Master Degree Project

Development of a Guideline for Cybersecurity Awareness-Raising in Large Swedish Public Organizations

A Design Science Project

Felicia Burvall

Master's Degree Project in Informatics
Second Cycle 30 Credits
Spring term 2023

Supervisor: Joakim Kävrestad
Examiner: Marcus Nohlberg

Abstract

Technological advancement has significantly impacted people and organizations during the last decade. Society is exposed to an increasing rate of cyber-attacks utilizing sophisticated tools to accomplish their objectives. Previously attackers' primary focus was exploiting technological vulnerabilities to access organizations' information; however, attackers have shifted their focus to exploiting the vulnerabilities in people's human nature instead. This has resulted in organizations acknowledging that technical security measures alone are insufficient in providing adequate protection for organizations and need to invest in mitigating the risk people pose to an organization's cybersecurity. Thus realizing the need to address cybersecurity's social-technical nature. Organizations have begun implementing cybersecurity awareness-raising initiatives to increase people's cybersecurity awareness to reduce human-instigated breaches. This is especially crucial for organizations in the public sector to achieve because they tend to produce more destructive and widespread repercussions to society. To provide organizations in the public sector with the means to achieve good cybersecurity awareness, this thesis aims to develop a guideline for managers in large Swedish public organizations to assist them in their complex cybersecurity awareness-raising endeavors. The thesis employs a design science research strategy to develop, evaluate, and validate the guideline with the assistance of cybersecurity awareness experts. The results show six principal factors have been established as significant for raising cybersecurity awareness in large Swedish public organizations. These factors range from user-oriented, managerial, and technical, supporting the assertion that cybersecurity is a complex socio-technical matter. The key contribution of this thesis is to introduce a highly abstract guideline to enhance large Swedish public organizations' cybersecurity awareness efforts.

Keywords: Cybersecurity Awareness (CSA), Cybersecurity Awareness-Raising, Design Science Research (DSR), Guideline Development, Large Swedish Public Organization

Contents

1 Introduction **1**
- 1.1 Problem Definition & Aim . . . 3
- 1.2 Research Question . . . 4
- 1.3 Delimitations . . . 4

2 Background **5**
- 2.1 Cybersecurity . . . 5
  - 2.1.1 Cybersecurity in Public Sector . . . 6
- 2.2 Human Factors in Cybersecurity . . . 7
  - 2.2.1 Social Engineering Threats . . . 8
  - 2.2.2 Cyber Hygiene . . . 9
- 2.3 Cybersecurity Awareness-Raising . . . 9
  - 2.3.1 Cybersecurity Awareness Training . . . 10
  - 2.3.2 Criticisms Against Awareness Training . . . 10
  - 2.3.3 Factors Beyond Training That Raises Cybersecurity Awareness . . . 11

3 Method **14**
- 3.1 Design Science Research . . . 14
- 3.2 Implementation of Design Science Research Framework . . . 16
- 3.3 Supporting Data Collection Methods . . . 18
  - 3.3.1 Selective Literature Review . . . 18
  - 3.3.2 Interviews . . . 19
- 3.4 Ethical Considerations . . . 22

4 Result **23**
- 4.1 Design Science Cycle 1 . . . 23
  - 4.1.1 Method Development . . . 23
  - 4.1.2 Artefact Demonstration . . . 28
  - 4.1.3 Evaluation . . . 29
- 4.2 Design Science Cycle 2 . . . 34
  - 4.2.1 Method Development . . . 35
  - 4.2.2 Artefact Demonstration . . . 36
  - 4.2.3 Evaluation . . . 37
- 4.3 Communication of the Final Results . . . 44
  - 4.3.1 Top Management Support . . . 46
  - 4.3.2 User Attitudes & Perceptions of Cybersecurity . . . 47
  - 4.3.3 Cybersecurity Advocates . . . 48

4.3.4 User Participation, Engagement & Motivation 49
4.3.5 Governance 51
4.3.6 Cybersecurity Education, Training & Awareness 52

5 Discussion **54**
5.1 Main Results 54
5.2 Research Contributions 57
5.3 Scientific Quality 58
5.4 Research Validity 60
5.5 Ethical Considerations 61

6 Conclusion **64**
6.1 Revisiting Aims & Objectives 64
6.2 Revisiting Research Contributions 65
6.3 Limitations & Future Research 65

References **I**

A Appendix: Guideline's First Draft in Design Cycle One **II**

B Appendix: Interview Questions in Design Cycle One **IV**

C Appendix: Guideline's Second Draft in Design Cycle Two **VII**

D Appendix: Interview Questions in Design Cycle Two **IX**

E Appendix: Guideline's Final Result **XI**

1 | Introduction

This chapter presents an introduction to the chosen subject of this thesis along with the problem definition, research aim, research question, delimitations, and an outline of how this thesis is structured.

Nowadays, living without the aid of information technology seems unthinkable as more than half of the earth's population are frequent internet users (Kovačević et al., 2020). During the latest decade, there has been a high demand for the ability to have easy access to technology and online connectivity, so much so that technologies are incorporated into essentially everything in use. This has created high internet consumption and prompted technological advancement affecting individuals and organizations, exposing people to countless security threats they would not have encountered in previous years. Despite people's adoption of technology in their daily life, they often are less unaware of the threats they can face when using various technologies (Zwilling et al., 2022). One could say that cybersecurity awareness (CSA) is the first line of defense of information systems and networks (Tasevski, 2016). However, the average user is often uneducated regarding the technical aspects of the technology they use while seemingly being an expert at how it can be used. As such, the average user has little to no awareness of how to obtain good cybersecurity for securing their devices against unauthorized access or attack. This entails not being able to recognize security problems that arise or how to deal with them appropriately (Kovačević et al., 2020). For instance, many computer users have some knowledge concerning stories of cyber-attacks and comprehend they threaten the confidentiality of the computer's data. However, many of these users remain unsure of how to keep their data secure and are unaware of how their insecure behavior can contribute to a systems compromise (Korovessis et al., 2017).

A lack of CSA in users creates extensive vulnerabilities but also creates opportunities for adversaries to exploit these vulnerabilities for whatever nefarious purposes they have (Kovačević et al., 2020). This is occurring due to a shift that has happened from the attackers' point of view. Previously attackers focused more on attacking operating systems and program applications and the like to find vulnerabilities to gain access to information systems and their sensitive data. However, as the technical side is more heavily protected against intruders nowadays, attackers have begun to focus their attention on human factors instead. This shift can be attributed to attackers choosing paths of least resistance; in many cases, those paths are unintentional vulnerabilities created by people. Cyber-attacks with the primary focus on taking advantage of the vulnerabilities the human factor presents steadily increase (Abawajy, 2014). Attacks targeting people are constantly evolving and increasing in frequency. Because of this, organizations are beginning to comprehend the importance of not undervaluing the human factor's influence on an organization's security (Abawajy, 2014). Therefore, CSA has become an urgent priority for organizations worldwide to be effectively developed due to the ongoing cyber-attacks, hacks, and breaches that will undoubtedly continue to rise in frequency, sophistication, and

cost. The urgency to raise CSA among users within organizations often depends on the view that people are considered the weakest link toward organizational security (Zhang et al., 2021). Indeed, many cyber-attacks and data breaches that have been identified and investigated have resulted from human-enabled errors. Therefore, the saying portraying the human factor as the most significant vulnerability towards security is accurate (Nobles, 2018). Although the human factor has been presented as a significant threat to organizational security, organizations are nevertheless investing their security efforts towards extensive technology-based information security solutions (Abawajy, 2014) instead of mitigating behavior-based risk (Nobles, 2018). These technology-based solutions that are continually being invested in are, for instance, firewalls, antivirus software, intrusion detection systems, etc. It should be noted that these solutions are imperative for achieving good security; however, it should not be forgotten that these solutions are ineffective on their own. Good technical security solutions are not enough to protect the overall security necessary to defend organizations' systems and assets from harm if the human side is not providing a strong defense. The human factor must, therefore, be managed with the same level of care as the technical aspect has long been done (Abawajy, 2014). This is because organizations, private and public alike, are socio-technical systems comprised of people, structures, technology, and processes designed to collect, process, store, and distribute information. That means that organizations can not exclude human's inevitable role in cybersecurity and other non-technical measures to rely on technology alone. The complex social-technical nature of cybersecurity must be addressed to defend organizations against cyber-attacks (Al Sabbagh, 2019).

To address the risks and threats the social aspect, the people, pose to an organization's security, organizations began incorporating the concept of creating and nurturing a cybersecurity culture (Gcaza and Von Solms, 2017; Kovačević and Radenković, 2020). A cybersecurity culture can be defined as assumptions and beliefs frequently expressed in collective values, norms, and knowledge of those a part of the organization's environment. The result of these collectives promotes or instills a sought-after security behavior among the people within this environment (Ramluckan et al., 2020). Building and maintaining a cybersecurity culture is widely recognized as a highly effective approach to combat undesirable security practices and enhance employees' CSA (Gcaza and Von Solms, 2017; Kovačević and Radenković, 2020). When striving to create a culture that fosters cybersecurity-conscious behaviors among people, it is of utmost importance to consistently work with CSA initiatives within the organization, and it should not be treated as a one-time event. Therefore, implementing CSA education programs in organizations that consistently educate and train their employees in various CSA initiatives is vital to minimize the vulnerabilities associated with human behavior and to cultivate a cybersecurity culture (Abawajy, 2014). Over the years, it has been reported that large organizations have begun prioritizing more of their annual budget toward raising CSA, such as investing more resources into security training than before or working harder at cultivating securer environments (Kovačević and Radenković, 2020). This is positive because it is essential that large organizations, especially within the public sector, focus on increasing their user's CSA. Because large public organizations are often exposed to cyber-attacks (Tu et al., 2018) that carry far more severe repercussions more widespread than private organizations (Aman and Al Shukaili, 2021). It should be noted that organizations are classified as large when there are a minimum of two hundred and fifty or more persons employed (Eurostat, 2016).

1.1 Problem Definition & Aim

Cybersecurity awareness (CSA) has lately gained increased recognition from public authorities worldwide (Wang et al., 2018). There is an increasing interest in CSA because organizations have realized that technical measures alone are insufficient in providing adequate protection for an organization against sophisticated cyber-attacks (Jeong et al., 2019). Organizations have long prioritized technical protection measures to combat cyber-attacks by heavily investing in strong technology (Nobles, 2018). However, the social side of cybersecurity has repeatedly been overlooked and neglected, resulting in the human factor becoming an uncontrollable weak link to an organization's security (Wang et al., 2018). Organizations recognized that a significant amount of security incidents could be linked to human errors, so they redirected their focus from technology toward examining human factors and their impact on cybersecurity. It became clear that people pose a substantial risk to an organization's security if left unchecked, which is a significant problem (Jeong et al., 2019). To rectify this problem, it has been acknowledged that if people can improve their CSA, it will greatly reduce the number of cyber-attacks in cyberspace to a significantly lower level, thus minimizing the risk people pose to an organization's security. It has been highlighted that primary actions to rectify this problem lie in organizations' implementing some form of comprehensive, systematic, and effective cybersecurity awareness-raising frameworks in addition to technology-based solutions. This is because organizations urgently need assistance from various aids to boost the efficiency of their CSA as much as possible. After all, increasing users' behavior is no easy task. Research on CSA is still new in the field of cybersecurity; therefore, various techniques and aids for CSA are constantly being developed to find new and improved ways to raise awareness (Wang et al., 2018). However, despite the magnitude of existing research on CSA, there seems no one has attempted to compile all this information into one single picture to provide a highly abstract overview of the essential factors that contribute to cybersecurity awareness-raising.

The aim of this thesis is to develop an artifact for cybersecurity awareness-raising by employing a design science research project. The artifact will be structured as a guideline to provide managers in large Swedish public organizations with a complete and holistic overview of highly essential and relevant contributing factors for cybersecurity awareness-raising, presented in a single frame. Compiling areas significant to raising CSA based on a magnitude of existing research in a highly abstract manner is beneficial because it can provide people with a unique perspective and a more comprehensive understanding of CSA in one glance. Managers in public organizations can utilize this guideline to gain insight into what areas should be included in their CSA efforts and be provided with detailed suggestions for what factors should be included per area. The guideline's factors are meant to provide managers with a complete picture to ensure no factors crucial to the success of cybersecurity awareness-raising efforts are missing or being overlooked. The guideline is targeted toward large Swedish public organizations because if cyber-attackers target them and are successful in their efforts, public organizations tend to produce more severe and widespread repercussions than private organizations. Therefore, public organizations were deemed more vital to be provided with assistance in their CSA endeavor. The guideline is intended to be evaluated, verified, and validated by experts in CSA working at large Swedish public organizations to ensure the guideline provides value to the intended audience.

1.2 Research Question

Based on the problem definition and aim, a research question was developed for this thesis to address. The research question consists of one main objective and two sub-objectives, and these are:

- What factors contribute to cybersecurity awareness-raising in large Swedish public organizations?
  - What factors contribute to cybersecurity awareness?
  - How can these contributing factors to cybersecurity awareness be described in a guideline for large Swedish public organizations?

1.3 Delimitations

This thesis has certain delimitations that must be considered as they affect the thesis greatly. Delimitations concern the researcher's boundaries and limitations for the thesis aims and research objectives to be achievable (Theofanidis and Fountouki, 2018). The first delimitation of this thesis is that the research will be conducted from a management perspective and not from the organization's employees. This is because the target audience meant to utilize the guideline is those with a strong influence over organizational cybersecurity awareness (CSA) endeavors. Cieslinska (2007) defines a manager in an organization as: "a person that makes plans and decisions, organizes, supervises and controls human, finance and information resources" (Cieslinska, 2007). These capabilities are needed in the people meant to organize, design, and implement CSA initiatives. This choice of perspective greatly influences what kind of data will be collected later on in the methodology chapter, which is a conscious choice on the researchers' part.

The second delimitation of this thesis is that the guideline is aimed at large Swedish public organizations. A large organization is defined according to Eurostat (2016), and it states that an organization is classified as large when there are a minimum of two hundred and fifty or more persons employed. In this case, the three organizations involved in this thesis are defined as large because the number of people in their employ ranges between four hundred to several thousand employees. The third delimitation of this thesis is that the concept of a guideline is defined according to Syafrizal et al. (2020) definition. Hence, a guideline is something that can be used to assist in plan-making, directing actions, building ideas, and so on. A guideline can be described as suggested activities that users can translate, apply, or use to further their own work (Syafrizal et al., 2020). In this thesis, the guideline will be structured as a highly abstract picture outlining relevant factors that contribute to cybersecurity awareness-raising. These factors can assist managers in large Swedish public organizations with planning, developing new ideas for what areas to prioritize, and providing suggested activities for what to include in their awareness initiatives. As such, this thesis develops something that assists organizations in directing their actions within cybersecurity awareness and can, therefore, be defined as a guideline.

2 | Background

This chapter presents the background information relevant to this thesis with three focus areas. The first pertains to cybersecurity, the second pertains to the human factors within cybersecurity, and the third pertains to cybersecurity awareness-raising.

2.1 Cybersecurity

The first mention of the cybersecurity concept in literature appeared only twenty years ago, so it is a relatively new notion but has already been widely recognized (Reegård et al., 2019). Since then, the internet has played a significant part in global communication and has become integral to people's lives, so much so that there are over three billion worldwide users of the internet and its cyberspace at the present day. Cyberspace can be defined as "Interconnected networks, from IT infrastructures, communication networks, computer systems, embedded processors, vital industry controllers, information virtual environment and the interaction between this environment and human beings for the purpose of production, processing, storage, exchange, retrieval, and exploitation of information." Cyberspace is essentially the place where all interactions and activities of users are occurring. As such, significant time in users' lives is spent interacting with cyberspace, and when cyberspace is subjected to cyber threats, users integrating with it can be significantly affected. The concept of cybersecurity is essential to organizations as it relates to their capability to secure their infrastructure and protect their private and customer data from attackers. Cybersecurity, therefore, entails the practical measures applied to protect an organization's information, networks, and data from both internal and external threats (Li and Liu, 2021).

When discussing safeguarding sensitive information from internal and external threats, the CIA triad is often mentioned as its principles of Confidentiality, Integrity, and Availability are ways of withholding information from unauthorized individuals (Li and Liu, 2021). However, the term cybersecurity has long been used interchangeably with information security. Still, while there is substantial overlap between the two terms, there is a difference between the concepts. The noteworthy difference is that cybersecurity includes the traditional boundaries of information security and includes factors beyond that definition, while information security does not. For instance, information security focuses mainly on "the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information," where an incident would result in a breach in the CIA of information. At the same time, cybersecurity focuses on those elements and elements beyond, which can include protecting people, household appliances, national infrastructure, and so on. When discussing assets in cybersecurity, it can be anything that can be reached through cyberspace. Thus, when mentioning the human factor in cybersecurity, it is referred to people being the potential target of cyberattacks. In contrast, the human factor within information security would be referred to as its

role within the security process. Therefore, these two concepts are related but not analogous (Von Solms and Van Niekerk, 2013). Computing and communication technologies are changing the field of cybersecurity because their rapid development constantly creates more advanced and sophisticated technologies. Each change creates new possible vulnerabilities to be exploited and thus needs a planned countermeasure response. Cyberspace is invariably a dynamic place where change is repeatedly occurring, making establishing cybersecurity measures more difficult because the threats and technology are changing with it (Li and Liu, 2021). These sophisticated technologies change the behavior of their users because a change in technology influences users' views of the internet. Thus, creating a whole new form of threat and protection models has been needed to accommodate the growing and ever-changing threat landscape. When cyber threats are evolving in relation to technology, it often makes it harder for users to efficiently protect their sensitive information accordingly. The reason for this often lies in there being a knowledge gap between today's existing technology and the knowledge people have to secure them effectively. This produces situations where people use advanced and sophisticated technologies while retaining minimal understanding or knowledge of how they function, which invites more considerable risks of security incidents. Users often have a general awareness of cybersecurity; for instance, many can vaguely explain what hackers are and why they are deemed harmful, but they often have great difficulty behaving securely. There are countless ways in which human errors manifest, and these are often related to users' flawed cyber hygiene. For instance, performing poor system configuration, poor patch management, using weak or default passwords and usernames, reusing passwords at different websites, clicking on infected email attachments, leaving laptops open when leaving the workstation, etc. (Szumski, 2018).

2.1.1 Cybersecurity in Public Sector

In the current business environment, information is a valuable resource for any organization's success and has become vital for its survival. Protecting that valuable resource is becoming increasingly harder when organizations are exposed to cyber-attacks, whether they originate from external or internal sources, thereby endangering the security of the organization and its information (Tu et al., 2018). Therefore, maintaining good cybersecurity is crucial for public and private organizations to safeguard their business objectives. However, when cyber-attacks occur within the public sector, the repercussions tend to be more severe. This is because the public sector covers a broader and more widespread user base compared to the private sector(Aman and Al Shukaili, 2021). The public sector performs critical functions in economic and social life and development; for instance, consisting of armed forces, police, emergency service, and legislative and judicial authorities. The public sector additionally consists of public organizations providing their citizens with services and goods that are considered critical infrastructures. These include banks, hospitals, educational institutions, energy, telecommunications, transport organizations, industries, manufacturers, etc. (Loukis and Spinellis, 2001). When these critical functions and infrastructures become vulnerable to cyber-attacks, any disruption in their services can result in consequences with a significant impact on society (Aman and Al Shukaili, 2021). It is important to note that critical infrastructures in the public sector contain systems with numerous dependencies on other infrastructures systems. If a cyber-attack occurs in one system, then it could disrupt other systems simultaneously(Dawson et al., 2021). There is a significant contrast between public and private organizations when it comes to the societal consequences of cyber-attacks. In the event that a public organization encounters a cyber-attack that disrupts its critical systems, the disruption would cause a larger-scale impact on society compared to that of private organizations. This is because such a widespread disruption would have greater economic and social impacts and could even pose a threat to the safety of citizens (Loukis and

Spinellis, 2001). It has been noted that the public sector has been experiencing a high frequency of targeted cyber-attacks. Research indicates that approximately seventy percent of security breaches are directed toward public or government organizations (Aman and Al Shukaili, 2021). In addition, another thesis revealed the fact that public organizations from various areas in the public sector, such as government, law enforcement, and healthcare, have been increasingly targeted by cyber-attacks. The findings of the thesis suggest that these cyber-attacks targeting public organizations may originate from external factors, such as outside hackers, and internal factors, such as current or former employees (Bendovschi, 2015). It is becoming increasingly evident that relying solely on technical measures to prevent cyber-attacks may not be enough for organizations in the public sector. Therefore, implementing strong socio-technical cybersecurity measures that account for human behaviors is crucial (Gandhi et al., 2011).

2.2 Human Factors in Cybersecurity

According to Hadlington (2017), there have been an increasing amount of reports indicating a rise in cyber-attacks, which is alarming due to the devastating consequences they can bring. For instance, the economic cost of successful cyber-attacks can be substantial for small, medium, and large organizations alike. It can be further estimated that approximately sixty-five percent of adults have been susceptible to some form of cyber attack. Thus, has the human factor within cybersecurity been brought to the attention of many organizations as a crucial factor to consider when protecting themselves against cyber-attacks (Hadlington, 2017). It has been stated for decades that human errors are one of the underlying causes of cybersecurity breaches and is an ongoing problem in the present day. Human error has always been present in industries and professions. Still, the causes of these errors have greatly been overlooked or even ignored as something inevitable to occur (Pollock, 2017). This disinterest in human factors and their errors has been repeatedly overshadowed by technological protections. For instance, this could be seen in research, where the main focus of cybersecurity has been related to concerns pertaining to technology instead of human factors. The emphasis was on how technology could be used to solve cybersecurity issues. Thus, organizations focused their efforts and capital on implementing technological safeguards, often at the expense of considering the human factor. Prioritizing the technical side over the social side in cybersecurity does not create better protection but hinders the creation and amelioration of cybersecurity countermeasures (Coffey et al., 2017).

