MSP.2007.11

Bauer, S., Bernroider, E. & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security*, 68, pp. 145-159. doi:10.1016/j.cose.2017.04.009

Baumbusch, J. (2010). Semi-Structured Interviewing in Practice-Close Research. *Journal for Specialists in Pediatric Nursing*, 15(3), pp. 255–258. doi:10.1111/j.1744-6155.2010.00243.x

Carroll, M. D. (2006). Information security: examining and managing the insider threat. *Proceedings of the 3rd annual conference on Information security curriculum development*, pp. 156-158. doi:10.1145/1231047.1231082

Caspi, A., Roberts, B. W. & Shiner, R. L. (2005). PERSONALITY DEVELOPMENT: Stability and Change. *Annual Review of Psychology*, 56(1), pp. 453–484. doi:10.1146/annurev.psych.55.090902.14191

Chen, C. C., Shaw, R. S. & Yang, S. C. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning & Performance Journal*, 24(1), pp. 1–14.

Cheng, L., Liu, F. & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *WIREs: Data Mining & Knowledge Discovery*, 7(5), pp. 1-14. doi:10.1002/widm.1211

Coles-Kemp, L. & Theoharidou, M. (2010) Insider Threat and Information Security Management. *Advances in Information Security,* 49, pp. 45-71. doi:10.1007/978-1-4419-7133-3_3.

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days?. *Information Security Technical Report*, 14(4), pp. 186–196. doi:10.1016/j.istr.2010.04.004.

Corriss, L. (2010). Information security governance. *Proceedings of the 2010 Workshop: Governance of Technology, Information & Policies*, pp. 35–41. doi:10.1145/1920320.1920326

Da Veiga, A. & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, 29(2), pp. 196–207. doi:10.1016/j.cose.2009.09.002

Dawes, S.S. (2009). Governance in the digital age: A research and action framework for an uncertain future, *Government Information Quarterly*, 26(2), pp. 257–264. doi:10.1016/j.giq.2008.12.003.

Elmrabit, N., Yang, S.-H. & Yang, L. (2015). Insider threats in information security categories and approaches, *2015 21st International Conference on Automation & Computing (ICAC)*, pp. 1–6. doi:10.1109/IConAC.2015.7313979.

Flowerday, S.V. & Tuyikeze, T. (2016) 'Information security policy development and implementation: The what, how and who', *Computers & Security*, 61, pp. 169–183. doi:10.1016/j.cose.2016.06.002.

Georgiadou, A., Mouzakitis, S. & Askounis, D. (2022). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, 35, pp. 486–505. doi:10.1057/s41284-021-00286-2

Gerber, M. & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*, 27(5/6), pp. 124–135. doi:10.1016/j.cose.2008.07.009

Heeks, R. & Stanforth, C. (2007). Understanding e-Government project trajectories from an actor-network perspective', *European Journal of Information Systems*, 16(2), pp. 165–177. doi:10.1057/palgrave.ejis.3000676

Höne, K. & Eloff, J. H. P. (2002a). Information security policy — what do international information security standards say?. *Computers & Security*, 21(5), pp. 402-409. doi:10.1016/S0167-4048(02)00504-7

Höne, K. & Eloff, J. H. P. (2002b). What Makes an Effective Information Security Policy?. *Network Security*, 2002(6), pp. 14-16. doi:10.1016/S1353-4858(02)06011-7

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), pp. 83–95. doi-org.libraryproxy.his.se/10.1016/j.cose.2011.10.007

Ismail, W. B. W., Widyarto, S., Adiyarta, K., Syafrullah, M., & Tajuddin, L. M. (2022). An Information Security Policy Development Process in Higher Education Institution: A Case Study Approach. *2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Electrical Engineering, Computer Science and Informatics (EECSI), 2022 9th International Conference On*, pp. 147–152. doi:10.23919/EECSI56542.2022.9946593