Therefore, it is essential to understand that cybersecurity is a complex socio-technical challenge for governments and private sectors to undertake (Khader et al., 2021). It has been recognized that human factors pose a far greater threat to organizations' security due to people's inherent weaknesses in their human nature than what technological threats pose (Wang et al., 2018). In cybersecurity incidents, the root causes of successful cyber-attacks can often be traced back to a human error component. For instance, a study has shown that thirty-seven percent of reported cybersecurity incidents have had human involvement and that these actions have, in some way, contributed to successful cyber-attacks. Nowadays, it is more common that human factors play a role in creating security breaches, whether intentional or unintentional, compared to those created by unanticipated vulnerabilities in information systems (Coffey et al., 2017). Attackers have also realized this and have shifted their efforts and attention to exploiting the vulnerabilities of human nature instead of the technical. This has created a more significant focus on threats related to various forms of social engineering, as these attacks focus on exploiting the human factor to conduct cyber-attacks (Wang et al., 2018).

2.2.1 Social Engineering Threats

Social engineering has emerged as one of the more challenging cybersecurity threats nowadays because of its nature to exploit human vulnerabilities (Aldawood and Skinner, 2018) and because of this focus on people's vulnerabilities, it can be said that attackers are using "the principle of easiest penetration." This entails that regardless of whether a system in itself is secure, it can not be more secure than its users (Nohlberg, 2008). This social engineering practice constitutes manipulation of human unawareness of cybersecurity practices and threats and the human nature to trust others to accomplish their malicious goals. Others might say that "social engineering is the art of manipulating human weaknesses in order to attain a malicious goal" (Aldawood and Skinner, 2018). The technique that social engineering attackers often use to manipulate their targets is posing as an insider or an authority to obtain access to information (Nohlberg, 2008). Attackers employing social engineering methods often seek to manipulate not only individuals in their homes but also entire institutions and companies by targeting people working in those environments (Al-Otaibi and Alsuwat, 2020). The challenge with social engineering attacks is that human vulnerabilities are not easily secured because people behave differently. Therefore, automatically securing all those varying vulnerabilities is incredibly hard. Additionally, social sites are frequent targets of social engineering attacks because people are more inclined to consent to communication if that communication has been packaged to look legitimate. Then, attackers have the chance to apply their manipulation and persuasion skills to obtain whatever information is sought to achieve their goals. Social engineering relies on manipulating legitimate users to relinquish confidential information or valuable assets by luring them to breach security prescripts (Aldawood and Skinner, 2018).

Phishing Threats

There are countless methods attackers use to try and manipulate people into giving up information. Phishing attacks are a common social engineering approach used by attackers to deceive people into relinquishing their hold on confidential information and sensitive data. Attackers do this through several methods of sending falsified emails with links to malicious sites, phishing for confidential information through phone calls, and so on. These phishing threats can be highly harmful to organizations and individuals due to the damage they can cause by exploiting people's lack of cybersecurity awareness. For instance, attackers can succeed in deceiving people working at organizations to download malicious files and software or click on links sent to their email. Hence, they give the attacker a way into the organization's confidential data by packaging these emails as seemingly legitimate. Attackers are also becoming more sophisticated in how they design these phishing attacks, much so that they are becoming harder to identify as non-legitimate, which is cause for great concern. Due to the harmful consequences that phishing can bring to an organization's systems and networks by exploiting the human factor, these social engineering attacks have become one of the more dangerous cybersecurity threats facing people today (Al-Otaibi and Alsuwat, 2020). Because of the influences that these types of attacks have on human personnel (Aldawood and Skinner, 2018), people need to raise their awareness of cybersecurity and establish improved cyber hygiene when integrating with technology.

2.2.2 Cyber Hygiene

The notion of cyber hygiene is closely linked to reducing human-instigated breaches in the cybersecurity arena. This is important due to the number of threats revolving around the human factor, such as socially engineered cyber-attacks and phishing scams (Neigel et al., 2020). It has been a commonly reported theme in cybersecurity of people having poor cyber hygiene because the behavior, or hygiene, they demonstrate is prone to causing errors and may result in continued security incidents. People are, for instance, quick at sharing passwords with others or giving away private information over various social sites. Compiled research on the average cost of cyber crimes has shown that weak cybersecurity is costing society significantly; for instance, the average cost countries have to pay in damages due to cybersecurity incidents is several million. Further statistics show that wholly ninety-eight percent of reported organizations have experienced malware-related attacks, and seventy of those percent have been social engineering and phishing attacks. Attackers are searching for vulnerabilities they can exploit, and these are often found within the human factor. The primary reason why vulnerabilities are found in people depends on them exhibiting poor cyber hygiene (Cain et al., 2018). Cyber hygiene can be defined as "establishing and maintaining important cyber health behaviors. Routinely monitoring technology for threats or attempted hacking, changing passwords and avoiding recycled passwords, updating virus protection software, storing online information securely, and running appropriate security scans" (Neigel et al., 2020). Hence, cyber hygiene essentially consists of norms and guidelines that should be followed in cyberspace to protect data and information from attackers (Singh et al., 2020). Consequently, promoting good cyber hygiene and safe behaviors among people is imperative to protect themselves against threats (Cain et al., 2018).

2.3 Cybersecurity Awareness-Raising

Within the literature, a distinction is made between the roles of education, training, and awareness-raising. Education is the space where security professionals integrate their skills and competencies in a single column of knowledge to be used for the design and implementation of cybersecurity. While training is the space where people gain security skills and competencies that enable them to perform their work activities (Alkhazi et al., 2022). In comparison, cybersecurity awareness (CSA) is about raising awareness of how people should protect personal and organizational information from unwanted adversaries by employing information security practices. The concept of awareness is often regarded as having knowledge of a situation and being aware of possible security issues and threats that allow people to make better-informed decisions (Korovessis et al., 2017). Essentially, many regard CSA as the first line of defense of information systems and networks in organizations. This is because good CSA among users provides more robust protection against those wishing harm (Tasevski, 2016). CSA can be further defined as "the person has the ability to identify possible threats to cyberspace, judging their harmfulness, preventing or resolving problems in time to protect personal information and property safety" (Wang et al., 2018). There are countless variations to the definitions of CSA; however, there is a consensus among the literature that organizations must continuously work with awareness-raising. It is recommended that "all employees of the organization should receive appropriate awareness, education, and training and regular updates in organizational policies and procedures, as relevant for their job function." Hence, it is recommended to implement these awareness-raising programs into the organization's overall security strategy (Alkhazi et al., 2022).

2.3.1 Cybersecurity Awareness Training

Countless studies have suggested that one of the more effective methods to raise cybersecurity awareness (CSA) is implementing training programs in organizations (Alkhazi et al., 2022). Training initiatives employed to improve people's knowledge of cybersecurity practices are deemed essential to raising awareness. This is because spreading CSA through education may make people more capable of mitigating threats and minimizing harm (Shillair et al., 2022). Acquiring a better understanding of the risks and threats involved when integrating with cyberspace may influence people to implement safer behavior patterns or cyber hygiene to make better and more informed decisions (Szumski, 2018). Numerous guidelines are presented in the literature for how organizations should develop awareness training programs. According to the author Alkhazi et al. (2022), these can essentially be stripped down into three fundamental phases: development, implementation, and evaluation. Furthermore, the activities in CSA training come in many forms. Generally, two important factors need to be considered within these activities for a cybersecurity training program to be effective. The first factor is that all training information should be relevant and up-to-date, as cyberspace constantly evolves. It is important to know the recent ongoings of; for instance, new technology being used in the world or the latest zero-day threats, etc., if there is a chance of protecting the systems against it. Therefore, the training materials in CSA programs could constantly be updated (Alkhazi et al., 2022).

The second factor that is exceedingly important for raising awareness through training is how the training program is designed. Hence what training activities are included in the program, how it is designed to teach users, the program's delivery methods, etc. It is essential to develop security awareness training so that users not only want to learn and improve their awareness but are also motivated enough to keep the work ongoing themselves (Alkhazi et al., 2022). Another author Kävrestad et al. (2022) classifies cybersecurity training into two broad categories: physical and digital security training. Physical security training refers to in-person training, while digital training mainly refers to various ways of conducting cybersecurity training digitally. For instance, e-learning platforms where users have on-demand access to training materials are a popular digital training method, as is game-based and contextual training. The former training method involves different games, such as quizzes, story-based, competitive-based, and single-player games, all developed to teach the material more engagingly. The latter training method involves simulation-based training, which is when users are provided with training material when they encounter certain situations that can pose a cybersecurity risk (Kävrestad et al., 2022). CSA training aims not to tell people the results of thinking about cybersecurity but to present people with opportunities to think about cybersecurity for themselves (Stahl, 2006).

2.3.2 Criticisms Against Awareness Training

Despite considering cybersecurity training as one of the more important measures to increase cybersecurity awareness, countless research criticizes that as little as one-third of the existing training programs are deemed effective in reducing security breaches (Alkhazi et al., 2022). Even when cybersecurity awareness training is provided, they often fail to do their job (Caldwell, 2016) and according to Stahl (2006), upwards to seventy-five percent of security awareness training programs fail shortly after implementation (Stahl, 2006). Numerous awareness training is available; however, there is a difference in training users and changing their behaviors. It is not uncommon for organizations to invest capital in training their users to behave more security conscious but fails to, for instance, follow up on the user's training to ensure whether the training has positively affected both the workplace and the user's approach to cybersecurity. This can quickly become a pitfall where organizations waste a lot of money on training that, in the end, is ineffective.

Organizations can not rely on training alone to change behavior and raise users' cybersecurity awareness, they need to condition their user's behavior and engage and empower them to become a part of the solution (Caldwell, 2016). The criticisms against the effectiveness of cybersecurity awareness training programs relate to the difficulty of genuinely changing people's risk perception to be positive, of agreeing on which delivery methods to use to produce effective training, and of having poorly established evaluation criteria to see if tangible improvements to awareness have been made due to cybersecurity awareness (CSA) training. It is often mentioned that the success of CSA programs depends upon the ability to engage and motivate the people involved. When the effectiveness of the training program is identified as inadequate, the problem often relates to a lack of user engagement and motivation. This lack of user engagement and motivation may relate to people viewing the awareness training initiatives as tedious, thus allowing their negative perception to impact their engagement.

Motivating and engaging users to enjoy learning about cybersecurity can remain a problem regardless of whether efforts are made to engage and motivate users. This is because people are headstrong and often have different needs, opinions, and perceptions regarding training that strongly affect their susceptibility to training. Thus, making the aspect of increasing CSA challenging. Efforts are continuously underway to overcome the challenge of making security awareness training more engaging and effective. One approach is to use game-based and simulation-based training methods, which are expected to produce better results and improve the overall effectiveness of security awareness programs. Lately, research has focused extensively on delivering 'Personalized Learning Theory' for cybersecurity training. This kind of training is tailored to specific individual's preferences, so the training is based on each person's learning objectives, learner's profile, and so on to create engaging ways for them to learn. However, this type of training has not yet been applied to cybersecurity training or awareness-raising programs. Still, this way of learning might be available for those purposes in the future (Chowdhury et al., 2022).

2.3.3 Factors Beyond Training That Raises Cybersecurity Awareness

It has time and again been established in academia that the human factor is assumed to be the "weakest link in security" (Bélanger et al., 2022) and the ultimate way to address this weakness is through the implementation of security awareness training (Alkhazi et al., 2022); however, other factors beyond training might be as important for raising awareness. Motivation plays a big part in encouraging people to adopt cybersecurity best practices and engage in cybersecurity behaviors that benefit organizational security. This is especially important as people often have negative perceptions of cybersecurity, and it is possible to categorize these negative user perceptions of cybersecurity into three sub-factors. The first sub-factor is that security is scary, the second is that security is confusing to grasp, and the third is that security is dull. Users' feelings toward cybersecurity have been partly responsible for organizations' inability to implement and effectively use cybersecurity practices and technologies, making user perception vital to successful awareness-raising. Therefore, it is essential to address these negative perceptions users can feel for organizations to better motivate and engage users to follow cybersecurity practices, accept new technologies, and facilitate more cyber-aware behaviors (Haney and Lutters, 2018). Those advocating for organizational cybersecurity awareness (CSA) must be able to motivate people to overcome their negative perceptions of security. One prerequisite to achieving this is being viewed as a trustworthy information source. Establishing trust among the people targeted to be influenced is paramount to successful awareness-raising. This is often accomplished through relying on the organization's reputation to establish credibility, demonstrating good technical knowledge, building relationships that foster trust, and leveraging insider trust to gain credi-

bility. Furthermore, there have been several ways in which motivation has been attempted to change people's negative perceptions of cybersecurity. Ways of creating motivation for people with the perception that cybersecurity is scary consist of conveying the importance and urgency of why cybersecurity is important while doing it honestly and empowering the people to take action. This means being forthcoming regarding the risks and what is at stake if security is not well-established and instilling a sense of hope in people so they believe changing their behavior is not pointless. Other ways of creating motivation for people with the perception that cybersecurity is confusing consist of bridging the gap between technical and non-technical users so common ground is established, providing users with straightforward instructions on how they can improve their security behaviors, providing practical and prioritized security recommendations, and promote the usability of technologies and policies to alleviate the complexity and burden of security (Haney and Lutters, 2018). Moreover, there are ways of creating motivation for people who perceive cybersecurity as dull, irrelevant, not worth the investment, etc. These ways involve persuading users to invest in good security behaviors by appealing to their internal and external motivations. This includes adapting to an individual's specific needs when, for instance, selling security instead of promoting a "one-size-fits-all" approach.

Attempts have been made to increase motivation for those believing security to be dull by creating, for instance, a rewards and consequence system to encourage people to foster a culture where security adaptation is supported. Others have attempted to make their communication regarding the importance of cybersecurity filled with enthusiasm and relatable stories to overcome people's disinterest. Others have attempted to relate it to other non-security risk domains to build trust, create awareness, and motivate people to act (Haney and Lutters, 2018). Another significant factor in raising CSA, which is closely interwoven with creating motivation, is cultivating and fostering a cybersecurity culture. The role of a cybersecurity culture is to close the gap between an organization's dictation of cybersecurity policies and the people's security behaviors because the effectiveness of a CSA training program ultimately depends on the motivations and behaviors pertaining to the human factor. There has been significant attention toward understanding people's behaviors since behavior depends upon what kind of knowledge people have, their perceptions, and what their instincts tell them to do (Stahl, 2006). A cybersecurity culture can be defined in numerous ways depending on the literature; for instance, two authors define cybersecurity culture as "a pattern of shared basic assumptions that the group learned; as it solved its problems of external adaption and internal integration, which have worked well enough to be considered valid; and therefore, to be taught to new members, as the correct way to perceive, think, and feel in relation to those problems" (Gcaza and Von Solms, 2017; Stahl, 2006).

Another author explains cultures as assumptions and beliefs frequently expressed in collective values, norms, and knowledge of those a part of the organization's environment. The result of these collectives promotes or instills a sought-after security behavior among the people within this environment (Ramluckan et al., 2020). Furthermore, another author presents the definition of a cybersecurity culture as a way of presenting basic assumptions regarding how the world is, compared to how it should be, in a way that a group of people shares perceptions, feelings, and thoughts that influence their behavior. The variations in definitions for the cybersecurity culture phenomenon are that way because it is a relatively new concept. Researchers have only recognized incorporating culture into an organization's security as important since the start of this century. Because of this, there have not yet been widely accepted key concepts, established definitions, or guidelines for a cybersecurity culture. Without a unified picture of what a cybersecurity culture entails, there will always be a variation in definitions and how these concepts are interpreted and applied practically in organizations (Reegård et al., 2019). However, the literature agrees

that a great need exists to establish and cultivate these environments that promote positive cybersecurity hygiene to influence positive cybersecurity behavior in people (Hadlington, 2017). A strong, committed leader must oversee an organization to cultivate a cybersecurity culture and raise awareness. This assignment could be part of the Chief Information Security Officer (CISO) job description to make the necessary cultural change possible. Because with strong commitment, energy, and time from a leader, it is possible to gradually succeed in embedding a cybersecurity subculture into the workings of the organization's dominant culture (Stahl, 2006). One could describe the CISO job description as "a strategic level position, responsible for ensuring that the information assets and IT systems are protected and secure and that such protection is in line with the strategic direction of the organization" (Hooper and McKissack, 2016). Therefore, a CISO could mold and shape the organization's culture so that, with time, the people in that environment behave correctly, pay attention to their security behaviors, and even train each other. The culture is built upon social relationships with the aim that when a group of people begins behaving in a certain way, more tend to follow the lead. Strong leadership is imperative to motivate and guide people toward contributing to cultivating and fostering a cybersecurity culture. It is thus an important sub-factor for raising CSA. As mentioned, changing a culture is about building relationships and fostering trust from the people expected to change how they perceive, think, and feel about cybersecurity. It is here where motivation and cybersecurity culture is closely interwoven as persuasion, and user engagement is needed in these areas for effective awareness-raising (Stahl, 2006).

3 | Method

This chapter presents the thesis's chosen research methodology, which consists of a Design Science Research strategy and two supporting data collection methods. The two data collection methods chosen are a selective literature review and interviews. Furthermore, a mention of limitations and ethical considerations has also been included.

3.1 Design Science Research

This project employs a Design Science Research (DSR) strategy, which has, since its inception in the field, staked its claim on being an equal companion to natural science research within the information systems research paradigm according to (Gregor and Hevner, 2013; Hevner, 2007). The ideas, concepts, and methods of design science that are acknowledged today have originated from disciplines relating to architecture, engineering, psychology, etc., so the idea of research in design is not entirely new. However, it was not until the early 1990s that it was recognized that DSR could be utilized for solving real-world problems within the context of information systems (Hevner et al., 2010). DSR goes beyond empirical research, aiming to describe, explain and predict various occurrences. Instead, DSR focuses on wanting to provide change and improvement to the world by creating something better than what was previously there before. The practice of providing change and improvement is by creating new artifacts. These artifacts could be, for instance, new software, processes, or systems intended to enhance the effectiveness or efficiency of an organization. Furthermore, artifacts could also be created to improve people's health, education, quality of life, community interaction, well-being, etc. Artifacts are thus used to aid people in fulfilling their needs, overcoming their problems, and presenting them with new opportunities (Johannesson and Perjons, 2014; Myers and Venable, 2014). DSR is often called "Improvement Research" because it focuses on problem-solving and performance enhancement (Hevner et al., 2010). When employing DSR, there are generally four types of artifacts that can be generated: constructs, models, methods, and implementations. A construct is regarded as the language of concepts, hence, the vocabulary used to formulate the phenomena within its environment. A model is regarded as a higher form of construct because it combines multiple constructs in the form of a model while describing the relationships existing between them (March and Smith, 1995). A method is regarded as a set of steps that can be viewed as an algorithm or guideline used to conduct a specific task. Lastly, implementation is regarded as the product of the artifact, whether it be a construct, model, or method (Vaishnavi, 2007).

In DSR, there are several types of knowledge an artifact can express, and this knowledge is usually utilized for three purposes; describing, predicting, and explaining phenomena (Johannesson and Perjons, 2014). These knowledge types can be classified into six categories depending on the artifact's purpose and be viewed in Figure 3.1.

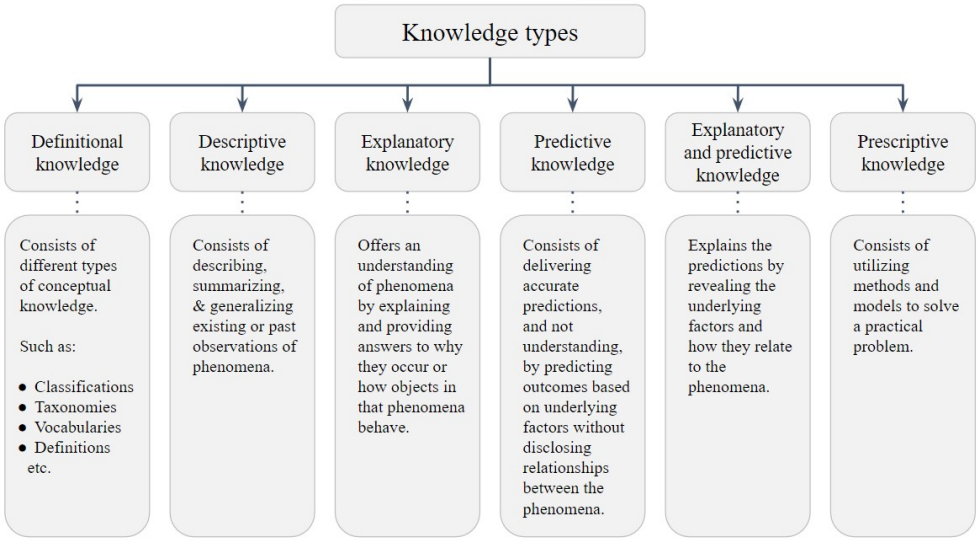


Figure 3.1: Knowledge types in artifacts (Authors Own). Information from Johannesson and Perjons (2014).

In 'Prescriptive knowledge,' a method could, for instance, be a guideline or procedure meant to aid people when solving problems. Prescription can be seen as a special type of prediction because when the method or model is utilized in a certain context, it will help achieve outcomes desired by certain stakeholders (Johannesson and Perjons, 2014). In addition to the various types of artifacts and knowledge types, there are four distinct types of artifact contributions in a DSR project. The first is 'Improvement,' which focuses on enhancing an existing artifact or improving upon an already established problem. Improvements are often made in usability, safety, efficiency, and maintainability. The second type is 'Exaptation,' which creates an artifact that adapts an existing solution to a new problem context. 'Routine design' is the third type, which produces an artifact by slightly modifying an existing solution to solve a known problem. Lastly, 'Innovation' is the fourth type that generates a new artifact to solve a new problem. Such contributions often create new research fields or enable new practices. Furthermore, a DSR project can involve many people or a single researcher because the scale of the project determines how the work is structured.

In this thesis, the kind of artifact that will be developed will be of a method type that uses prescriptive knowledge because these artifacts are good for defining guidelines and processes and utilizing them to solve problems and achieve certain goals. Examples of these types of artifacts can be new database design methods or developing new management change initiatives. Therefore, this kind of artifact is suitable for this thesis's intended goal, which is to develop a guideline to be utilized by large Swedish public organizations to aid them in their cybersecurity awareness work. In addition, a single researcher will be involved in the DSR project (Johannesson and Perjons, 2014).

3.2 Implementation of Design Science Research Framework

It could be said that the heart of any design science research (DSR) project is the internal design cycle. This design cycle is important because it is where the actual work of design science research is performed, hence the rapid and iterative work of the artifact's design. As such, design cycles revolve around a continual loop of refining the construction of the artifact, evaluating it, and generating subsequent feedback to refine the artifact further. Design cycles are essentially a way for the researcher to generate design alternatives by evaluating them against chosen requirements. This iterative work is completed only when a satisfactory design has been achieved (Hevner, 2007). This thesis will adhere to the well-known DSR framework established by Peffers et al. (2007), consisting of six phases. The visualization of this DSR framework is depicted in Figure 3.2.

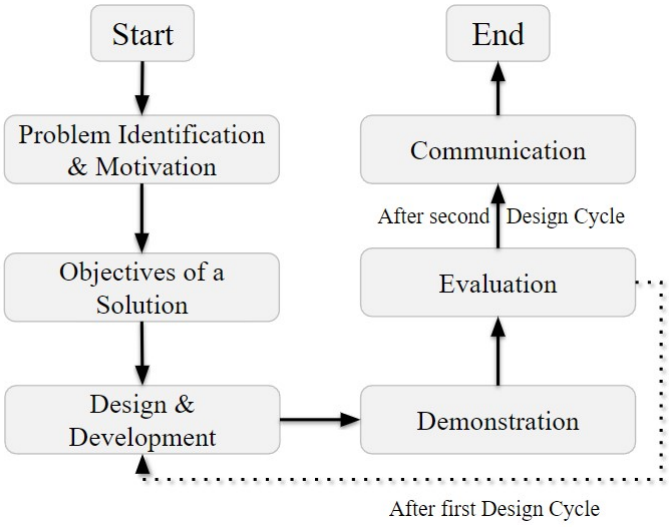


Figure 3.2: Visualization of DSR research strategy (Authors Own). Information from Peffers et al. (2007).

The first phase, 'Problem identification and motivation,' defines a specific research problem and justifies why the proposed artifact can provide value. Providing a definition and motivation is equally important because they contribute to creating an effective artifactual solution. Without defining the problem, the proposed artifact wants to solve; it will be exceedingly more difficult to grasp the problem's complexity. As such, a conceptualization of the problem ultimately facilitates a better solution. Justifying an artifact's value motivates the researcher conducting this process and the audience who partakes in it to better embrace the artifact and its produced results. Justification further provides the audience with insight into how the researcher has reasoned and can thus better comprehend the importance of the artifact (Peffers et al., 2007). The second phase, 'Objectives of a solution,' presents quantitative or qualitative objectives derived from the problem definition. The second phase further presents the objectives of how the artifact can provide value by providing a solution to the identified problem (Peffers et al., 2007). These objectives entail determining the criteria or requirements the artifact should meet. Furthermore, this phase is vital because these objectives influence how the artifact should later be evaluated (Kävrestad, 2022). The third phase, 'Design and development,' consists of creating

the devised artifact, which includes the artifact's desired functionality and architecture. The fourth phase, 'Demonstration,' consists of demonstrating the proposed artifact by utilizing one or several supporting data collection methods to produce results used to evaluate and validate the artifact. Supporting data collection methods include interviews, experimentation, simulations, case studies, etc. The fifth phase, 'Evaluation,' consists of analyzing and evaluating the established objectives of the artifact with the results obtained from the demonstration phase. These results can indicate whether the developed artifact resolves the intended problem. Suppose the artifact's architectural design is not satisfactory. In that case, the researchers need to decide whether to iterate back to phase three to refine and improve the effectiveness of the design or continue to phase six regardless of the unsatisfactory design. The decision of whether to pursue additional iterations in the DSR process is ultimately left to the researcher. If they choose to continue, they often do so knowing the artifact has room for improvements in future projects but is unable to make the improvements at present. The sixth and final phase, 'Communication,' involves communicating the artifact's final results obtained from the DSR process (Peffers et al., 2007).

This thesis' DSR process will accommodate two design cycles where each cycle consists of several phases, and this process is depicted in Figure 3.3.

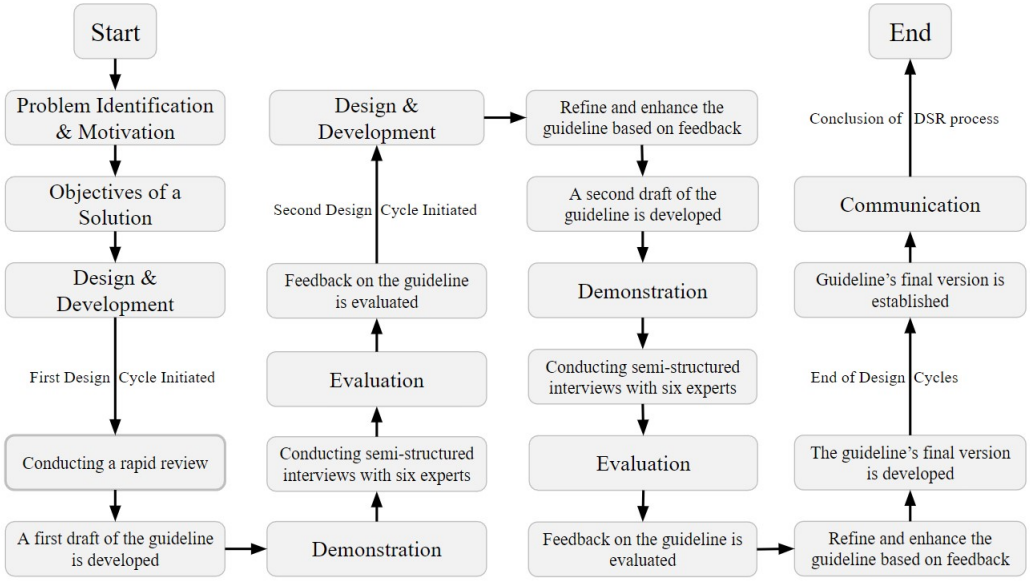


Figure 3.3: DSR process for the development of guideline (Authors Own).

The two phases, 'Problem Identification & Motivation' and 'Objectives of a Solution,' are included in the DSR process but not specifically in the design cycles. This is because the first phase is applied when defining the thesis's primary research problem, which is done by justifying why the artifact can provide value, which is done in 'Problem Definition.' The second phase is applied when determining the thesis's objectives, which is done in 'Research Aim,' by presenting objectives of how the artifact can provide value by providing a solution to the identified problem. Thus, the first design cycle is initiated with the 'Design & Development' phase, where a first draft of the proposed artifact will be developed and constructed. This first draft will be described in a guideline format, presenting contributing factors to cybersecurity awareness-raising. The

information the guideline is based on has been derived from relevant literature on cybersecurity awareness (CSA) through a rapid review by compiling and extracting relevant factors for ways to raise CSA. When a first draft of the guideline has been completed, it will be demonstrated in the 'Demonstration' phase through semi-structured interviews. The semi-structured interviews will be conducted with people possessing expert knowledge about CSA and working within large Swedish public organizations. This is because the guideline is meant to be adopted by managers in these organizations, making it important to gather insights from those with in-depth expertise. The purpose of conducting interviews is to evaluate whether the proposed guideline can be further refined and enhanced through feedback and validated as useful by people with deep insight into CSA. After that, in the 'Evaluation' phase, the acquired feedback will be evaluated to determine how the guideline will be refined and improved in the next design cycle. The second design cycle is initiated by going back to the 'design & development' phase to incorporate the acquired feedback from design cycle one's evaluation phase into the guideline's design to further refine and enhance its development. Another set of interviews will be conducted with the same group of interviewees used in the first design cycle's demonstration phase. Interviewees should remain the same during both design cycles because they possess a better chance of producing more in-depth feedback in the second cycle as they have already acquired significant insight into the guideline and the interviewer's thesis from the first cycle. Then another set of evaluations will be conducted in the evaluation phase to incorporate the new and in-depth feedback to further refine and enhance the guideline for the last time before communicating the final version and results. The final results of the guideline for cybersecurity awareness-raising are then presented in the 'Communication' phase. When this has been concluded, it signifies the end of this thesis's DSR process.

3.3 Supporting Data Collection Methods

A Design science research's (DSR) purpose is not only the creation of artifacts but also to answer the questions posed by the artifacts and their environments. It is, therefore, vital that research methods are used to provide valid and reliable answers. Furthermore, it is necessary to note that no methods should be excluded in advance for these kinds of projects as many of them can be valuable. In DSR, it is natural to use more than one research method as a supporting data collection, as different phases in the process may require the support of additional methods. For instance, one method can be useful for eliciting objectives used to design the artifact, while another may be useful for evaluating the artifact. As such, two supporting methods that are both of a qualitative approach have been chosen for this thesis's DSR project; selective literature review and interviews. Employing a qualitative methods approach deepens the understanding of the cybersecurity awareness phenomenon and produces descriptive results (Johannesson and Perjons, 2014; Kävrestad, 2022), which would be useful in this thesis.

3.3.1 Selective Literature Review

The selective literature review that will be conducted in this thesis is a rapid review. By utilizing systematic review methods, such as a rapid review, to search and evaluate existing literature, the selective literature review enables the assessment of what is already known about specific issues. The strengths of rapid reviews are that they aspire to be rigorous and explicit in method, which produces a systematic assessment of the literature in a shorter time frame. Because rapid reviews advocate for speed, they are not as extensive as a complete systematic literature review because the many aspects and stages of those reviews are lacking in rapid reviews. This means that par-

ticular elements of the systematic literature review process have deliberately been limited due to time constraint issues, and intentionally applying these limitations is what conducting a selective literature review entails. These limitations in rapid reviews often include using more carefully focused search questions, using broader or less sophisticated search strategies, searching in fewer databases, conducting reviews on reviews, applying heavier restrictions on what literature to include, choosing literature with specific key variables, performing simpler quality appraisals on the literature, etc. It depends entirely on the researcher to determine the extent of limitations to apply to the review and report the effects such a method can have on the compiled report (Grant and Booth, 2009). For this thesis, strategies were employed to intentionally restrict the time spent on the review. These tactics included utilizing less complex search methods, incorporating literature reviews, selecting relevant literature based on key variables, and conducting simple quality evaluations.

Furthermore, rapid review weaknesses are mostly related to being subjected to bias due to fast-tracking the review process by applying extensive limitations. This kind of risk is true for any review, but here, it is accentuated and therefore needs to be better acknowledged. When choosing a rapid review, there also needs to be a deliberation if this risk of increased bias is worth it to produce a selective literature review at the rapid timescale needed to (Grant and Booth, 2009). In this thesis, accepting the higher level of bias is more worthwhile than choosing a different type of selective literature review. This is because this thesis is entirely dependent on using a rapid review since the artifact is to be developed upon the extracted literature from one on cybersecurity awareness-raising. Although a rapid review is significant to this thesis, there is no need to perform an entire systematic literature review, which is why a selective literature review in the form of a rapid review was a better fit. When choosing among several other types of selective literature reviews, the rapid review was the preferred choice because it better advocates its strengths of conducting a review under time constraints compared to others, which is a sought-after aspect.

3.3.2 Interviews

This data collection method is a communication session between two or more parts, with one being the interviewer and one being the interviewee. Interviews are an effective choice where the focus is on gathering complex and sensitive information from those with access to privileged information. Furthermore, interviews are primarily used to extract opinions, experiences, and attitudes from the ones being interviewed in a detailed way. An interview session is often structured in one of three ways: completely structured, semi-structured, or unstructured. A wholly structured interview session has a predefined protocol that the interviewer follows, and no deviation from this protocol is allowed. This type of interview is built upon several existing sets of questions the interviewer is allowed to ask and where each question can be answered by a set of allowed and predetermined responses. Semi-structured interviews are similar to structured interviews in that they also follow a predetermined set of questions. However, the difference lies in the ability to be flexible in formulating the questions for the interviewee. Essentially, the interviewer is allowed to interpret the predetermined questions in their own words so the discussion can become slightly more open. Unlike the other structures, unstructured interviews do not follow a predetermined set of questions. Unstructured interviews focus more on the interviewees' ability to have the chance to talk freely and without restraint when being asked a question. Therefore, the interviewer focuses on being as unobtrusive as possible during the interview so this can be attained (Johannesson and Perjons, 2014).

There are different advantages to using these three interview structures, depending on when they are most suitable. If the goal is to conduct a quick interview without the need to interpret the interviewee's responses, structured interviews are the way to go. However, semi-structured or unstructured interviews are better suited if the goal is to investigate complex issues, as they allow interviewees to express themselves more freely. This enables interviewees to delve further into the issues they wish to scrutinize (Johannesson and Perjons, 2014). For this thesis, semi-structured interviews will be conducted because of that structure's ability to allow interviewees more expressive freedom while the interviewer still adheres to a predetermined set of questions. This is important because the interviewer wants to collect feedback from different people on the same subject, which is the artifact, and as such, the questions for every interview need to be the same. However, because the interviewer wants unfiltered feedback from the interviewees, they must be able to express themselves as they choose and not adhere to specific protocols when responding, which is why semi-structured interviews are the preferred choice. In addition, all interviews will be conducted in Swedish, which means this thesis will use translated responses when presenting the obtained results from the interviews.

Sampling of Interviewees

When utilizing qualitative methods, such as interviews, choosing a study sample is an important step in any research since it is not feasible, practical, or ethical to study entire populations. Sampling in qualitative interview-based research aims to provide a representative sample of the population intended to be examined so the sample can be generalized back to the population. In qualitative research, the sample size should be sufficient to address the research question effectively, and this is also the case for choosing which target audience shall be included in the sample. A common sample strategy for qualitative research is a purposeful sample strategy, which involves actively selecting people with the best chance of answering the research question. One method frequently used in this strategy is key informant samples, people with particular expertise within a specific area that produces rich and in-depth information in that area. These people are often sampled according to certain selection criteria (Marshall, 1996).

In this thesis, the sampling strategy chosen is a purposeful sample strategy using a key informant sample to conduct the interviews. The sample, or target audience, selected for interviews is experts on cybersecurity awareness (CSA), and they should possess certain merits to be designated as an expert and be included in the interview process. Hence, the interviewees should have a deep understanding and competence in the field of CSA that has been accumulated for several years, they have considerable skills and experience in working with CSA, and they should currently work at a large Swedish public organization within the security department. According to (Eurostat, 2016), this classification of a large organization is when at least two hundred and fifty or more persons are employed. This classification is appropriate for the three Swedish public organizations chosen for this thesis, as they employ between four hundred to several thousand employees. The reason for choosing experts with these criteria to interview is because they possess knowledge about the subject that this study focuses on and can provide the researcher with valuable insight and an in-depth understanding of cybersecurity awareness that can aid in developing the guideline. Furthermore, the interviewees originate from three different large Swedish public organizations, whereas three out of six interviewees originate from the first organization, two of the six interviewees originate from the second organization, and one out of six interviewees originate from the third organization. There will be a total of six experts being interviewed for this thesis, and they will be interviewed twice due to having two design cycles. It should be noted that the people being interviewed should remain the same during both design cycles be-

cause they possess a better chance of producing more in-depth feedback in the second interview. The motivation for choosing these three organizations is that the researcher knew someone with personal contact with cybersecurity awareness experts working at those organizations. Thus, several experts were contacted, and six accepted the proposal to partake in this thesis interview process. These organizations also aligned with this thesis's delimitations; hence, them fulfilling the criteria of being large Swedish public organizations.

Analysis of Interviews

Thematic analysis is a flexible approach often used in qualitative research for identifying, analyzing, and reporting patterns, also referred to as themes, within data. This type of data analysis provides a comprehensive and detailed view of the collected data with minimal organization. Additionally, there is no set agreement on how to perform this analysis, making it highly flexible. For researchers who are new to qualitative research, this analysis approach is highly beneficial. It can efficiently summarize extensive amounts of information, identify similarities and differences, highlight key features, etc. The thematic analysis involves identifying themes in two ways: through inductive analysis and theoretical thematic analysis. The inductive analysis involves coding data without trying to fit it into pre-existing frames established by the researcher, making the thematic analysis more data-driven. On the other hand, the theoretical thematic analysis attempts to fit data into pre-existing frames, making it more analyst-driven. This kind of analysis tends to provide less detailed and rich descriptions of the overall data compared to inductive analysis because of focusing on a detailed analysis of one specific aspect of the data. Choosing between these two types depends on whether the researcher wants to code the data for a specific theme or allow the theme to emerge from the data itself (Braun and Clarke, 2006). In this thesis, the semi-structured interviews were recorded so they afterward could be transcribed and analyzed thematically. The thematic analysis will be conducted through an inductive analysis approach because of wanting themes to derive and evolve from the coding process and provide detailed descriptions of the overall data transcribed from the interviews instead of focusing on a specific theme. The thematic analysis process used in this thesis is depicted in Figure 3.4.

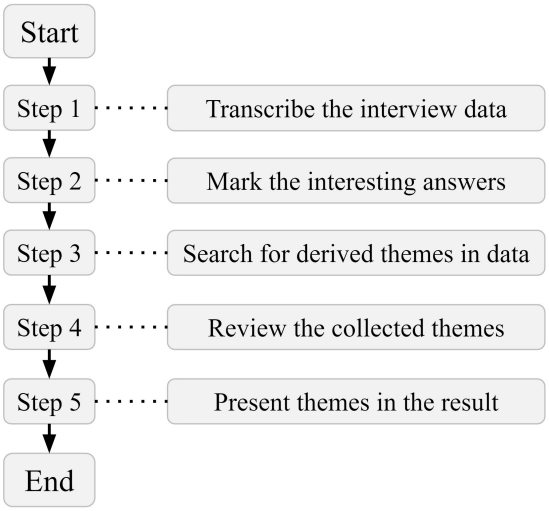


Figure 3.4: Thematic analysis process. (Authors Own). Inspiration gained from Braun and Clarke (2006).

The first step in the thematic analysis process is to transcribe the data obtained from the interviews with the experts. This is done by listening through the recorded interview and writing down each interviewee's answer word by word in a separate document, and then listening to the recording once more to ensure the transcription is correct. After that, the transcribed documents are read to mark any interesting answers, and then the transcribed documents are read once more to search for themes derived from the collected data. Following this, a review of the collected patterns or the themes is done, and then they are presented in the results.

3.4 Ethical Considerations

Addressing ethics in research is essential as ethical principles are essential to preserve and protect the rights of those participating in that research. Researchers are expected to approach their tasks ethically, observe privacy, confidentiality, and truthfulness of issues, and not cause harm. This expectation stems from the view that researchers should protect the public from those researchers that seek to use any means accessible to them to acquire knowledge on a given topic. Certain types of research require ethical approval, and this thesis uses one of those included: interviews. Interviews, among several other research methods, need ethical approval because the data collection is from or about living individuals. Researchers must take extra precautions to ensure participants' well-being by abiding by ethical principles when people are involved in research. These ethical principles include providing protection for their interests, ensuring any participation is voluntary and wholly based on informed, often written, consent, protecting them against deception, maintaining scientific integrity, and complying with the country's laws (Hasan et al., 2021; Denscombe, 2014).

Ethical considerations were thought of throughout this thesis to conduct tasks in accordance with an ethical manner. Specific tasks, such as conducting interviews for data collection, were the main focal point wherein ethics were heavily addressed. For instance, in all interviews, there was transparency to what was expected of the interviewees because they were provided with interview material beforehand so they could look it over, approve it and prepare themselves if needed. Before the interviews commenced, the interviewees were explicitly asked whether they consented to three different aspects. The first aspect was whether the interviewees consented to partake in the interview or not after the interviewer had explained to them what rights they had as interviewees. An interviewee has the right to withhold answers to any questions they are uncomfortable with and can withdraw their consent at any moment during the interview. The second aspect was whether the interviewees consented to allow a recording of the interview to be made after the interviewer had explained the purpose of the recording, which is for transcription purposes, and that any recording would be deleted after an approved thesis. The third aspect is whether the interviewees consent to allow the interviewer to use the collected data in their thesis or not after the interviewer has explained to them how the data will be processed and used, which is that interviewees are anonymous and will thus be referenced as numbers between one and six and any confidential information expressed during the interview that can break anonymity will not be included in the thesis. Furthermore, these aspects were given consent twice: before the recording was made and after the recording was underway.

4 | Result

This chapter presents the thesis's obtained results regarding the developed guideline through the application of 'Design Science Research Strategy' (DSR). The presentation of the results will be divided into a method development sub-section, an artifact demonstration sub-section, and an evaluation sub-section, which together signify the core phases of design cycles involved in DSR. Lastly, a communication sub-section presenting the cybersecurity awareness-raising guideline's final results will be included.

4.1 Design Science Cycle 1

In 'Method Development,' the first design cycle focused on constructing an artifact for cybersecurity awareness-raising by establishing a guideline. The creation of the guideline is based on literature compiled through the execution of the rapid review, and due to this review, a first draft of the proposed guideline could be developed. After that, in 'Artifact Demonstration,' a demonstration of the content and structure of the guideline's first draft was carried out to receive feedback and validate the guideline by interviewing six cybersecurity awareness experts working at large Swedish public organizations. Lastly, in 'Evaluation,' an evaluation was conducted by presenting and analyzing the received thoughts and feedback from the experts partaking in the interview using thematic analysis.

4.1.1 Method Development

The rapid review is used in this thesis to design and develop the proposed guideline. Before the execution of the rapid review, there was a need to decide what type of scientific literature should be obtained and from where. The desired scientific literature should somehow mention how to increase cybersecurity awareness (CSA) or contain the most critical factors organizations should focus on for cybersecurity awareness-raising. Therefore, several search terms and databases were used during the rapid review to find relevant literature following those desired aims, and these are depicted in Figure 4.1.

Databases used	Search terms
1. ScienceDirect	"Cybersecurity awareness"
2. SpringerLink	"Security awareness key factor"
3. Web of Science	"Cybersecurity awareness raising"
4. IEEE Xplore	"Cybersecurity awareness initiatives"
5. Emerald	"Cybersecurity awareness key factor"
6. ACM	"Cybersecurity culture AND awareness"
	"Cybersecurity awareness literature review"
	"Improving cybersecurity OR cyber security AND awareness"

Figure 4.1: Databases & Search Terms used in the rapid review. (Authors Own).