Ismail, W. B. W., Widyarto, S., Ahmad, R. A. T. R. & Ghani, K. A. (2017). A generic framework for information security policy development. *2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Electrical Engineering, Computer Science and Informatics (EECSI), 2017 4th International Conference On*, pp. 1–6. doi:10.1109/EECSI.2017.8239132

Knapp, K. J., Franklin Morris, R., Marshall, T. E. & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, 28(7), pp. 493–508. doi:10.1016/j.cose.2009.07.001

Knopf, J. (2006). Doing a Literature Review. *PS: Political Science & Politics*, 39(1), pp. 127-132. doi:10.1017/S1049096506060264

Koza, E. (2022). Semantic Analysis of ISO/IEC 27000 Standard Series and NIST Cybersecurity Framework to Outline Differences and Consistencies in the Context of Operational and Strategic Information Security. *Medicon Engineering Themes*, 2, pp. 26-39.

Kwon, J. & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, 38, pp.451-471. doi:10.25300/MISQ/2014/38.2.06.

Lopes, I. M., Guarda, T. & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. *2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Information Systems and Technologies (CISTI), 2019 14th Iberian Conference On*, pp. 1–6. doi:10.23919/CISTI.2019.8760937

Mazzarolo, G., & Jurcut, A. D. (2019). Insider threats in Cyber Security: The enemy within the gates. *ArXiv*. doi:10.48550/arXiv.1911.09575

Merriam, S. B. (1995). N of 1?: Issues of Validity and Reliability in Qualitative Research. *PAACE Journal of Lifelong Learning,* 4, pp. 51-60.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. & Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. *Procedia – Social and Behavioral Sciences*, 147, pp. 424-428. doi:10.1016/j.sbspro.2014.07.133

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, 88*,* pp. 1-14. doi:10.1016/j.cose.2019.101608

Rees, J., Bandyopadhyay, S. & Spafford, E. H. (2003). PFIRES: A Policy Framework for Information Security. *Communications of the ACM*, 46(7), pp. 101–106. doi:10.1145/792704.792706

Safa, N.S., von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, pp. 70–82. doi:10.1016/j.cose.2015.10.006

Safa, N.S., von Solms, R. & Futcher, L. (2016). Human aspects of information security in organizations. *Computer Fraud & Security*, 2016(2), pp. 15–18. doi:10.1016/S1361-3723(16)30017-3.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), pp. 217–224. doi.org/10.1016/j.im.2013.08.006

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. *International Cybersecurity Law Review*. 1, pp. 51-61. doi:10.1365/s43439-020-00014-3

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security*, 3(2), pp. 20-26. doi:10.1108/09685229510792988

Thomson, M.E. & von Solms, R. (1998). Information security awareness: educating your users effectively, *Information Management & Computer Security*, 6(4), pp. 167-173. doi:10.1108/09685229810227649

Tu, Z. & Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management: A Literature Review Completed Research Paper. *20th Americas Conference on Information Systems 2014,* 1, pp. 1874-1886. doi:10.1.1.819.6637

van Niekerk, J. & von Solms, R. (2005). A holistic framework for the fostering of an information security sub-culture in organizations. *Proceedings of the ISSA 2005 New Knowledge Today Conference*, pp. 1-13.

Van Niekerk, J. F. & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, 29(4), pp. 476–486. doi:10.1016/j.cose.2009.10.005

von Solms, R. & van Niekerk, J. (2013) From information security to cyber security, *Computers & Security*, 38, pp. 97–102. doi:10.1016/j.cose.2013.04.004.

Walton, R. & Limited, W.-M. (2006). Balancing the insider and outsider threat. *Computer Fraud & Security*, 2006(11), pp. 8–11. doi:10.1016/S1361-3723(06)70440-7

Wolff, J. & Atallah, N. (2021). EARLY GDPR PENALTIES: Analysis of Implementation and Fines Through May 2020. *Journal of Information Policy*, 11, pp. 63–103. doi:10.5325/jinfopoli.11.2021.0063

Standards

International Organization for Standardization (ISO) (2004). *ISO 14001:2004.* Environmental management systems — Requirements with guidance for use. ISO.