Furthermore, an 'Inclusion & Exclusion Process,' containing four steps, is followed when determining what literature is deemed relevant enough to include in the rapid review, and this process is depicted in Figure 4.2. This process starts when there is a paper to be evaluated and ends either with the paper being excluded during a step or when the paper has gone through all four steps and is included in the rapid review. Then the end signifies the end of that paper's inclusion and exclusion process, and another paper is next in line to go through the process.

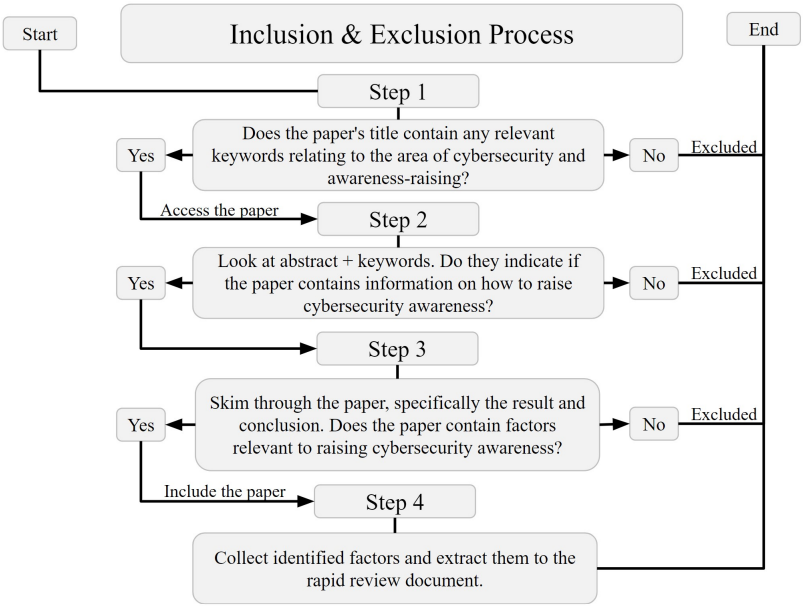


Figure 4.2: Inclusion & Exclusion Process used in the rapid review. (Authors Own).

At the beginning of the 'Inclusion & Exclusion Process,' it was considered to utilize three databases to collect the literature. This is because fewer databases are often preferred when conducting a rapid review; however, after finding it challenging to uncover relevant literature with that number of databases, the databases used were expanded from three to six. The primary reason for including this number of databases and search phrases in the rapid review was

because of the difficulty of finding relevant literature. Thus, it became more heavily focused on searching through as many databases as time allowed with various search phrases in the hope of finding enough relevant literature on cybersecurity awareness-raising to design and develop a guideline. By adhering to the inclusion and exclusion process, many factors pertaining to cybersecurity awareness-raising were identified, collected, extracted, and compiled into a separate document named rapid review. In the end, this thesis' rapid review document included seventy-one extracted papers deemed relevant to cybersecurity awareness-raising. The papers collected from the rapid review are depicted in Table 4.1, and they contain all the cybersecurity awareness-raising factors used to develop the guideline.

Themes	**Papers**
Top Management Support	(Tonkin et al., 2022; Mansfield-Devine, 2017; Renaud, 2018; Grassegger and Nedbal, 2021; Alshaikh et al., 2021; Kemper, 2019; Bakari et al., 2007; Drevin et al., 2007; Arbanas et al., 2021; Dahabiyeh, 2021; Jouaibi et al., 2022; Aldawood and Skinner, 2019; Uchendu et al., 2021; Trim and Lee, 2019; Khando et al., 2021; Caldwell, 2016)
User Participation & Engagement	(Stahl, 2006; Haney and Lutters, 2018; Safa et al., 2015; Safa and Maple, 2016; Kemper, 2019; Alshaikh et al., 2021; Ruighaver et al., 2007; Drevin et al., 2007; Alahmari and Duncan, 2020; Albrechtsen and Hovden, 2010; Dahabiyeh, 2021; Kalhoro et al., 2021; Trim and Lee, 2019; Li et al., 2016; Sardar and Wahsheh, 2020; Caldwell, 2016; Abawajy and Kim, 2010; Cone et al., 2007; Jouaibi et al., 2022; Bada and Nurse, 2019; Cone et al., 2006; Alahmari et al., 2022; Ki-Aries and Faily, 2017; Khando et al., 2021)
Interest & Motivation	(Haney and Lutters, 2018; Furnell and Rajendran, 2012; Alshaikh et al., 2021; Caldwell, 2016; Tolah et al., 2021; Alanazi et al., 2022; Kemper, 2019; de Bruijn and Janssen, 2017; Ruighaver et al., 2007; Drevin et al., 2007; Rohan et al., 2021; Albrechtsen and Hovden, 2010; Parsons et al., 2014; Uchendu et al., 2021; Trim and Lee, 2019; Ki-Aries and Faily, 2017)
Cybersecurity Policies	(Fielding, 2021; Alshaikh et al., 2021; Wong et al., 2022; Rohan et al., 2023; de Bruijn and Janssen, 2017; Bakari et al., 2007; Georgiadou et al., 2023; Rohan et al., 2021; Ahlan and Lubis, 2011; Whitman, 2004; Parsons et al., 2014; Tirumala et al., 2019; Uchendu et al., 2021; Cone et al., 2006; Alzubaidi, 2021; Tolah et al., 2021)

Cybersecurity Education, Training & Awareness	(Solomon et al., 2022; Stahl, 2006; Chaudhary et al., 2022; Tonkin et al., 2022; Adelola et al., 2015; Filipczuk et al., 2019; Sardar and Wahsheh, 2020; Abu-Amara and Tamimi, 2021; Reeves et al., 2021; Safa et al., 2015; Safa and Maple, 2016; Mansfield-Devine, 2017; Renaud, 2018; Caldwell, 2016; Grassegger and Nedbal, 2021; Alshaikh et al., 2021; Abawajy and Kim, 2010; Rohan et al., 2023; Fielding, 2020; Kemper, 2019; Chang and Coppel, 2020; Cone et al., 2007; Rohan et al., 2021; Alahmari and Duncan, 2020; Whitman, 2004; Parsons et al., 2014; Aldawood and Skinner, 2018; Wang et al., 2018; Amjad et al., 2016; Arbanas et al., 2021; Aldawood and Skinner, 2019; Bada and Nurse, 2019; Uchendu et al., 2021; Hart et al., 2020; Cone et al., 2006; Abawajy and Kim, 2010; Alahmari et al., 2022; Scholefield and Shepherd, 2019; Quayyum et al., 2021; Tschakert and Ngamsuriyaroj, 2019; Khando et al., 2021; Alzubaidi, 2021; Furnell and Vasileiou, 2017; Wong et al., 2022; Chung, 2020; Jouaibi et al., 2022; Trim and Lee, 2019; Ki-Aries and Faily, 2017)
Attitudes & Perceptions of Cybersecurity	(Safa et al., 2015; Grassegger and Nedbal, 2021; Tolah et al., 2021; Alshaikh et al., 2021; Furnell and Vasileiou, 2017; Wong et al., 2022; Hall, 2016; Chung, 2020; Alanazi et al., 2022; Furnell and Rajendran, 2012; Bakari et al., 2007; Georgiadou et al., 2023; Rohan et al., 2021; Alahmari and Duncan, 2020; Ahlan and Lubis, 2011; Albrechtsen and Hovden, 2010; Parsons et al., 2014; Chumaera et al., 2022; Wang et al., 2018; Tariq et al., 2014; AL-Nuaimi, 2022; Kalhoro et al., 2021; Kovačević and Radenković, 2020; Kovačević et al., 2020; Hart et al., 2020; Ki-Aries and Faily, 2017; Khando et al., 2021; Safa and Maple, 2016; Caldwell, 2016; Abawajy and Kim, 2010; Aldawood and Skinner, 2018; Jouaibi et al., 2022; Aldawood and Skinner, 2019)

Cybersecurity Culture	(Stahl, 2006; Furnell and Rajendran, 2012; Safa et al., 2015; Safa and Maple, 2016; Power and Forte, 2006; Fielding, 2021; Caldwell, 2016; Tolah et al., 2021; Furnell and Vasileiou, 2017; Abawajy and Kim, 2010; Hall, 2016; Rohan et al., 2023; Fielding, 2020; Chung, 2020; Kemper, 2019; Ruighaver et al., 2007; Bakari et al., 2007; Georgiadou et al., 2023; Rohan et al., 2021; Parsons et al., 2014; Amjad et al., 2016; Arbanas et al., 2021; AL-Nuaimi, 2022; Aldawood and Skinner, 2019; Bada and Nurse, 2019; Kalhoro et al., 2021; Uchendu et al., 2021; Trim and Lee, 2019; Kovačević et al., 2020; Khando et al., 2021)
Cybersecurity Advocates	(Stahl, 2006; Haney and Lutters, 2018; Power and Forte, 2006; Hall, 2016; Arbanas et al., 2021; Bada and Nurse, 2019; Uchendu et al., 2021; Caldwell, 2016; Chang and Coppel, 2020; Kalhoro et al., 2021; Trim and Lee, 2019)

Table 4.1: Papers collected from rapid review.

To create the guideline's first draft based on the information obtained from the rapid review, a process of twelve steps was followed, which is depicted in Figure 4.3. The first action was to go through the rapid review document containing all compiled cybersecurity awareness-raising factors to highlight the frequently mentioned factors, which was done to produce themes according to the most relevant factors. When the goal is to create something well-structured, understandable, and visually appealing, producing themes to make vast amounts of information manageable can be beneficial. It is noteworthy to mention that the papers depicted in Table 4.1 can occur in multiple themes, as one paper can include factors relevant to more than one theme. When themes were produced of the cybersecurity awareness-raising factors identified in the rapid review document, these were extracted to another program, diagrams.net (draw.io), to create a visualization of the guideline. The program diagrams.net provides a web-based diagramming application named draw.io, which offers sketching and diagramming functionalities to create a vast range of visualizations easily. The program also provides the ability to integrate the visualizations with other software like google drive (Draw.io, 2023), which is advantageous as it is the researcher's cloud service to store files. Due to the program's features and the researchers' previous knowledge of the tool, it was chosen for creating the guidelines visualization. After that, the identified themes were placed as boxes in the program, and boxes in this visualization represent the cybersecurity awareness-raising factors, and those boxes were marked green to illustrate them as the principal factors. Then a circular figure was created to clarify that the guideline's purpose is to visualize factors contributing to cybersecurity awareness-raising, and the principal factors were placed so they surround it to symbolize these are the factors contributing to awareness-raising. The arrows enveloping the circle were created to symbolize cybersecurity awareness-raising is a continuous work; hence announcing these factors is something that an organization, such as a large Swedish public organization, needs to continuously work within their cybersecurity awareness-raising efforts.

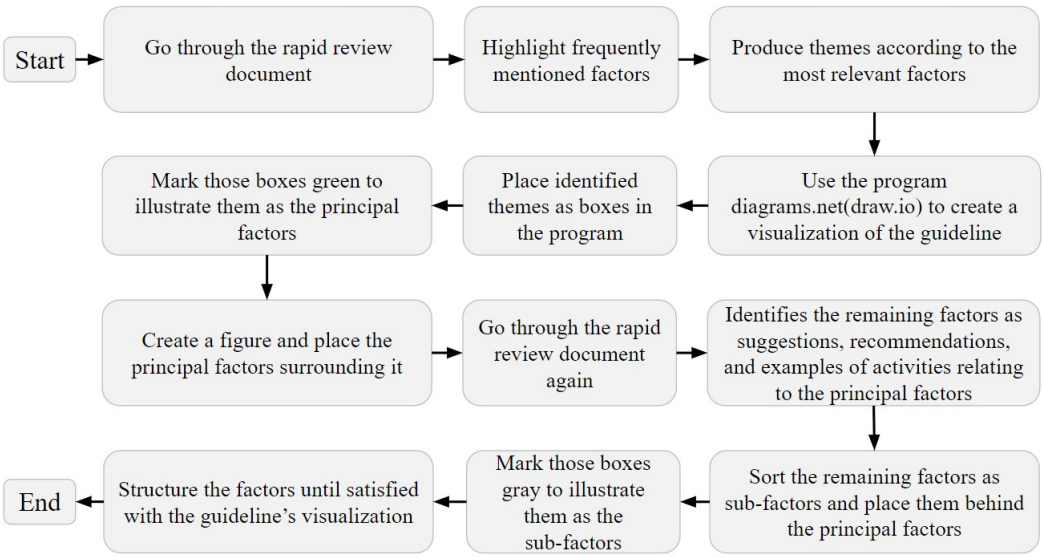


Figure 4.3: The process of creating the guideline's first draft. (Authors Own).

Then, another round of going through the rapid review document took place, which made it possible to identify the remaining factors as suggestions, recommendations, and examples of activities relating to the principal factors. These factors were then extracted from the rapid review document to the diagrams.net program and were represented as sub-factors and then placed in boxes behind the principal factors. The sub-factors were marked gray to illustrate them as the sub-factors more clearly. The color coding was designed to highlight the principal factors with a bright green hue, while the sub-factors were given a subtle grey shade to make them distinguishable from the white background. This helps the viewer quickly identify the key elements in the guideline. The boxes' structure was fine-tuned until the researcher was satisfied with the visualization of the guideline. The end result was aimed to be a well-organized, comprehensible, and visually pleasing representation.

4.1.2 Artefact Demonstration

The first draft of the guideline consists of eight principal factors, which are visualized as green boxes. These are 'Top Management Support,' 'User Participation & Engagement,' 'Interest & Motivation,' 'Cybersecurity Policies,' 'Cybersecurity Education, Training & Awareness,' 'Attitudes & Perceptions of Cybersecurity,' 'Cybersecurity Culture,' and lastly 'Cybersecurity Advocate.' Each of these principal factors contains its own sub-factors, which are visualized as grey boxes, indicating more specific suggestions for what should be included in the different areas of the cybersecurity awareness-raising work. The visualization of the guideline's first draft developed under design cycle one is depicted in Figure 4.4, and a bigger picture of it can be viewed in Appendix A.

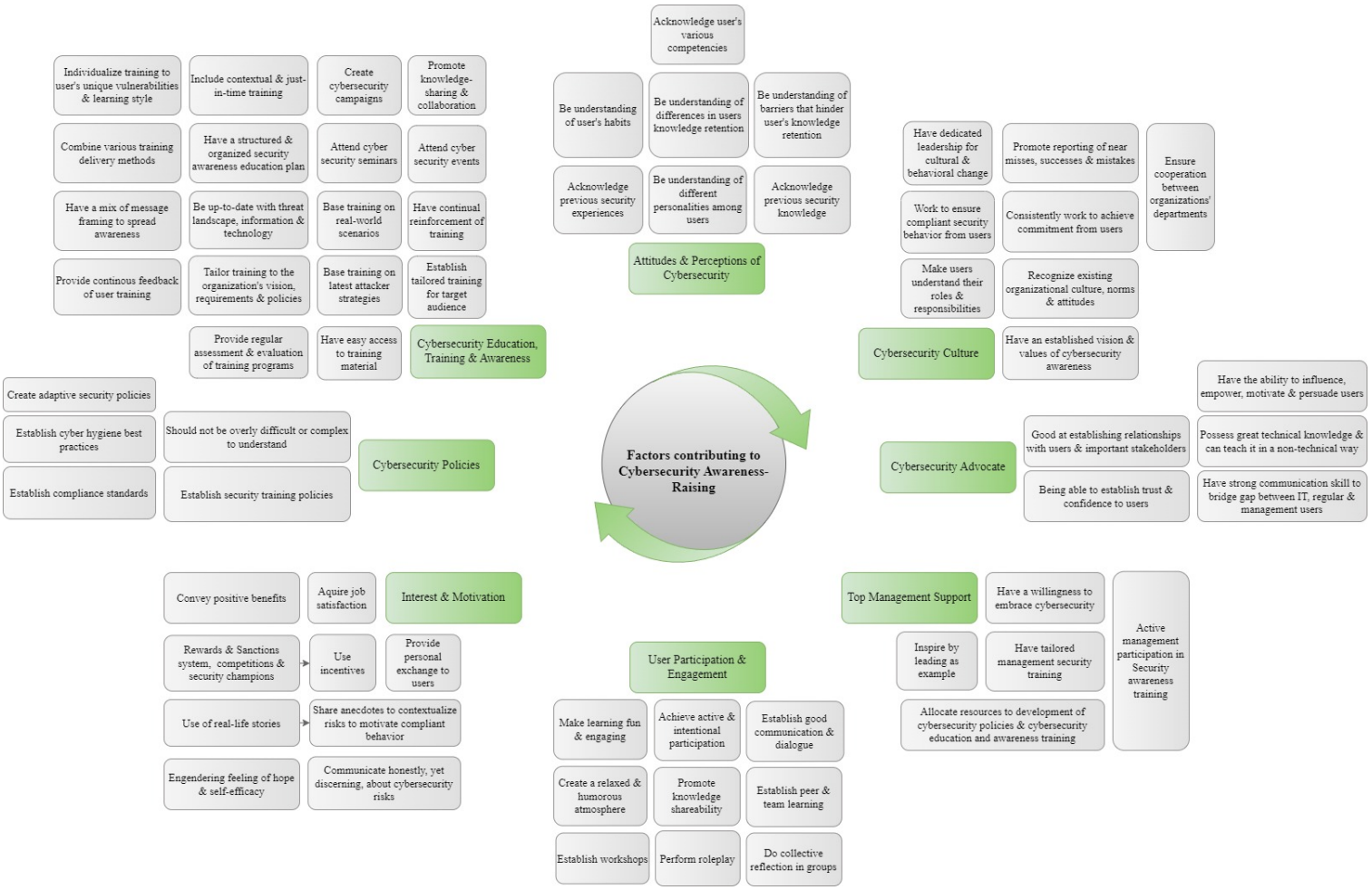


Figure 4.4: Guideline design in design cycle one. (Authors Own).

4.1.3 Evaluation

The guideline's first draft was presented and demonstrated to six interviewees during the demonstration phase for the first time. Meanwhile, the interview questions used during the first design cycle can be viewed in Appendix B, however, note that all interview questions have been translated to English from Swedish as every interview was originally conducted in Swedish. All quotes used in this evaluation have been translated into English from Swedish. After conducting interviews with six experts from three large Swedish public organizations, there has been a lot of information and feedback to partake in during the evaluation phase, especially regarding thoughts and desired changes to the guideline. Each interviewee will be referenced in the text according to Table 4.2.

Interviewed experts:	**Referenced in text as:**
Interviewee One	I1
Interviewee Two	I2
Interviewee Three	I3
Interviewee Four	I4
Interviewee Five	I5
Interviewee Six	I6

Table 4.2: Interviewees linked to their text reference.

Interviewee One

I1 declared that they thought the presented guideline has captured most or all relevant parts regarding the cybersecurity awareness (CSA) work and highlighted that presenting the guideline as eight principal factors makes the guideline, as stated: "It is easier to absorb and understand the guideline when it is broken down into these eight different factors." I1 further assesses that the central goal of the guideline is to raise CSA and concludes that the factors involved contribute to raising awareness. It also mentions that there should not be more principal or sub-factors included in the guideline. However, I1 advocated that the guideline could contain fewer factors to absorb the information easier. Still, I1 can not, as of this moment, say which factors should be removed, only that the guideline should be further defined and clear. Later on, I1 noted a lack of a measurability component for CSA in the guideline and advocated how significant it is to include a measurement to show the positive effect of what is being done because otherwise, the top management will not allow continued work if no value or impact can distinctly be presented. Therefore, adding measurability is a significant success factor that should be included.

Furthermore, I1 believes the presented guideline will be useful for Swedish public organizations to adopt because it highlights eight relevant and important factors to CSA and thoroughly explains what should be included in the CSA endeavor. However, I1 notes that it will be quite demanding to carry out the work practically as there are no clear indications in the guideline as to what area to prioritize first. Still, the logical first step may be toward the top management support because their support is needed before any work can be done. I1 did not express any wrongdoings with the guideline but instead proclaimed that the guideline is based on aspects they have experience working with; for instance, I1 finds an anchoring to recognizable standards, frameworks, and best practices in the guideline, which is good since these are important aspects in the CSA work. Sometime later, I1 realized that the two principal factors, 'User Participation & Engagement' and 'Interest & Motivation,' could be moved together if one wished to minimize the number of factors since they are closely related. However, they could remain separated as they have slightly different approaches and ways of following them up. Lastly, I1 determines the guideline to be comprehensible to understand, providing a good layout while presenting its complexity and would be useful for their organization.

Interviewee Two

I2 mentioned straight away that the two principal factors 'User Participation & Engagement' and 'Interest & Motivation' were quite similar to each other and questioned why those two factors were separated because several sub-factors included in, for instance, 'Interest & Motivation' could also belong in 'User Participation & Engagement,' precisely as I1 also thought. As such, I2 desired to combine the two principal factors. I2 mentioned some confusion with the sub-factors as few seemed to be examples of activities rather than what is to be accomplished per the principal factor. Thus, they suggested trying to improve the sub-factor by making them uniform but overall thought the guideline was good and well summarized. Furthermore, I2 positively reinforced that the concept of cybersecurity advocates, or champions as they liked to name it within their organization, was a great factor to include as it is a classic role many authorities and organizations should have within different parts of their organizations. Because advocates are important to include in an organization's different departments to increase and spread CSA but are, unfortunately, an aspect that many organizations lose sight of. I2 further believes the guideline would be useful for Swedish public organizations to adopt if translated into Swedish. Still, I2 considers the guideline useful and constitutes good support for Swedish organizations. For instance, as stated: "The guideline would act as a good guide for what requirements and activities should be involved for those who want to carry out and build a security awareness program. Then we have, with the aid of the guideline, already identified what activities we could include and how all of these activities relate to one another". Lastly, I2 does not seem to believe anything is wrong with the guideline that should be removed. Rather, it is a comprehensive and understandable guideline with a good layout.

Interviewee Three

I3 pointed out that the first aspect that stood out was how many good areas and factors important to cybersecurity awareness-raising were included in the guideline and that eight factors are enough. I3, for instance, expressed delight in having top management support included because they believe it to be one of the more important factors since it is essential to have good top management support of CSA, especially for CSA to, as stated: "it should trickle down through the entire organization." However, I3 explicitly stated that this notion of 'trickle down' is essential because it indicates it is equally important to have support throughout the organization as it is having support from up top. I3 agrees with interviewees one and two regarding the similarities of the principal factors 'User Participation & Engagement' and 'Interest & Motivation.' I3 proclaimed that the areas contain major overlapping because the factors relating to interest and motivation will undoubtedly lead to increased user engagement and participation and thus contain major dependencies on one another that would be hard to change. Therefore, I3 recommended the best solution to combine the two factors into one principal factor to avoid unnecessary confusion and make the guideline clearer.

Furthermore, I3 seemed to share the same notion as I1 that measurement of the CSA work is lacking in the guideline. I3 states that including a factor of measurement within the CSA endeavor is important. Because organizations rely heavily on producing value and thus need to provide feedback to see whether the organization's overall awareness levels increase depending on what awareness measure is enacted. Moreover, I3 believes the guideline is useful for Swedish public organizations to adopt because it contains relevant factors that should all be included in a CSA venture. I3 mentions, for instance, a public organization could use the guideline to ensure they are heading in the right direction by checking the guideline on what to do next within different awareness areas to act according to the various factors. Lastly, I3 determines

that nothing in the guideline should be classified as wrong, only certain aspects that could be improved. Such as producing more, as stated: "crisp" and "clear delimitations" in conjunction with those aspects previously mentioned, but believes, nonetheless, the guideline to be great, comprehensible to understand, and has a good and simplistic layout.

Interviewee Four

I4's first thoughts on the guideline were that it felt complete. Because there were no aspects that were completely new and thus proclaimed: "I recognize everything, but to see it so put together and compiled on a single page as this is fantastic." I4 continued to mention that the guideline could be useful as a roadmap for how organizations should carry out the awareness work. I4 mention exactly what I1, I2, and I3 previously indicated, which is the overlapping of the two principal factors 'User Participation & Engagement' and 'Interest & Motivation.' I4 also suggested they be added since a few sub-factors within the two principal factors could be used in both areas and thus felt no reason to separate them. Consequently, I4 further pointed out a need to review the guideline's sub-factors and assess whether some could be joined together or kept separate to minimize the number of sub-factors. I4 mentioned that minimizing the number of sub-factors would create an improved guideline because, as stated: "There are a lot of things on one page that makes it very compact and a tad bit intimidating to grasp at first glance and some sub-factors are merely synonyms or examples of another so those could be combined with others, so focus on condensing and reducing the number of boxes without reducing the clarity and meaning of the guideline."

Furthermore, I4 vaguely questions the alignment of this guideline by asking: "How are these factors specific to a public organization?". I4 proclaims that the guideline conveys CSA factors that are good for everyone, whether they are public or private organizations since every organization works with CSA in one way or another. Apart from the mentioned aspects, I4 does not consider anything significant missing from the guideline. After that, I4 started fantasizing about how this guideline could be used as groundwork in future endeavors by further developing the guideline. One possible way to do this would be by breaking down the guideline into checklists covering each sub-factor and providing instructions for how each sub-factor should be carried out. Lastly, I4 believes the guideline to be useful for Swedish public organizations to adopt, despite it possibly being useful for private organizations as well. Because the guideline covers many significant areas that will be useful for CSA work and is comprehensible to understand, and has a good overall layout.

Interviewee Five

I5 uttered that the guideline gave them the impression of it being extensive while appearing easy to grasp. However, when delving deeper into the various factors, I5 realized how complex and intricate the guideline truly is. I5 additionally noted that the guideline included important aspects that should be obvious for an organization to conduct regularly, for instance, implementing real-world scenarios into awareness training. I5 mentioned that this is often not done to the extent needed; therefore, it felt very positive to have it included in the guideline as a sub-factor in training. Furthermore, I5 questioned whether allowing people to make mistakes is sufficiently represented within the 'Cybersecurity culture' factor because I5 feels strongly that people should be allowed to make mistakes and not be singled out. I5 proclaims, as stated: "Mistakes should be acceptable in organizations because we are only human, and through mistakes, we learn and improve." I5 continued to mention the importance of condensing the guideline factors into fewer boxes, as interviewees one and four also thought to simplify the intricate guideline. This seemed

particularly necessary when wanting this guideline to be adopted and used in practice within an organization. Moreover, I5 believes the guideline to be useful for Swedish public organizations to adopt because, as stated: "Through this guideline, we can understand exactly how massive this awareness work is and more specifically what goes into it. The guideline can also act as a guiding hand for the direction of the awareness work by looking at how many factors we already have checked off today and how many more we have to go for us to reach our desired goal". I5 proclaims that the guideline can be used as a groundwork for, for instance, a GAP analysis where an organization's current CSA performance is compared with its desired or expected awareness performance. Lastly, I5 claims that if the guideline is aimed at Swedish organizations, then the language of the guideline should be in Swedish, but otherwise, believe the guideline to be really good, comprehensible to understand, and have a good layout.

Interviewee Six

I6 thought the guideline to be natural and that nothing feels astonishingly out of place since, as stated: "All this is really recognizable and true to what is actually needed in security awareness work so I think all factors are needed and that is great." I6 further points out that all these factors that create the guideline contribute to a cybersecurity culture and are truly needed to raise awareness. However, the guideline can be challenging to work with in practice because, as stated: "Essentially all factors are entwined with each other, so there is a need for the guideline to have better-defined areas if you want to work with it in real life." Furthermore, I6 agrees with I3 that having good top management support is one of the more crucial factors in achieving good CSA throughout the organization. I6 explained that it is essential because when a topic, such as CSA, is communicated by top management and the work has their support, there is a greater chance of more people throughout the organization listening and wanting to adhere to what is being said because it is deemed important. I6 mentions, likewise the majority of interviewees, that the guideline need to make the sub-factors more, as stated: "crisp" and "clear delimitations" and thus should combine the two principal factors 'User Participation & Engagement' and 'Interest & Motivation' and rename it as 'User Participation, Engagement & Motivation.' Because as stated: "There is no great added benefit to distinguish between user participation and engagement and interest and motivation and therefore they should be put together, which also achieves better delimitations."

I6 further proclaims that the 'Cybersecurity Culture' factor is the overall goal of the entire guideline and that the principal factors are merely the awareness-raising factors that contribute toward increasing CSA, which in turn cultivates a cybersecurity culture. As stated: "Getting a better safety culture is almost like the big goal, and that is why we work with all these different factors. Hence why we have great policies, why we have excellent education and training, why we have ambassadors or advocates around the organization, and so further because all that contributes to a better cybersecurity culture". Therefore, I6 believes the guideline could be improved by removing the principal factor of 'Cybersecurity Culture' and clarifying its importance under other factors. I6 is quick to point out that even though culture can be removed as a principal factor, its sub-factors should not be removed along with it because they explain what culture entails. Culture is a vital aspect of the CSA work that should still, in some way, be included. I6 believes the guideline to be useful for Swedish public organizations to adopt because of its great content and relevant factors. However, I6 mentions, as I4 did, that the guideline is not specific to public organizations because it is first and foremost written in Swedish and secondly because it lacks factors relating to how public organizations are managed. I6 explained, as stated: "Public organizations are heavily regulatory driven by laws and regulations that dictate how an

organization should protect and manage their information, and we are required to give out various information if requested by the public, for example, emails between the two of us could be released." Therefore, I6 suggested changing the principal factor 'Cybersecurity Policies' to 'Governance of information' instead of 'Cybersecurity Policies' into a sub-factor. This is because public organizations are revolved around governance, internal and external regulations, and laws such as 'offentlighetsprincipen,' 'Arkivlagen, 'Sekretesslagen,' and 'Samhällsberedskap' etc., and if the guideline wants to be aimed more at public organizations than private, these should in some way be included according to I6. Especially since the primary difference between public and private organizations, according to I6, is that private organizations are not required to give out information the same way as public organizations do since they do not adhere to exactly the same laws and regulations. Lastly, I6 also believes, as the majority of the interviewees do, that the guideline is really good and useful, comprehensible to understand, and possesses a good layout.

Conclusion of Interviews for Design Cycle One

To conclude with a summary of the evaluation, the overall assessment from the six interviewees is that the guideline is quite extensive but really good and useful because it is well summarized, comprehensible to understand, possesses a good layout design, and has captured the most significant and relevant factors important for raising CSA. According to the interviewees, this would make the guideline an incredibly useful guide or groundwork for further development for Swedish public organizations like theirs to adopt. The interviewees all shared this generally positive perception, despite two interviewees slightly questioning how the guideline distinctly applies to Swedish public organizations because they believe it applies to all organizations working with CSA that need guidance. Furthermore, most interviewees seemed to agree that the guideline's areas needed to be more clearly condensed and delimited, which would be achieved by reducing the number of boxes by either removing or combining them. There were also a few suggestions made for change that the interviewees thought necessary to improve the guideline, but overall, they agreed that nothing in the guideline was inaccurate.

4.2 Design Science Cycle 2

In 'Method Development,' the second design cycle focused on selecting feedback acquired from the first design cycle's evaluation phase and incorporating it into the guideline's design to further refine and enhance the guideline's development. In 'Artifact Demonstration,' a second demonstration of the guideline's second draft was conducted through interviews. The interviews were with the same six cybersecurity awareness experts working at large Swedish public organizations as in design cycle one to receive final feedback and validation regarding the guideline. In 'Evaluation,' a second evaluation was conducted by presenting and analyzing the received thoughts and feedback from the interviewees to incorporate the new and in-depth feedback to further refine and enhance the guideline before communicating the final results. When the evaluation phase is concluded, it signifies the end of the design cycles for this thesis.

4.2.1 Method Development

After concluding design cycle one, the six interviewees gave lots of feedback that needed to be evaluated to determine which feedback should be included or excluded from being incorporated into the guideline's second draft. Based on information acquired from the interviewees and presented in design cycle one's 'Evaluation' sub-chapter, there were three bigger changes to be made, and some changes required multiple steps to achieve.

First Change

The first change was to improve the guideline's clarity and simplicity by condensing and delimiting its content, as the guideline was extensive and contained much information that could be simplified. The first step to condense and delimit the guideline was combining the principal factors 'User Participation & Engagement' and 'Interest & Motivation' into one factor, as all interviewees had voiced this suggestion. They proclaimed that those two areas contained significant overlapping since their sub-factors were too similar for them to have sufficient reason for being separated. As such, the two principal factors and their sub-factors were combined into 'User Participation, Engagement & Motivation' as one interviewee had suggested. To further condense and delimit the guideline, all sub-factors under each principal factor were looked over, specifically under 'User Participation, Engagement & Motivation,' as was suggested by the interviewees. This resulted in several boxes being removed, primarily sub-factors that seemed to be merely synonyms or examples of another, which were an aspect that a few interviewees previously took notice of.

The second step of condensing and delimiting the guideline was by removing the principal factor of 'Cybersecurity Culture,' as interviewee number six mentioned. The reason for this choice was that I6 was right that the indirect goal of the guideline becomes the cultivation of a cybersecurity culture since all remaining factors, even after removing culture, together produce the most relevant factors for raising cybersecurity awareness (CSA). Because when 'Cybersecurity Culture' becomes the goal of the awareness-raising activities, that factor does not belong on the same level as the remaining principal factors. Therefore, the principal factor seemed correct to remove, but instead of removing all its sub-factors along with the green box, the most relevant sub-factors were spread out to other areas. A few of the culture's sub-factors were spread out to, for instance, 'Top Management Support' and 'User Attitudes & Perceptions of Cybersecurity.' This was because some sub-factors related better to management due to linking to leadership, vision, and goals. At the same time, other sub-factors related better to user attitudes due to linking to attitudes, norms, culture, and reporting of mistakes.

Second Change

The second change was to the principal factor 'Cybersecurity Policy' because of wanting to specify and adjust the guideline more towards public organizations as this was an important criticism that was received. As suggested by I6, the principal factor formerly known as 'Cybersecurity Policy' has been renamed 'Governance of Information.' This change was made because public organizations are largely governed and regulated by external and internal laws and regulations that impact their cybersecurity work. These laws and regulations include 'GDPR,' 'offentlighetsprincipen,' 'Arkivlagen, 'Sekretesslagen,' and 'Samhällsberedskap' other EU legislation. Therefore, including these sub-factors seemed suitable. It was especially vital to include 'offentlighetsprincipen,' as, according to I6, it is a law that only public organizations are required to adhere to. Based on this, three sub-factors were created under 'Governance of Information.'

The first was 'Adhere to external laws & regulations for the management of information (GDPR, EU legislation),' the second was 'Adhere to internal laws & regulations for the management of information (offentlighetsprincipen, sekretesslagen, arkivlagen), and the third was 'Establish community preparedness (samhällsberedskap) regulations.'

Third Change

The third change was creating a sub-factor named 'Measure effects of cybersecurity awareness work' because interviewee number one had expressed how important incorporating measurement of the cybersecurity work is. Because showing the effects of the implemented awareness-raising activities is an essential success factor and was, therefore, included in 'Top Management Support.' The sub-factor was placed under management as these measurement results affect whether the management will continue with a certain awareness-raising activity. Furthermore, the layout structure was slightly changed due to having minimized the principal factors from eight to six. Lastly, there were no underlying thoughts on how the principal factors were initially positioned other than 'Top Management Support' being at the top because two interviewees mentioned that factor as one of the more important factors for CSA.

4.2.2 Artefact Demonstration

The second draft of the guideline consists of six principal factors, which are visualized as green boxes. These are 'Top Management Support,' 'User Attitudes & Perceptions of Cybersecurity,' 'Cybersecurity Advocate,' 'User Participation, Engagement & Motivation,' 'Governance of Information,' and lastly 'Cybersecurity Education, Training & Awareness.' Each of these principal factors still contains its own sub-factors, which are visualized as grey boxes, indicating more specific suggestions for what should be included in the different areas of the cybersecurity awareness-raising work. The visualization of the guideline's second draft developed under design cycle two is depicted in Figure 4.5, and a bigger picture of it can be viewed in Appendix C.

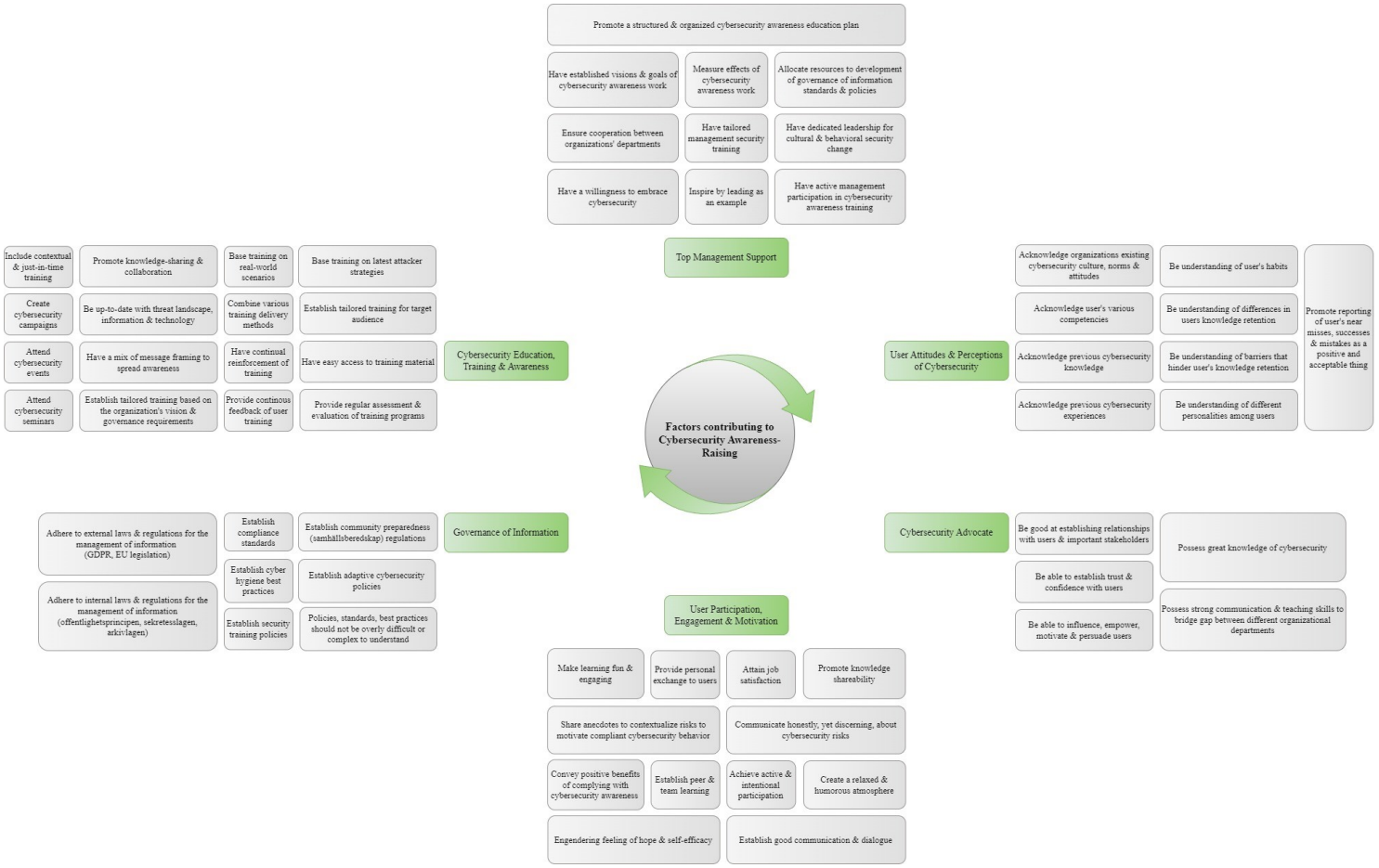


Figure 4.5: Guideline design in design cycle two. (Authors Own).

4.2.3 Evaluation

The guideline's second draft was once more presented and demonstrated to the same six interviewees as was done during the demonstration phase for the first design cycle. Meanwhile, the interview questions used during the second design cycle can be viewed in Appendix D. All quotes used in this evaluation have been translated into English from Swedish. After conducting the second set of interviews with the same six experts from the three large Swedish public organizations, additional information has been gathered regarding desired changes to the guideline. Each interviewee will continue to be referenced according to Table 4.2, as previously done in the evaluation phase for design cycle one, to uphold a similar structure while preserving the interviewees' anonymity.

Interviewee One

I1 proclaimed that they greatly approved of reducing the number of principal factors from eight to six by combining 'User Participation & Engagement' with 'Interest & Motivation' and removing 'Cybersecurity Culture' because, as stated: "The fewer areas there are, the easier is it to

remember, rehearse, and guide others who will inherit and adopt the guideline further down the line about how it works." I1 continued to share how effective fewer factors can be in a guideline compared to a larger amount and explained how the NIST Cybersecurity framework with only its five factors had been deemed great by countless security professionals regardless of its few factors. The point that I1 seems to make is that fewer and more condensed factors are more understandable and sought-after than a larger amount, which makes a guideline with those capabilities more valuable and sought-after. I1 further states that removing 'Cybersecurity Culture' as a principal factor and spreading its sub-factors across the guideline was the right move for two reasons. Firstly, because it makes the guideline more condensed and easier to read, as mentioned, and secondly, the remaining factors demonstrate more clearly their contribution toward awareness-raising by cultivating a cybersecurity culture. As I1 stated: "When you have awareness training, top management, user attitudes, advocates, governance, and user participation and engagement and work with it on an ongoing basis, then you improve peoples cybersecurity awareness (CSA), which in turn provides a change in culture towards a more cyber-secure culture." However, an aspect that I1 suggested adding was to better clarify that culture still exists and is extremely relevant in the guideline by either expressing the notion of culture into the middle circle of the guideline that represents continuous work or by adding some form of a near transparent box that stretches across the entire guideline to illustrate that, as stated: "That this whole package, with these awareness-raising factors, creates a cybersecurity culture in an organization."

I1 mentions that it was better to rename the principal factor 'Cybersecurity Policies' into 'Governance of Information' and focus heavier on governance as a whole than simply focusing on security policies because governance includes, for instance, the use of management systems, adhering to internal and external regulations which are incredibly important in public organizations. I1 further declares that including laws and regulations is a good change to make the guideline more applicable for public organizations. However, I1 declares there are no such things as external laws or internal laws. Additionally, I1 proclaims that the guideline has countless possibilities for future work because it raises the curiosity of how one could work with CSA, as stated: "When or where do we in an organization start working with the guideline and what does the timeline for such work look like in order to make the best use of it." I1 continues by saying that possible future work with the guideline would be to break down each area and produce checklists for each principal factor's sub-factors with a detailed description of how to work with them. Otherwise, I1 is pleased that a measurability factor has been added to 'Top Management Support.' I1 further considered the guideline to be greatly improved compared to the guideline's earlier version by adding missing factors and minimizing the number of factors, producing a more delimited, coherent, and well-structured guideline. Lastly, I1 continues to believe the guideline to be a good and extensive groundwork that will be of great use to Swedish public organizations as a guiding tool for cybersecurity awareness-raising while continuing to be comprehensible to understand.