International Organization for Standardization (ISO) (2013). *ISO/IEC 27001:2013.* Information technology – Information security management systems - Requirements. ISO.

International Organization for Standardization (ISO) (2018). *ISO/IEC 27000:2018.* Information technology — Security techniques — Information security management systems — Overview and vocabulary. ISO.

International Organization for Standardization (ISO) (2022). *ISO/IEC 27002:2022.* Information security, cybersecurity and privacy protection — Information security controls. ISO.

Statutes and Regulations

MSBFS 2020:6. *The Swedish Civil Contingencies Agency's regulations on information security for government authorities [Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter]*. Swedish Civil Contingencies Agency (MSB).

MSBFS 2020:7. *The Swedish Civil Contingencies Agency's regulations on security measures in information systems for government authorities [Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter]*. Swedish Civil Contingencies Agency (MSB).

SFS 2018:585. *Security Protection Act [Säkerhetsskyddslag]*. The Swedish Riksdag.

SFS 2009:400. *Public Access to Information and Secrecy Act [Offentlighets- och sekretesslag]*. The Swedish Riksdag.

Websites

All European Academies (ALLEA) (2017). *The European Code of Conduct for Research Integrity*. Berlin: All European Academies. Available at: https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf (Accessed: 2023-02-08).

European Union Agency for Cybersecurity (ENISA) (n.d.). *CMMI*. https://www.enisa.europa.eu/topics/risk-management/current-risk/business-process-integration/operational-it-processes/cmmi [2023-03-28]

Swedish Civil Contingencies Agency (MSB) (2002a). *The Information Security Check [Infosäkkollen]*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/infosakkollen/ [2023-03-28]

Swedish Civil Contingencies Agency (MSB) (2022b). *The Information Security Month [Informationssäkerhetsmånaden].* https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/informationssakerhetsmanaden [2023-03-28]

Swedish Research Council. (2002). *Research-ethics principles in humanistic-social scientific research [Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning]*. Stockholm: Swedish Research Council. Available at: https://www.vr.se/analys/rapporter/vara-rapporter/2002-01-08-forskningsetiska-principer-inom-humanistisk-samhallsvetenskaplig-forskning.html (Accessed: 2023-02-08)

APPENDIX A: INTERVIEW INVITATION

Hi.

My name is Osama Abdulhadi and I am studying my last year of the Systems Science programme at the University of Skövde. I am currently writing my degree project and as part of my degree project I am conducting a study on information security in government agencies and I would like to invite you to participate in an interview.

The purpose of this study is to gain knowledge on how government agencies work to develop and enforce information security policies and regulations and to identify challenges these agencies face in communicating and enforcing these policies and regulations. Your participation and insights as an employee of a government agency would be greatly appreciated.

The interview will be anonymous and apart from your position within the organisation, no identifying information will be presented in the thesis, either personal or related to the organisation that you represent. The interview is expected to last approximately 60 minutes and will be conducted either in person or via any online communication software such as Zoom. Whichever suits you best. The interview will be audio recorded and the recording will be permanently deleted after the completion of the study.

I want to interview both someone responsible for information security and an employee with no information security role who can answer questions about how information security is perceived. The questions that will be asked to you are about your views on the development of information security policies and guidelines, how these are communicated to employees and how the employees adopt them.

I am very grateful if you want to participate in this study. Please send me an email with your interest in participating no later than the _____.

Kind regards

Osama Abdulhadi

APPENDIX B: INTERVIEW INFORMATION AND TERMS

Before we start the interview, I just wanted to inform you about the purpose of the study again and just bring up some more information about it.

The purpose of the study is to gain knowledge on how government agencies work to develop and enforce information security policies and regulations and to identify challenges these agencies face in communication, enforcement and compliance with them. The main focus of the thesis is on the human factor in information security.