Interviewee Two

I2 thought that it became, as stated: "Much better and clearer" by combining the two principal factors 'User Participation & Engagement' with 'Interest & Motivation' and removing unnecessary factors such as examples because the guideline became better defined with much-improved delimitations. However, I2 further mentions that the sub-factors need to be carefully checked to produce more uniform factors since there are minor instances where factors continue to be formulated as examples of activities rather than as goals to be accomplished. I2 further declares that they agree with removing the 'cybersecurity culture' principal factor because the sub-factors incorporating culture into the guideline remain. However, it could be made slightly clearer since

it is a fundamental building block for raising CSA. I2 believes that a few sub-factors under the principal factor 'Governance of Information' could be grouped, for instance, adding the factors relating to compliance standards, cyber hygiene best practices, and security training policies into one. I2 continues on this path and suggests having one factor that contains laws and internal and external regulations contrary to having them separated because that would be yet another chance to minimize the amount of, as stated: "Redundant factors that could easily be grouped together instead," and I2 continued to state: "And while you are at it you should also simplify the text explanations a bit as some are confusing to what you mean." Essentially I2 means that certain factors, such as 'Policies, standards, best practices should not be overly difficult or complex to understand,' are written in a way that confuses the user about the meaning and should, therefore, simplify the text. Furthermore, I2 declares that 'Establish community preparedness regulations' is termed 'civil preparedness' and should fall under internal regulations rather than being its own factor and suggests changes to be made. Other changes I2 mentioned were related to 'Cybersecurity Advocate' by suggesting changing advocate to plural instead of singular due to it being, as stated: "It is the structure of advocates we are looking for, where these advocates are placed on different levels of an organization to drive the CSA work further, therefore, it should not be singular as that suggests we only mean one single person doing the job." Otherwise, I2 regards the guideline to be improved compared to the first draft because of being better defined with better delimitations and contains very relevant and important factors for raising CSA, which can be useful for organizations to get a better grasp on what is included in the awareness work as an overview. Lastly, I2 means that the guideline is a good groundwork for continued work where it develops to be used practically. They further state that the guideline has a good layout and is comprehensible to understand.

Interviewee Three

I3 pointed out that it was the right choice to combine the two principal factors 'User Participation & Engagement' with 'Interest & Motivation.' Because the removal of principal factors and sub-factors created a guideline with crisp, better-defined, and clear delimitations, which improved the guideline greatly compared to the previous draft. However, I3 noted instances where factors could be further defined and crisped, such as the principal 'Governance of Information' sub-factors. As I3 stated: "In that area, there are five boxes beginning with 'establish' so you could either remove 'establish' in the text or merge them together into one factor of 'establishing' various kinds of policies. Just make sure the guidelines language is consistent". I3 additionally thought that a sub-factor under 'Governance of Information' should be added relating to information security management systems to make the guideline further applicable to Swedish public organizations. I3 mentioned removing the parenthesis in the internal law and external law boxes as they seem to be examples of laws and regulations and that the factors 'Adhere to external laws & regulations for management of information' and 'Adhere to internal laws & regulations for management of information' need to be looked over. I3 mentioned those factors to be looked over because they are probably wrong due to the researcher having misunderstood the context when creating them. I3 explained that if one intended to create a factor containing international laws and regulations, one does not name them 'external'; the same applies to naming national laws and regulations as 'internal.' I3 states: "When talking about external and internal regulations, you talk in context to the organization itself. So an organization is governed by external laws and regulations such as GDPR, other EU legislation, and Swedish laws while also being governed by internal regulations which are specific to the organization in the form of internal regulations, policies, rules, and so on".

Therefore, I3 strongly suggests either removing the existing factors and replacing them with a factor named 'Laws, regulations & Recommendations' or renaming them to 'international laws and regulations' and ' national laws and regulations.' I3 further suggested adding the factor 'Establish community preparedness regulations' under national laws instead and minimizing the number of factors. Furthermore, I3 was at first undecided whether they liked the removal of the principal factor 'Cybersecurity Culture' because, as stated: "It is such an important factor for raising people's awareness so it should preferably be included." However, I3 later noted rather happily that culture's sub-factors were still included in the guideline, which seemed to reduce fears that culture would disappear entirely. Nevertheless, I3 stated that culture should somehow be better clarified regardless of being removed as a principal factor due to its importance in cultivating CSA. The outlook on removing two principal factors seems to be a positive change at last, according to I3, because a guideline with fewer factors is preferred to a guideline with a significant amount of factors. Because otherwise, it will be, as I3 stated: "a too messy guideline with a too high detail level which is not something that facilitates understanding." Lastly, I3 firmly believes the guideline has a good layout, is comprehensible to understand, and is useful for their and other Swedish public organizations as the guideline covers areas important to CSA quite well. As stated by I3: "You are definitely not out cycling because you really know what you are talking about and have made a useful guideline applicable for public organizations. The question is only regarding how to minimize the factors even further to make it easier to absorb because your guideline is complex and very well done, but it is like a tsunami of information".

Interviewee Four

I4 declared the changes made to the guideline to be generally positive because, as stated: "You have structured the guideline up a bit and reduced the number of total boxes, both sub-factors and principal factors, which is perfectly reasonable and I think that is a change in the right direction." As such, I4 seemed quite positive with the primary changes of combining the two principal factors 'User Participation & Engagement' with 'Interest & Motivation' and the reduction of factors that were deemed unnecessary, such as examples and synonyms, thereby making the guideline better than the previous draft and better condensed. I4 further mentioned that the principle factor 'Governance of Information,' even if that terminology is correct, could be changed to simply 'Governance' to simplify it. I4 thought it slightly unnecessary to limit the factor solely to the governance of information instead of including governance as a whole, especially when laws and regulations are involved. I4 mentioned, as I3 did, that using the terms external and internal as done in this context opens up confusion and should therefore term it either as 'International Laws & regulations' and 'National Laws & Regulations' or combine them into one factor and discard the distinction between international and national. Furthermore, I4 thought the changes made to the guideline, as previously mentioned, to be generally positive because they found it quite surprising for the principal factor 'Cybersecurity Culture' to be lacking. I4 stated that the choice to remove the factor was, in the end, a correct choice because the remaining principal factors and their sub-factors undoubtedly demonstrate their contribution toward awareness-raising and that cultivating a cybersecurity culture did indeed seem to be the goal of the guideline. However, despite understanding why the culture factor was removed, I4 states: "In your context, I think you are right to remove the culture factor, but I tend to greatly advocate the importance of culture because I work very hard with it so I know how incredibly important it is to have to be able to succeed with CSA. Therefore, I understand and accept the choice you made, but I still feel as if you should have it more clearly mentioned in some way". I4 suggested the same thing as I1, I2, I3, and I4 did, which was to clarify that culture is still included in the guideline and that this is done more clearly than simply having a few

sub-factors related to culture. Only then would I4 seem to wholeheartedly agree with removing that factor. Consequently, I4 mentioned that culture could be added to the middle circle of the guideline and call the green arrows culture or draw a cloud-like figure that covers the entire guideline, similar to a blanket according to I4, that symbolizes that all factors included in the guideline contribute to a cybersecurity culture. Moreover, I4 mentioned examples of how the continuous endeavor of this guideline could be done because they believe this guideline could become, as stated: "A fantastic guide for public organizations to use in their CSA work because all areas included are very relevant and I know for a fact there are many who need guidance in the CSA work." According to I4, this continuation work has a natural path toward creating a roadmap portraying where an organization currently is, where they desire to be, and how and with what factors one should start the CSA work with. I4 strongly believes the guideline could easily be used in other future endeavors, such as the previously mentioned roadmap, to create a guideline that is used practically by providing a step-by-step checklist for all the guideline's factors. Then organizations could use these checklists to determine the next steps of how their CSA work should proceed. Lastly, I4 considers the guideline comprehensible to understand with a much-improved layout and content.

Interviewee Five

I5 affirmed the changes made to the guideline have been considerably better because, as stated: "You have more clearly delimited the different factor areas so they are more comprehensible as to what they mean and that is an art in itself to succeed in, and I think you have done so." I5 continues to explain the importance of succeeding in that aspect because it is challenging to create a vast guideline as this and do so in a way that readers understand the meaning of factors without having a separate sheet explaining their interpretations. I5 further mentions that the guideline has become clearer due to combining the principal factors 'User Participation & Engagement' with 'Interest & Motivation.' However, I5 did not mention that aspect previously, and due to removing factors to condense the guideline factors into fewer boxes. I5 mentioned the importance of avoiding the concept of 'the more, the merrier' because adding more than necessary is not something one should do, mainly because comprehension of the visualization will decrease. Furthermore, regarding the removal of the principal factor 'Cybersecurity Culture,' I5 uttered that it was a positive change because the remaining factors still convey the meaning of achieving a cybersecurity culture, even if it is not expressed as a principal factor. I5's interpretation is that the entire purpose of the guideline is to reduce or prevent risk and that this is done through achieving a good cybersecurity culture, which in turn is established and cultivated by the awareness-raising factors included in the guideline. After that, I5 noted the guideline still contains factors with dependencies to each other; for instance, in 'Top Management Support,' there are sub-factors that must be implemented first because other factors depend on them to succeed. Solving this aspect of 'what to do first' would be greatly needed, according to I5, either now or in future endeavors, to produce a guideline that can continue to be useful for guiding organizations in their CSA work. For instance, I5 once again proclaims the guideline to be incredibly useful as groundwork for a GAP analysis to, as stated: "To see what the journey of an organizations awareness work looks like, and through your guideline be able to see where we are, what activities we want to do, in what order, and where we want to reach." Lastly, I5 continues to believe the guideline to be very useful for public organizations like their own and that the guideline is comprehensible to understand with an improved layout.

Interviewee Six

I6 expressed that the changes made to the guideline were substantially better than the first draft because the guideline incorporated much of the feedback previously given, producing more delimited, crisped, and clear areas. As I6 stated: "The guideline has improved substantially because you have removed or combined things that were similar to already existing sub-factors and perhaps did not contribute as much, so good job." I6 was, therefore, positively inclined that the two principal factors 'User Participation & Engagement' and 'Interest & Motivation' were combined, the removal of the principal factor 'Cybersecurity Culture' and changes made to the previously named principal factor 'Cybersecurity policies.' I6 noted, regarding 'Cybersecurity Culture,' that it was the correct choice to remove it, as stated: "I do not feel like you are missing any green principal factor as its sub-factors are still incorporated in other areas to indicate the importance of culture. This makes me understand that all these factors contribute to increased CSA, which goes hand in hand with a better and improved cybersecurity culture". However, I6 mentioned that it could be possible to add culture into the green middle circle of the guideline to clarify culture if wanted because then the circle would symbolize that culture is a part of the main goal of the guideline. An aspect that I6 strongly advocated to be incorporated into the guideline was related to the principal factor 'User Participation, Engagement & Motivation.' In this principal factor, I6 advocated that a sub-factor regarding allocating time to training should be added because, as stated: "It is an important factor to ensure that people actually do the training and other awareness-raising activities, that you actually get time reserved each week to do it because it is important to feel that you have the time to prioritize training." I6 further stated that people often feel they do not have time to regularly allocate an hour to training because of other duties and thus do not engage in training until it becomes imperative.

Therefore, I6 strongly believes that a sub-factor regarding the allocation of time reserved each week for CSA training is essential to include, as this notion is a regular occurrence in organizations. According to I6, this sub-factor should be placed under user participation. However, it was noted that depending on the perspective, it could also be placed under the principal factor, 'Top Management Support.' The reason is that if the manager communicates the importance of allocating time to partake in awareness-raising activities, more employees may be inclined to do so, as approval from the boss acts as an incentive to comply. Furthermore, I6 questioned whether incentives should be included in the sub-factor 'Provide personal exchange to users' in 'User Participation, Engagement & Motivation.' Because as I6 stated: "Do incentives only have to be a personal exchange in order to motivate or engage? This formulation sounds like the only way to motivate or engage someone is by giving them positive incentives in exchange". I6 explains that positive and negative incentives motivate and engage people to comply in an organization. For instance, people may receive positive incentives like salary increases or certifications for participating in cybersecurity awareness activities. On the other hand, there could be negative incentives in the form of compulsory work obligations that involve mandatory participation in certain awareness-raising activities required for a specific job. Consequently, individuals may be motivated to participate due to the obligation, which can be considered an incentive, albeit not in the positive sense typically associated with incentives. Therefore, I6 believes the sub-factor of 'Providing personal exchange to users' should be relocated to 'Top Management Support' as only management can provide personal exchanges as salary incentives or compulsory activities to users. Instead, I6 suggests creating another sub-factor under 'User Participation, Engagement & Motivation' named 'Incentives,' which includes the positive and the negative incentives used to motivate and engage users to participate. Moreover, I6 was in agreement with what I3 stated regarding 'Governance of Information,' which was that the two sub-factors of external and internal

laws could be combined into one single factor named 'Laws & Regulations' rather than having it divided because one does not term international and national laws as external and internal. I6 mentions, however, that the guideline could be difficult to use in practice at present because it is somewhat lacking in where one should start and what the next moves are. Although, the guideline does provide a great groundwork for the continued development of a more detailed 'how to' or 'step-by-step' guideline, according to I6. Lastly, I6 considers the guideline to be great because it contains areas that are extremely relevant and recognizable to cybersecurity awareness-raising and provides a great overview of the complex CSA work in a comprehensible layout.

Conclusion of Interviews for Design Cycle Two

To conclude with a summary of the evaluation, the overall assessment from the six interviewees is that the updated guideline is greatly improved compared to the guideline's earlier draft due to having incorporated many of the suggested changes to condense, clarify and simplify the guideline. According to the interviewees, these changes have created a guideline that is still comprehensible to understand and contains extremely relevant and important factors for raising CSA but does so in a slightly more condensed manner. Because of these qualities, there is unanimity among the interviewees that the updated guideline would undoubtedly be a useful tool for Swedish public organizations. Not to mention, the interviewees seemed to agree that focusing on condensing the guideline's content by removing and combining factors has yet again produced better delimited, crisped, and clear areas without sacrificing the guidelines meaning or coherency while continuing to uphold a good and structured layout design. As mentioned, the general consensus among the interviewees is that the changes of, for instance, reducing the number of principal factors by combining 'User Participation & Engagement' with 'Interest & Motivation and creating the principal factor 'User Participation, Engagement & Motivation' have been especially positive. Furthermore, it was perceived as positive to add a measurability factor for the effects of CSA to top management support, renaming the previous principal factor 'Cybersecurity Policies' into 'Governance of Information' and including laws and regulations to produce a guideline more specific to public organizations.

However, a few interviewees have regarded certain changes with apprehension. This apprehension specifically concerns having removed 'Cybersecurity Culture' as a principal factor since all interviewees agree that it is an extremely important aspect of cybersecurity awareness-raising. While the majority of interviewees wholly support the choice of removing 'Cybersecurity Culture,' since culture indirectly becomes the overall goal of the guideline and does not belong at the same level as the remaining principal factors, they nevertheless believe culture ought to be clarified that it is still incorporated in the guideline in some way. Lastly, a majority of interviewees expressed a desire to continue developing the guideline to make further improvements; however, they understood that is beyond the scope of this thesis. The interviewees suggested a few aspects of improvement they thought should be incorporated into the guideline's final draft. These changes related to 'Governance of Information,' 'User Participation, Engagement & Motivation,' and 'Top Management Support.' The changes to 'Governance of Information' primarily related to grouping sub-factors to delimit factors further, correcting a few inaccuracies within the sub-factor's content, and simplifying the principal factor by renaming it to 'Governance.' The changes to 'User Participation, Engagement & Motivation' primarily related to adding a sub-factor regarding users allocating time to CSA training and relocating the sub-factor 'Provide personal exchange to users' to 'Top Management Support' and instead adding a sub-factor named 'Incentives.' The changes to 'Top Management Support' primarily relate to adding the sub-factor 'Providing personal exchange to users' and adding a sub-factor relating to the man-

ager's involvement with allocating the time for users. Additional aspects of improvement that interviewees suggested incorporating in the guideline were carefully reviewing the guideline's factors to determine if additional factors could be combined to further delimit and condense the guideline. Most interviewees also expressed the desire to emphasize that culture is still integrated into the guidelines in some manner due to its importance. Furthermore, they suggested reviewing all the guidelines factors to see if they are uniformly and clearly written.

4.3 Communication of the Final Results

Before concluding design cycle two, the interviewees suggested seven areas where the guideline needed improvement, and it was determined those aspects were relevant enough to be incorporated into the guideline's final draft.

The Seven Changes Made

The first and biggest change made to the guideline involved clarifying 'cybersecurity culture.' This was done by incorporating cybersecurity culture as a blue box. This box was placed underneath to emphasize that cybersecurity culture encompasses all awareness-raising factors because they indirectly contribute to creating and nurturing a cybersecurity culture when performed. The second change was enclosing the blue box in a white box to signify that the entire guideline, with the culture surrounding the awareness-raising factors, falls under the umbrella of cybersecurity awareness. The third change involved reviewing each factor to determine if the language clearly portrayed the desired meaning. Upon review, it was discovered that the text of multiple factors could be clarified. As a result, a significant number of factors' texts were altered. The fourth change involved the principal factor, 'Governance of information,' because several changes were made. Firstly, the principal factor was renamed 'Governance' to simplify it. Secondly, the previous inaccuracies in the sub-factors, 'Adhere to external laws & regulations for the management of information,' were changed to 'Adhere to international & national laws, regulations & recommendations for an organization's governance.' While the other sub-factor, 'Adhere to internal laws & regulations for the management of information,' were changed to 'Adhere to internal policies, standards, procedures, best practices & other recommendations for an organization's governance.' Thirdly, five sub-factors concerning standards, best practices, policies, and regulations were removed as they would be included in the remaining two sub-factors, thus considerably delimiting the area. The fifth change involved adding the sub-factor 'Allocate time to cybersecurity awareness training' and the sub-factor 'incentives' to 'User Participation, Engagement & Motivation.' The sixth change involved adding 'Ensure users allocate time to cybersecurity awareness training' and the sub-factor 'Decide on personal exchange incentives with users' to 'Top Management Support .' The seventh and last changes related to visualization, making the factors smaller and the areas more boxed-in.

Final Result

The final result for the guideline is depicted in Figure 4.6 and consists of six principal factors visualized as green boxes. These are 'Top Management Support,' 'User Attitudes & Perceptions of Cybersecurity,' 'Cybersecurity Advocates,' 'User Participation, Engagement & Motivation,' 'Governance,' and lastly 'Cybersecurity Education, Training & Awareness.' Each of these principal factors contains its own sub-factors, which are visualized as grey boxes, indicating more specific suggestions for what should be included in the different areas of the cybersecurity awareness-raising work. Cybersecurity culture is incorporated in the guideline as a blue box

placed underneath to emphasize that cybersecurity culture encompasses all awareness-raising factors because they indirectly contribute to creating and nurturing a cybersecurity culture when performed. The white box enclosing the blue box signifies that the entire guideline, with the culture surrounding the awareness-raising factors, falls under the umbrella of cybersecurity awareness. In addition, an in-depth explanation for all six principal factors will be held below, and each principal factor will have an enlarged image of its corresponding visualization depicted in Figure 4.6. A larger visualization of the guideline's final result can be viewed in Appendix E.

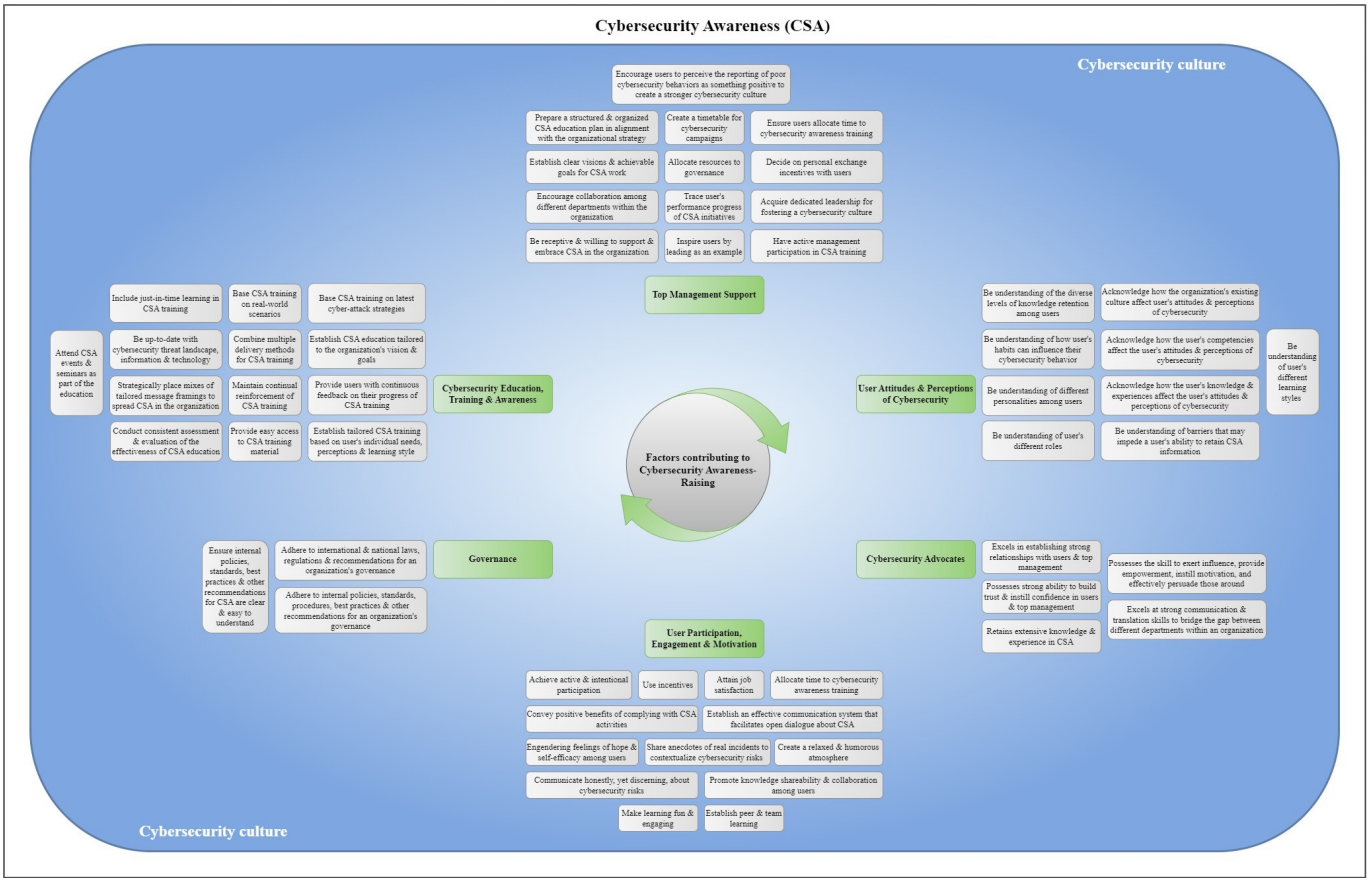


Figure 4.6: Guideline design final result. (Authors Own).

4.3.1 Top Management Support

Research and cybersecurity experts have both verified that 'Top Management Support' is a crucial principal factor in raising cybersecurity awareness (CSA). This principal factor encompasses twelve underlying sub-factors that provide valuable recommendations for what should be incorporated into this area when utilizing the guideline. A visualization of 'Top Management Support' is depicted in Figure 4.7.

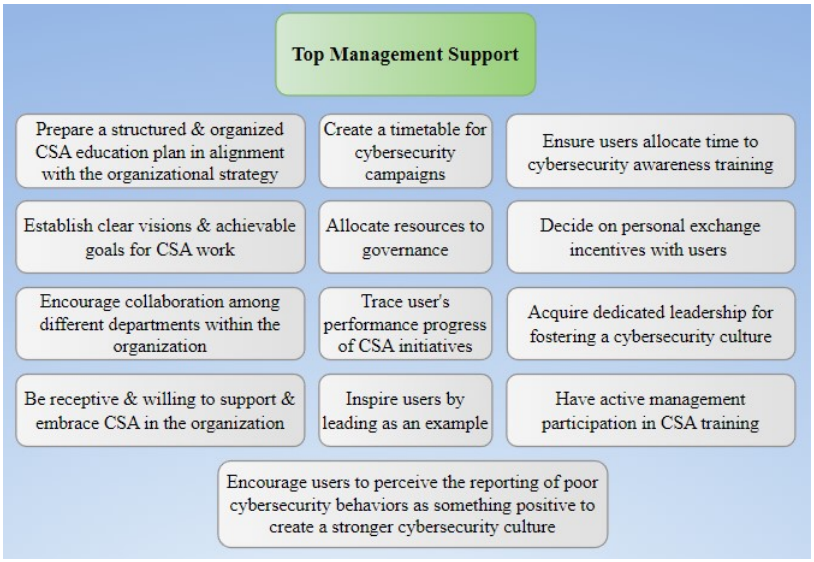


Figure 4.7: Final Result - Top Management Support. (Authors Own).

It has been acknowledged that top management support is essential for promoting positive CSA behavior in organizations (Jouaibi et al., 2022). This is because the support of top management has been proven to yield increased CSA and compliance with CSA best practices in organizations. It has been further stated that top management has the authority to mobilize or allocate funds for CSA. Therefore, they must prioritize facilitating the necessary resources required for CSA development (Khando et al., 2021). This aspect is, for instance, represented in the guideline by the sub-factor 'Manage allocating resources.' Furthermore, the sub-factor 'inspire users by leading as an example' relates to the top management actively leading an example to the rest of the organization by engaging in CSA and actively participating in CSA endeavors to inspire others to follow their behavior. Khando et al. (2021) reinforces the importance of managers displaying leadership because it is important to be a role model to motivate, engage, and raise employees' CSA. Khando also mentions that managerial security participation has one of the strongest effects on employees' awareness and that top management participation strengthens the relationship between an organization's cybersecurity efforts and the increase of CSA. Khando declares that when top managers are willing to embrace CSA efforts by volunteering to be part of them, it serves as a catalyst for enhancing an organization's CSA. If they are not willing or engaged, then the employees are very likely to not better their CSA behaviors (Khando et al., 2021). These two aspects are represented in the guideline. For instance, the first aspect regarding managerial security participation is included in the sub-factor 'Have active management participation in CSA training.' Because as previously mentioned, it is extremely important to have management actively participating in CSA efforts as it greatly influences raising CSA in

an organization. The second aspect regarding managers being willing to embrace CSA efforts is included in the sub-factor 'Be receptive & willing to support & embrace CSA in the organization,' as previously mentioned, greatly enhances an organization's CSA. Khando et al. (2021) continues saying that top management support is critical for making cultural changes possible (Khando et al., 2021). The guideline represents this aspect with the sub-factor 'Acquire dedicated leadership for fostering a cybersecurity culture.' Because without the support of top management, no measures would perhaps be taken to foster a cybersecurity culture, such as hiring a person or placing more responsibilities on people to work with cultivating and fostering a cybersecurity culture.

4.3.2 User Attitudes & Perceptions of Cybersecurity

Research and cybersecurity experts have both verified that 'User Attitudes & Perceptions of Cybersecurity' is a crucial principal factor in raising cybersecurity awareness (CSA). This principal factor encompasses eight underlying sub-factors that provide valuable recommendations for what should be incorporated into this area when utilizing the guideline. A visualization of 'User Attitudes & Perceptions of Cybersecurity' is depicted in Figure 4.8.

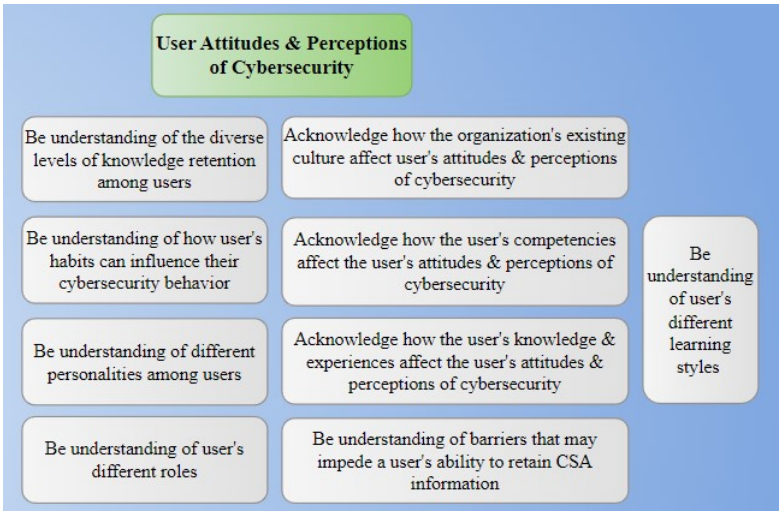


Figure 4.8: Final Result - User Attitudes & Perceptions. (Authors Own).

The human interaction in organizations, hence their interaction with systems and processes, needs to be acknowledged and understood if CSA in an organization is to be effectively addressed. Therefore, user-centered approaches must be integrated into organizations' CSA programs to identify user audiences' needs and goals to produce effective CSA requirements for an organization's CSA efforts. The integration of strategies aiming to understand the human factor aids organizations in reducing the risk of human errors and raising a more positive-minded cybersecurity culture due to constructing better-tailored CSA initiatives (Ki-Aries and Faily, 2017). It is uncommon for organizations to have delved deep into identifying what their users might need to raise their CSA based on their predisposition to cybersecurity. Consequently, these user-centered approaches need to take users' predisposition to cybersecurity into acknowledgment when tailoring CSA for an individual's needs and goals. These predispositions generally involve users' individual attitudes and perceptions of cybersecurity, which are influenced by the

organizations existing cybersecurity culture. For instance, organizations need to reflect if users are already compliant with policies or are tending toward disobedience, if users are risk-tolerant or risk-averse, or if they are accepting of cybersecurity or resistant. Understanding users' positive and negative feelings about cybersecurity is essential to raise their CSA (Furnell and Vasileiou, 2017). On this basis, organizations need to take into account these sub-factors for understanding users' attitudes and perceptions of cybersecurity, for example, user's prior knowledge and experiences, user competencies, user learning style, user barriers, user knowledge retention, user habit, user personality, etc. Furnell and Vasileiou (2017) explains that a user's ability to absorb and apply knowledge, which concerns knowledge retention, could be hindered by barriers of, for instance, personal or cultural sorts. Furthermore, understanding users' roles refers to their responsibilities in context to the data they access, the systems they use in organizations, and how they behave accordingly. Learning style refers to the understanding that users learn differently, so CSA training material must suit users' individual needs and perceptions (Furnell and Vasileiou, 2017). Understanding personalities refers to users' personality traits and how they can influence a person's attitudes and perceptions about CSA, which can impact an organization's cybersecurity culture (Tolah et al., 2021). For instance, organizations can, through personality traits, identify users that may be at risk of committing insider incidents and strategically prevent it or tailor content based on users' receptive nature. As such, personality traits can influence users' behaviors and ultimately raise users' CSA (Khando et al., 2021).

4.3.3 Cybersecurity Advocates

Research and cybersecurity experts have both verified that 'Cybersecurity Advocates' is a crucial principal factor in raising cybersecurity awareness (CSA). This principal factor encompasses five underlying sub-factors that provide valuable recommendations for what should be incorporated into this area when utilizing the guideline. A visualization of 'Cybersecurity Advocates' is depicted in Figure 4.9.

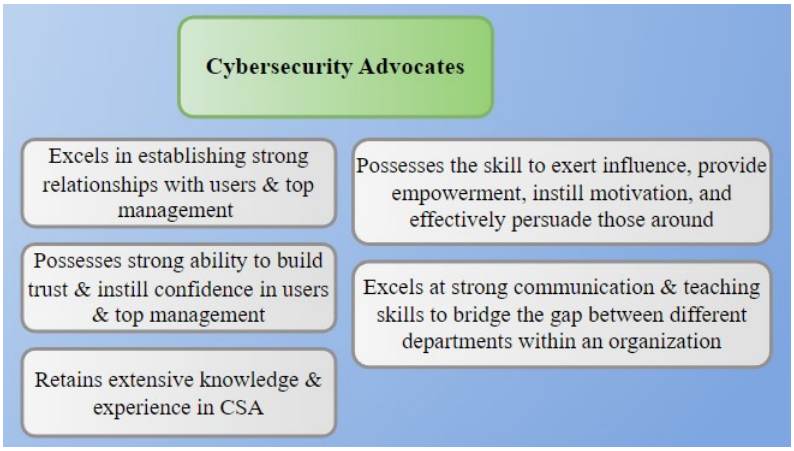


Figure 4.9: Final Result - Advocates. (Authors Own).

Cybersecurity advocates are necessary for organizations to utilize to overcome users' negative perceptions of cybersecurity. These advocates encourage and facilitate the adoption of CSA best practices in organizations, and for them to be successful in their tasks, these advocates need to motivate users to engage in beneficial security behaviors (Haney and Lutters, 2018). The prerequisites advocates need to possess to be successful in influencing users' negative perceptions

and promoting positive security behaviors are represented in the guideline. Haney and Lutters (2018) reinforces these prerequisites by stating that it is essential for advocates to establish trust and be viewed as trustworthy information sources. Because without having the ability to build trust and instill confidence in users, changing negative perceptions will not work. Advocates also need to demonstrate good technical knowledge of CSA to establish credibility, which has been attained through years of experience. Furthermore, advocates must possess strong interpersonal skills to build relationships because it is through a trusted relationship that influence can be exerted to a higher level. If advocates and an organization's users have a good relationship, they are more susceptible to engaging in beneficial security behaviors. The best way for advocates to motivate users is by exerting influence established through trust and relationships and giving users tools to feel empowered, motivated, and persuaded to take action. Advocates must excel at strong communication and translation skills to communicate with different audiences, such as users in different organizational departments. For example, the language used between technical and non-technical users can differ drastically, and advocates need to bridge the gap and translate concepts into words various audiences can understand (Haney and Lutters, 2018).

4.3.4 User Participation, Engagement & Motivation

Research and cybersecurity experts have both verified that 'User Participation, Engagement & Motivation' is a crucial principal factor in raising cybersecurity awareness (CSA). This principal factor encompasses thirteen underlying sub-factors that provide valuable recommendations for what should be incorporated into this area when utilizing the guideline. A visualization of 'User Participation, Engagement & Motivation' is depicted in Figure 4.10.

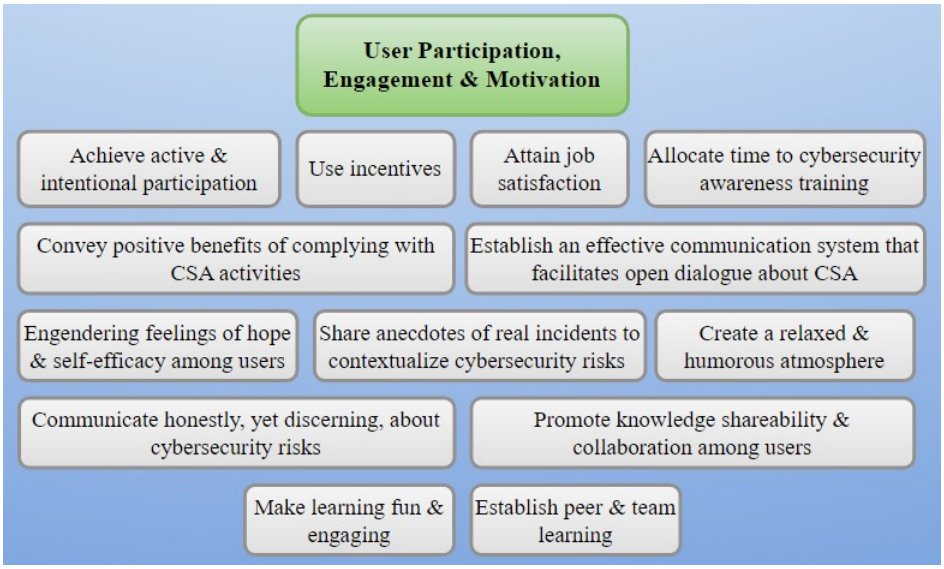


Figure 4.10: Final Result - User Participation, Engagement & Motivation. (Authors Own).

Organizations need to provide a place where users can partake in open dialogue with other users and partake in interesting and relatable content about CSA. One way to accomplish this is for organizations to establish communication channels supporting open dialogue and relatable content to increase users' participation by motivating and engaging them. This aspect is represented in the guideline by the sub-factor 'Establish effective communication systems that

facilitate open dialogue about CSA.' To raise engagement and motivation among users, there is countless way to go; for instance, organizations need to provide users with tools for them to engender feelings of hope and self-efficacy regarding CSA because users with higher self-efficacy are more motivated to participate in CSA initiatives and engage in positive security behaviors (Haney and Lutters, 2018). There are several sub-factors in the guideline that organizations can utilize to create opportunities for users to increase their participation levels and stay motivated and engaged in CSA endeavors. These are: providing users with incentives, providing users with means to attain job satisfaction, providing users with a relaxed and humorous atmosphere, and providing users with positive benefits for complying with CSA. In addition to providing users with learning materials that are fun and engaging, providing users with the means to learn from each other and in teams to share knowledge and collaborate, etc. Furnell and Rajendran (2012) reinforces that job satisfaction is an important factor that influences users cybersecurity behavior at the workplace. For instance, if users' disdain for their job outweighs participating or engaging in security-related responsibilities, such as adhering to best practices, that can invite deficient cybersecurity behaviors (Furnell and Rajendran, 2012).

The aspect of attaining active and intentional participation is important for organizations because that implies the users are motivated enough to take action with CSA of their own volition, which is what is sought to cultivate a cybersecurity culture. Organizations frequently use incentives to engage users to adhere to CSA initiatives. This is because some people need tangible reasons to actively participate and engage in CSA efforts that contribute to their company's cybersecurity. Some incentives could engage users positively, such as being offered additional vacation days (Kemper, 2019). However, there may also be incentives that engage users but does so in a less positive way by introducing compulsory things that become incentives for participating. Haney and Lutters (2018) addresses that when organizations provide users with relatable CSA materials, users' motivation to take action increases. This is because communicating about cybersecurity risks through anecdotes entails contextualizing them in a familiar setting; users tend to be more invested. This aspect is represented in the sub-factor 'share anecdotes of real incidents to contextualize cybersecurity risks.' Talking about cybersecurity risks honestly, yet discerning, acts as a motivator for users that are fearful of cybersecurity to overcome that perception. This is because communicating about risks in such a manner gives users a better understanding of the importance and urgency of tackling cybersecurity risks. Hence, users become motivated to engage and participate in CSA initiatives instead of ignoring them due to fear (Haney and Lutters, 2018).

4.3.5 Governance

Research and cybersecurity experts have both verified that 'Governance' is a crucial principal factor in raising cybersecurity awareness (CSA). This principal factor encompasses three underlying sub-factors that provide valuable recommendations for what should be incorporated into this area when utilizing the guideline. A visualization of 'Governance' is depicted in Figure 4.11.

Figure 4.11: Final Result - Governance. (Authors Own).

In this case, governance concerns a public organization's external and internal environments that influence cybersecurity awareness efforts. Incorporating governance in the guideline is incredibly important because public organizations' governance differs quite drastically from private organizations. The biggest differences are that public organizations' governance is more rigid and under a greater regulatory burden because they are subject to laws, regulations, and the needs of stakeholders. Governance in public organizations includes laws and regulations external to the organization that must be adhered to and internal regulations such as policies, procedures, standards, best practices, programs, and operating agreements related to the specific organization. The top management's role is to ensure that an organization's governance, with all its internal regulations and policies, is followed and complies with external laws and regulations (IPPF, 2014).

Due to this guideline being aimed at large Swedish public organizations, governance was essential to include as it would affect their CSA work. This is represented in the guideline with the two sub-factors 'Adhere to international & national laws, regulations & recommendations for an organization's governance' and 'Adhere to internal policies, standards, procedures, best practices & other recommendations for an organization's governance.' The first sub-factor concerns international and national laws, regulations, and recommendations that affect cybersecurity. International law, regulations, and recommendations relate to, for instance, GDPR legislation and other EU legislation that public organizations should comply with. National law, regulations, and recommendations relate to those specific to Swedish public organizations' governance of information, for example, 'Offentlighetsprincipen,' 'Arkivlagen,' 'Sekretesslagen,' etc. The second sub-factor concerns large Swedish public organizations' internal regulatory environment, such as their internal policies, standards, procedures, best practices, and other recommendations that influence their CSA work. For instance, cyber hygiene best practices, security training policies, adaptive cybersecurity policies, etc. Fielding (2021) state that internal policies as these should be clearly defined and written down, in addition to being consistent across the organization. Internal policies should not be too difficult to follow or too complex to understand, and this is referenced in the guideline's sub-factor 'Ensure internal policies, standards, best practices & other

recommendations for CSA are clear & easy to understand.' This notion is important because organizations want to avoid restricting user productivity; otherwise, people may begin using non-sanctioned tools or techniques to bypass the IT department's control which could produce an additional risk to the organization's security (Fielding, 2021).

4.3.6 Cybersecurity Education, Training & Awareness

Research and cybersecurity experts have both verified that 'Cybersecurity Education, Training & Awareness' is a crucial principal factor in raising cybersecurity awareness (CSA). This principal factor encompasses thirteen underlying sub-factors that provide valuable recommendations for what should be incorporated into this area when utilizing the guideline. A visualization of 'Cybersecurity Education, Training & Awareness' is depicted in Figure 4.12.

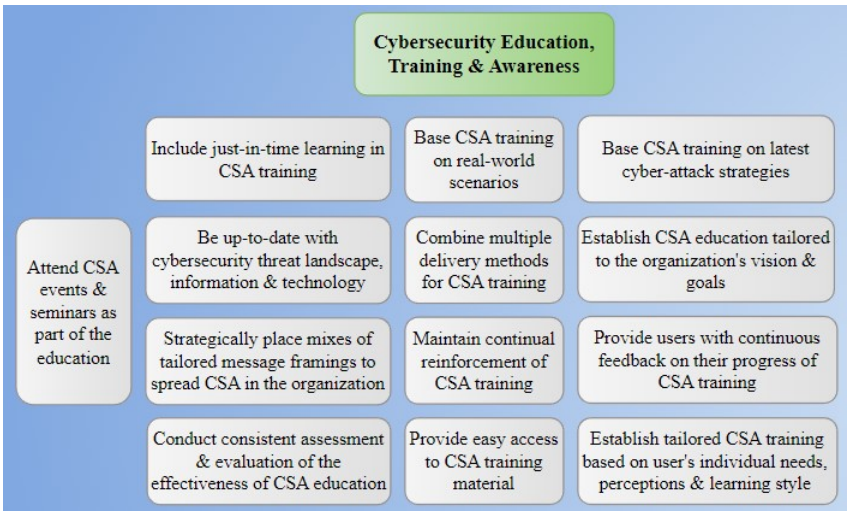


Figure 4.12: Final Result - Education, Training & Awareness. (Authors Own).

Employing cybersecurity education, training, and awareness programs in organizations (Reeves et al., 2021) is essential because they play a key role in raising users' CSA. These programs are considered among the most effective factors influencing users' CSA in organizations due to providing users with competencies and knowledge about CSA (Khando et al., 2021). CSA education, training, and awareness programs aim for users to improve their ability to mitigate cybersecurity threats (Reeves et al., 2021) and become more security-conscious (Abawajy and Kim, 2010). There are numerous aspects considered essential for raising CSA via education and training, which is represented in the guideline as having established tailored CSA training based on the user's individual needs, perceptions, and learning style, having easy access to CSA training materials, and having continual reinforcement of CSA training. In addition to having multiple delivery methods for CSA training, having just-in-time learning, having a mix of tailored message framing strategically placed and spread in the organization, having established CSA education tailored to the organization's vision & goals, etc. Paterson (2021) reinforces the need to have tailored training and education within an organization because choosing a one-size-fits-all approach should not be done. This is because an organization needs to adjust its education and training to highlight its threat conditions, adhere to organizational vision and goals, and tailor to individual users to raise users' CSA in that workplace effectively. CSA education and training should be conducted on a regular basis, hence as the sub-factor states, 'Maintain continual reinforcement

of CSA training.' Furthermore, training should include authentic situations, such as 'Basing CSA training on real-world scenarios' and include 'Base CSA training on latest cyber-attack strategies, such as phishing simulations (Paterson, 2021). It has been asserted that organizations should maintain a combination of delivery methods, such as game-based, simulation-based, online-based, etc., as it regularly improves the success of CSA training and education efforts as users may respond better to some delivery methods or a combination of them. For instance, game-based are typically highly interactive methods that challenge users and keep them interested and engaged, while simulation-based include simulations to assess the users' susceptibility to different cyber-attacks. Several delivery methods can be needed in an organization to effectively provide users with training material in various ways to aid them in increasing their CSA (Abawajy and Kim, 2010). Likewise, a mix of message framing, such as posters, emails, websites, leaflets, newspapers, etc., is needed in organizations to spread CSA messages effectively (Chaudhary et al., 2022). Just-in-time learning is important to include in CSA training because it allows users to locate any material they need and when they need it at their own pace (Riel, 1998).