- The interview will be completely anonymous, meaning that no identifying information about you or the organisation you represent will be included in the work. The only thing that may be mentioned is your role.
- You have the right to choose not to answer any specific question for any reason and you have the right to cancel the interview at any time.
- All information collected will be treated confidentially and will only be used for academic purposes.
- The interview will be recorded in audio format. The interview will then be transcribed and translated into English.
- The transcribed and translated interview will be sent to you for verification that it is consistent with what was said today. The data collected will not be used in the thesis until I have gotten your approval. Once the interview has been transcribed and translated, the recording will be deleted.

Given this information, do you still wish to continue with the interview?

APPENDIX C: INTERVIEW GUIDE – MANAGEMENT & IS-PERSONNEL

Introductory Questions

- Can you briefly describe your role and responsibilities within the organisation?
- How long have you been working in your current role?

Development

- Can you describe the process that your organisation goes through to develop information security policies and regulations for information security?
- Which people within the organization are involved in the development of information security policies and regulations?
- How does your policies and regulations deal with the human factor and insider threats in information security?
- In the literature, different researchers and experts address different steps that are important in the development of information security policies. If you could choose a few steps that you personally believe need to be taken when developing information security policies, what would they be?

Communication

- Can you describe the communication channels used to communicate information security rules and policies to employees?
- How do you measure the effectiveness of these communication channels?
- If possible, can you describe what training or awareness programs are in place to help employees understand and comply with information security policies and regulations?
- How do you think the communication of information security policies and regulations could be improved in your organisation?

Employee Attitudes

- How do employees in your organization typically respond to and comply with information security policies and regulations?
- How does your organization ensure that these policies and regulations are followed?
- Can you discuss specific challenges or obstacles that your organization has encountered in ensuring compliance with information security policies and regulations?
- Can you give examples of information security incidents that have been prevented due to employee compliance with policies and regulations?
- If possible, can you give examples of information security incidents that have occurred due to employees not following policies and regulations and if so, how did you deal with them?
- In your opinion, what are the main challenges in ensuring compliance with information security policies and regulations in your organisation?

- How do you think employee attitudes and behaviour regarding information security can be improved in your organisation?
- What is your view on the human factor and the insider threat in information security?
- Do you think I missed asking about something you think is important?

APPENDIX D: INTERVIEW GUIDE – EMPLOYEES

Introductory Questions

- Can you briefly describe your role and responsibilities within the organization?
- How long have you been working in your current role?
- How would you rate your awareness of your organization's policies and regulations on a scale of 1 to 5, with 1 indicating minimal awareness and 5 indicating exceptional awareness? Please provide an explanation for your rating.
- How would you rate your awareness of information security threats towards you and your organization on a scale of 1 to 5, with 1 indicating minimal awareness and 5 indicating exceptional awareness? Please provide an explanation for your rating.
- How would you rate your understanding of your organization's policies and regulations on a scale of 1 to 5, with 1 indicating an inadequate understanding and 5 indicating a profound understanding? Please provide an explanation for your rating.

Communication

- How were you informed about your organization's policies and regulations?
- Do you feel that these policies and regulations were clear and easy to understand?
- Have you received any training or awareness training on information security policies and regulations? If so, how do you perceive the effectiveness of the education/training for your understanding and compliance with these policies?
- Can you describe any suggestions or improvements you would suggest for the communication and application of information security policies and regulations in your organization?

Employee Attitudes

- Can you describe your understanding and awareness of your organization's information security policies and regulations?
- Can you give examples of policies and regulations that your organization has for handling sensitive data?
- Have you ever had any concerns or questions about these?
- How do you ensure compliance with these policies and regulations in your daily work?
- Have you personally ever had any incidents of non-compliance with information security policies and regulations? If so, can you describe the situation and the outcome?
- Have you ever been aware of a colleague not complying with information security policies and regulations? If so, how did you handle the situation?

- What do you think about the importance of following information security policies and regulations in your work?
- Have you ever become aware of any incidents of insider threats in your organization?
- Do you feel that you have received sufficient education and training on these policies and regulations?
- Have you ever found yourself in a situation where you were unsure how to comply with a particular policy or regulation? How did you handle it?