5 | Discussion

This chapter presents the discussion of the thesis's results. The discussion consists of how this thesis addressed the research questions expressed in 1.2 in the 'Main Results' section. In addition, the discussion consists of Research Contributions, Scientific Quality, Research Validity & Ethical Considerations, which this thesis addresses in their respective sections.

5.1 Main Results

The main results in this thesis relate to the development of the guideline for cybersecurity awareness-raising within the context of large public Swedish organizations by employing design science research (DSR). For this DSR project, one main research question was posed, which contains two sub-questions; therefore, by answering the two sub-questions, the main research question is naturally answered. The first sub-question to be addressed in this thesis was: "What factors contribute to cybersecurity awareness?". To address this question, a rapid review was conducted, which entailed identifying factors within research on CSA that were deemed important for raising CSA in general, hence in private and public organizations alike. The rapid review included seventy-one extracted papers that were deemed relevant for the subject of cybersecurity awareness-raising. Based on the literature extracted and compiled in the rapid review document, which can be viewed in Table 4.1, numerous authors provided significant insights into aspects considered essential for raising CSA. For instance, the author Khando et al. (2021) referenced as number two in the rapid review noted several security awareness-raising factors within the public sector that were deemed important. These factors were management support, culture, security perceptions of users, education and training, attaining user participation, skills, and competencies (Khando et al., 2021).

In conclusion, the rapid review demonstrates that CSA is a complex matter impacted by numerous factors. These factors range from user-oriented, managerial, and technical, supporting the assertion that cybersecurity is a complex socio-technical nature, as Al Sabbagh (2019) noted. The author exemplified this by proclaiming that out of all the security incidents investigated in the paper, only twenty-six percent could have been solved by relying solely on technical means. This means that seventy-four percent of cybersecurity incidents must be managed holistically by addressing people's influence on technology, an organization's policies, etc. (Al Sabbagh, 2019). It can further be noted that many of these contributing factors influence each other. The author Kovačević et al. (2020) delves into this notion by conveying that factors, such as a user's perception of CSA, a user's knowledge of CSA, a user's experience of CSA, etc., are interconnected in the fact that they influence a user's CSA levels. In turn, it has been noted that people's CSA levels influence their cybersecurity behavior. Following this, it has been noted that people's cybersecurity behavior has a noticeable impact on security breaches. For instance,

a clear and significant negative correlation exists between cybersecurity breaches and password behavior. This indicates that people with deficient cyber hygiene, such as employing insecure passwords or sharing passwords with others, have more experience being exposed to cybersecurity incidents. However, it has been further noted that there is a positive correlation between cybersecurity breach experiences and cybersecurity knowledge. This indicates that those frequently involved with cybersecurity incidents possess a higher knowledge level than those that do not (Kovačević et al., 2020). Furthermore, the author Alqahtani (2022) also establishes that people's technical knowledge of cybersecurity, such as knowledge of password security, browser security, and cybersecurity threats on social media, etc., actively increases their CSA levels. This shows that factors such as education and training in cybersecurity do contribute to raising users' CSA (Alqahtani, 2022). Similarly, the author Uchendu et al. (2021) presents essential elements organizations need to include to cultivate a cybersecurity culture and to cultivate and maintain a positive cybersecurity culture; cybersecurity awareness-raising is needed. Thus, confirming that factors contributing to cybersecurity awareness-raising directly influence an organization's ability to cultivate and maintain a positive cybersecurity culture. The factors the author presented were: leadership involvement, such as top management support, cybersecurity policies and procedures, CSA, CSA training, compliance with CSA training, motivation, trust, communication, a network of champions, rewards and sanctions, user commitment, etc. (Uchendu et al., 2021). This provides a good representation of what factors were found in the literature contributing to CSA.

The second sub-question to be addressed in this thesis was: "How can these contributing factors to cybersecurity awareness be described in a guideline for large Swedish public organizations?". To address this question, a guideline was developed based on the factors identified in the literature as contributors to CSA. The guideline's objective was to assist managers in large Swedish public organizations with their CSA efforts. To achieve this objective and produce a guideline aimed at large Swedish public organizations, it is essential to incorporate people from the intended audience into the guidelines development process. Then, during the guidelines development, it can be tailored and tweaked to effectively represent the wants and needs of large Swedish public organizations. Choosing the right people to incorporate into the DSR project is crucial because, in this case, they need to possess in-depth knowledge and years of experience with CSA to ensure the guideline meets the set objectives and requirements as intended. While also bearing insight into the public organizations' current CSA endeavors and challenges. This task would be ideal for experts within the field of CSA in comparison to utilizing managers, even though managers are the intended audience that should use the guideline within the context of large Swedish public organizations. This is because it is doubtful that managers possess the knowledge about CSA that is sought; their strengths lie elsewhere. Nevertheless, to claim that the guideline applies to large public Swedish organizations, it must be verified and validated by trusted people in those environments. Therefore, the ideal group of people to incorporate in the development process of the guideline was experts with deep understanding and competence in the field of CSA that has been accumulated for several years. However, any experts knowledgeable in CSA are ineffective because not every expert has insight into how large Swedish public organizations function. Because of this, it is paramount to restrict experts meant to evaluate, verify and validate the guideline to those working within large Swedish public organizations. Only then can the guideline be designated for large Swedish public organizations. To address this, the guideline was solely demonstrated and evaluated based on the CSA knowledge, skills, and experiences of experts working at large Swedish public organizations. This produced comprehensive insights into what experts within those environments deemed were important factors for raising CSA, which were described in the guideline. Although the guideline is aimed at large Swedish public

organizations, it could be argued that it also applies to private organizations. This may be accurate since CSA is important for all organizations. If the guideline is deemed useful for public organizations, it is not unreasonable to believe it would also be useful for private organizations. Because providing a holistic overview of relevant factors that contributes to CSA is perhaps not something that would only be useful to specific organizations since public and private organizations alike need good CSA. Nonetheless, because the guideline has exclusively been evaluated and validated from a public organization perspective, one can not confidently say that everything in the guideline would be advantageous for private organizations. To determine this, the guideline would also need to be evaluated and validated by CSA experts in private organizations.

The main research question addressed in this thesis was: "What factors contribute to cybersecurity awareness-raising in large Swedish public organizations?". This thesis addressed this question by concluding the two design cycles and presenting the final results of the developed guideline in 'Communication of the Final Results.' The final results establish what factors contribute to cybersecurity awareness-raising in large Swedish public organizations. To recap the answer to the research question, the principal factors that contribute to cybersecurity awareness-raising in large Swedish public organizations are: 'Top Management Support,' 'User Attitudes & Perceptions of Cybersecurity,' 'Cybersecurity Advocates,' 'User Participation, Engagement & Motivation,' 'Governance,' and lastly, 'Cybersecurity Education, Training & Awareness.' The sub-factors of each principal factor can be seen in Appendix E. A summary of the key results produced from this thesis relates to the expert's overall assessment of the guideline. Their final estimation of the guideline is that it is comprehensible to understand, contains highly relevant and critical factors for raising CSA in large Swedish public organizations, and is a highly beneficial guide to have. This is because the guideline holistically presents the most significant information about raising CSA in a single frame. The experts interviewed for this thesis have years of experience working with CSA and proclaimed to never have seen such a detailed and complete overview of the entire CSA work as this guideline has provided. Consequently, experts evaluated, verified, and validated this thesis guideline as a useful cybersecurity awareness-raising tool for large Swedish public organizations' CSA endeavors. Because of this, the experts expressed a lot of interest in developing the guideline further, which signifies how relevant and important the contribution of this guideline can be to organizations' CSA efforts.

The expert's assessment of the guideline has been incredibly positive for the duration of the DSR project, despite having acknowledged all areas in the guideline that needed refinement. Nevertheless, there are advantages and disadvantages to developing a high abstract guideline such as this. The advantage of a guideline with these characteristics is that it gives organizations a means to regard the most significant aspects of a highly complex topic with one glance. Organizations can better understand what is expected of them by being presented with areas their CSA efforts should include to raise their user's CSA. Managers in organizations can easier organize and plan CSA education programs by being provided with a clear overview of the factors that this plan should entail. Let us illustrate how managers in their organizations could use the guideline. For instance, a manager views the guideline to gain an overview of what CSA entails. Then the manager studies how many factors in this guideline they have already begun addressing or how many they have planned to address or realizes how many critical factors they have neglected. Perhaps the manager did not realize the importance of addressing, for example, users' predisposition to cybersecurity, their knowledge retention, or their preferences or needs when planning their tailored CSA training and, therefore, does not understand why certain users excel at cybersecurity training while others do not. The guideline's factors are meant to provide managers with a complete picture to ensure no factors crucial to the success of cybersecurity

awareness-raising efforts are missing or being overlooked. The factors in the guideline also provide managers with valuable recommendations for more detailed suggestions on what they should focus on and prioritize. For instance, if the organization wants to increase users' participation in training, they need to focus on engaging and motivating users by, for example, using incentives, allocating time to CSA training, creating a relaxed, humorous atmosphere, etc. If the managers want to increase users' CSA through establishing good cybersecurity training, they must prioritize easy access to training materials, providing effective training by combining delivery methods, etc. The disadvantage of the guideline is that it does not provide the managers with a means to explain how these factors should be executed in a step-by-step list. The guideline provides an overview, recommendations, and suggestions for what to include to enhance their cybersecurity awareness-raising efforts. Still, it does not provide a precise 'how-to-do' list of activities or exercises for achieving that. This means that organizations can use this guideline as an aid for what to include in their plans and what structures need to be present but decide on their own what factors to prioritize, when certain factors should be accomplished, how each factor should be enforced, etc. These aspects are major challenges with this guideline because many of the guidelines' factors are interconnected. This makes it challenging to focus on one area at a time because to do so, other factors may be required to be accomplished first. For instance, if an organization's first aim is to establish education and training for its users to raise CSA, they will not get far without having attained top management support.

5.2 Research Contributions

This thesis makes a valuable contribution to society and the scientific community, as it presents a novel application of existing knowledge structured as a guideline. The guideline provides valuable contributions to Sweden's public society by developing a high abstract guideline to assist managers in cybersecurity awareness (CSA) efforts, specifically within large Swedish public organizations. By identifying key areas for raising CSA and outlining relevant factors that contribute to raising awareness, this guideline plays a vital role in promoting cybersecurity across public organizations. Organizing the guideline's information into a single, comprehensive, and complete frame allows organizations to easily view all important details at a glance. Representing the most relevant aspects of a particular matter in one highly abstract single frame can be very beneficial. Because this can make the task seem less daunting and complex, thereby aiding organizations that may feel overwhelmed by the CSA work. Furthermore, the guideline contributes to the scientific community by providing, as mentioned, a new application of existing knowledge of CSA. The reason for stating this guideline to be a new application of existing knowledge is that no papers have been encountered that have produced a similar guideline as this on CSA. For instance, when exploring other research on CSA, numerous authors are covering almost every imaginable subject on CSA, such as scouring the threat of human factors in cybersecurity in different ways, exploring the implementation of various methods, techniques, and frameworks to raise CSA, or exploring the impact of awareness training and so on. Although there is a wealth of information on CSA, no previous studies have attempted to condense the most relevant aspects of CSA into a single visual aid for large Swedish public organizations. This thesis provides new insights into the field of CSA, as no comparable research has been conducted under these circumstances, which is of great value as CSA is a relatively new subject with global significance. The scientific community constantly generates new information to further its understanding of CSA. Therefore, this thesis can provide additional aid and offer a fresh perspective on CSA that hasn't been presented before.

5.3 Scientific Quality

Evaluating the quality of research is crucial in scientific studies as it ensures the production of high-quality research. Consequently, researchers face immense pressure to publish research of this caliber (Lindgreen et al., 2021), but the question is what constitutes high-quality research. This paper Stenfors et al. (2020) defines four essential characteristics or markers that good quality papers conducting qualitative research should possess. These markers are widely used to appraise the trustworthiness of qualitative research. These markers include credibility, dependability, confirmability, and transferability. Determining the plausibility and trustworthiness of research results is defined as credibility, which demands that the chosen methodology be explicitly justified. This justification is achieved by examining the alignment between theory, research question, data collection, analysis, and results. Additionally, it involves scrutinizing whether the analytical steps taken are appropriate within the framework. Dependability refers to the extent to which research can be replicated under similar conditions. To ensure this, researchers must provide sufficient information on their methodology so that another researcher can follow the same procedural steps. However, it should be noted that the conclusion may differ upon replication. Confirmability is defined as the assessment of the connection between the data utilized in research and the resulting outcomes. This is accomplished by scrutinizing whether the researcher has thoroughly explained their discoveries and backed them up with quotations. Transferability refers to whether the results can be transferred to another setting, context, or group. To determine transferability, it is important to consider if the research provides a comprehensive description of the context in which it was conducted and how this context may have impacted the results (Stenfors et al., 2020).

When evaluating this thesis's scientific quality, these metrics will be used in the discussion. The researcher of this thesis would deem it credible because it achieves the requirements set to reach credibility. For instance, this thesis incorporates previous and well-known research, theories, and literature relevant to raising cybersecurity awareness, and statements are backed up by published scientific sources. In this thesis, every decision has been thoroughly explained and justified. This includes the selection of the subject matter, the importance of addressing it, the research questions posed, the methodology chosen to provide the necessary answers, and how the data were analyzed and presented. Thereby achieving good alignment between theory, research question, data collection, analysis, and results. To elaborate, the methodology used in this thesis is design science research (DSR). This approach was chosen to accomplish the thesis aims and objectives by utilizing a DSR framework guiding the researcher through six steps of the guideline development process. To create and validate the guideline, data collection methods, such as rapid reviews and interviews, were necessary. The reasons behind these choices are also explained and justified. As a result, this thesis is considered to be trustworthy and credible. The researcher for this thesis would also say that dependability, confirmability, and transferability have reached good levels in this thesis. A good level of dependability is achieved because this thesis provides extensive information on every significant step made in the methodology and provides justification for those choices, so it would be easy for a researcher to follow the same procedural steps if wanting to replicate this guideline. However, some aspects must be noted that affect dependability. This is because even if another researcher replicates the methodology and the justifications are incorporated into their decision-making, another researcher may produce a slightly different guideline. One aspect, for instance, could be when the other researcher conducts their rapid review. Even if they use the same databases and search terms, the compiled literature could differ because perhaps this thesis overlooked relevant literature, or perhaps the other researcher overlooks relevant literature included in this thesis. But suppose the researcher looked at Table

4.1 afterward to ensure all literature they had used was incorporated in this thesis's rapid review. In that case, another researcher probably produces a similar guideline to this thesis. The second aspect that might differ during replication relates to using the compiled literature to create the first draft of the guideline. This is because the guideline can differ in content and structure between researchers if different interpretations or opinions are made on what factors should be included first and where or how each factor should be organized. This is because this thesis did not provide a step-by-step explanation for how the first draft was created, only the broad strokes of it. A third aspect to note here that affects dependability is what results are highlighted in the thesis evaluation chapters. This is because the researcher decided what parts of the transcribed interviews were the most relevant and significant to note as the results in evaluations, in addition to all the transcribed material not included as an appendix in this thesis. Other researchers might have different opinions on what should be brought forth, affecting the guideline's development. A fourth aspect that can affect dependability is which experts the other researcher is interviewing. This is because the experts' input vastly affects the guideline's development. If another researcher interviews their own set of experts, then that input would differ from what this thesis produced. This is not shocking because different people produce different results even if the same interview questions were used. However, because semi-structured interviews were used in this thesis, this also opens to the input being different if another researcher seeks to replicate it because interviewees are free to express themselves beyond the established interview questions. Despite these aspects, this thesis produces a sufficient level of dependability so other researchers could easily replicate this guideline in broad strokes. However, these aspects are still something other researchers should note.

A good level of confirmability is reached in this thesis by clearly connecting the data utilized in developing the guideline and the resulting outcomes. This can be seen in this thesis evaluation chapter because there is when this thesis provides detailed descriptions and explanations of the interview results. The most significant discoveries were all noted, and many of them were backed up with quotations from the interviews. Thus, other researchers could easily see how the interviewees' input data influenced the changes made to the guideline. Lastly, a good level of transferability is reached in this thesis because good descriptions are made concerning the context of the guideline during its development. For instance, the guideline is aimed to be adopted by managers at large public organizations in Sweden, which means the guideline must be verified as relevant and useful. This can often be done via experts because people trust they know what they are talking about because of their extensive knowledge and years of experience on the subject in question. Therefore, utilizing experts working at large Swedish public organizations to help shape the development of the guideline is within the established context of this thesis, which provides good transferability. An aspect that might affect this thesis's transferability is that regardless of choice in context, the guideline can perhaps be transferred to the context of private organizations as well. This is because the guideline provides a complete and holistic view and is verified and validated by public organizations. However, that does not mean the guideline is not useful for private organizations wanting guidance with cybersecurity awareness. In conclusion, the researcher of this thesis would declare that the thesis is of good scientific quality, but of course, improvement could be made.

5.4 Research Validity

Validity is fundamental in evaluating any research instrument used for conducting good research. Ensuring validity in research involves verifying the truthfulness of the findings. This is done by establishing to which degree the generated results satisfy the requirements set by the chosen scientific research method. Thereby promoting transparency and minimizing the chances of researchers introducing their own biases. The reason for exploring validity is to ensure the research is sound, replicable, and accurate. (Mohajan et al., 2017). Despite validity being a fundamental component in research, such as in social sciences, the notion is severely overlooked in design science research (DSR). Nonetheless, DSR research requires validity to offer researchers a systematic approach to gather and scrutinize evidence and substantiate their claims and findings Larsen et al. (2020). This can be seen by popular authors writing on DSR because they scarcely mention validity as a part of the research process. For example, the author Ken Peffers is well-known in DSR and has written several papers about it. In one paper referenced in this thesis, Peffers et al. (2007), Peffers proposes a DSR framework consisting of six activities to follow when conducting a DSR project. This framework is well-known and popular to apply when doing a DSR project, so much so that this thesis uses it to base its DSR project. However, the author once mentions the notion of validity in that paper by stating that a case for validity has been made by successfully bringing design research into the Information Systems research community. Peffers continues by saying that small amounts of DSR have successfully been published in the Information Systems research community but that a conceptual model, such as a framework, for employing DSR with validity being incorporated into the evaluation of artifacts is lacking (Peffers et al., 2007).

In addition, based on these two papers that Peffers writes on the topic of DSR: Peffers et al. (2018), Peffers et al. (2012), validity is only mentioned in one of them, i.e., the latter. The paper Peffers et al. (2012), however, dedicates explaining the importance of validity in DSR by reporting on principles for evaluating DSR artifacts. For instance, the paper states that evaluation should address the validation of incremental design decisions at the beginning of a DSR process to ensure that a design science researcher makes design decisions disciplined and consistently and thoroughly work towards creating a valuable artifact. To do this, the paper proposed forming evaluations according to three principles that have been synthesized and combined from previous literature on the topic (Peffers et al., 2012). Furthermore, another author that is well-known for DSR is Alan R. Hevner, and he has written countless papers on the DSR process, some of which this thesis has referenced, such as (Hevner, 2007), (Hevner et al., 2010), and (Gregor and Hevner, 2013). The first two papers mentioned nothing about validity, but the third paper said it six times. In the third paper Gregor and Hevner (2013), validity was noted in the DSR process' evaluation phase by proclaiming that it is essential for an artifact to be demonstrated and evaluated to provide evidence of its worth. This evidence shall be provided by evaluating the artifact using validity, utility, quality, and efficacy criteria. The validity criteria must be addressed in DSR to ensure the artifact works and does what it is meant to do; hence, it is trustworthy to achieve its goals (Gregor and Hevner, 2013). Considering how important research declares validity to be, it has been established by Larsen et al. (2020) and partly examined in this thesis that validity concepts are narrowly used in DSR. It has been claimed that validity has not been utilized enough to strengthen the claims of DSR. Therefore, the author Kai R. Larsen specifically concentrates on correcting this by proposing a validity framework for DSR projects to incorporate validity as an integral aspect of DSR. This framework consists of three steps to sustain validity in DSR: design antecedent validity, development and use context validity, and design outcome validity. The first step concerns validity in the input to the design

process. The second concerns validity in the artifact's internal design in addition to the environment the artifact is intended to be placed. The third concerns validity in the artifacts utility of the innovative design solution, hence how well the artifact's design meets the set criteria and how the artifact compares to other corresponding design solutions (Larsen et al., 2020). Peffers et al. (2007) also noted that to ensure validity is incorporated in a DSR process, a framework should be adhered to even if that were not present in his proposed framework. Moreover, this thesis adhered to Peffer's notion of utilizing frameworks and thereby used the established DSR framework he proposed, presented in Peffers et al. (2007), to develop the guideline. Furthermore, this thesis applied Larsen et al. (2020) DSR validity framework for discussion purposes to indicate how this thesis developed an artifact that ensured validity in its DSR process. For instance, concerning the 'design antecedent validity' step, this thesis DSR process ensured that the input to the DSR process was only of good scientific literature that supported the thesis topic. Hence, the literature used in 'Method Development 4.1.1' to construct the guideline via a rapid review was deemed good scientific quality because it related to cybersecurity awareness, and they were published in well-known journals, conference proceedings, etc., to ensure they were peer-reviewed. The input gathered from the 'Artifact Demonstration' phases, utilized in the 'Evaluation' phases to assess the guideline, was of high quality. This is because cybersecurity awareness experts provided it. Concerning 'development and use context validity,' this thesis DSR process ensured that the guidelines internal design, hence all the factors, are constructed for its intended environment. This environment is a large Swedish public organization, and all human input used in the DSR process to evaluate the guideline came from people with expert knowledge of cybersecurity awareness and working within that environment. By doing this, the guideline was evaluated and verified as useful, accurate, and sound by the people the guideline is intended for, which promotes the validity of the artifact's design. Concerning 'design outcome validity,' this thesis DSR process confirmed that the guidelines utility of the design solution met the criteria set. For example, the objective of this guideline was to be useful to managers in large Swedish public organizations to aid them in their cybersecurity awareness work, which was confirmed by the people participating in the evaluation processes as something accomplished. Furthermore, it was also demonstrated by previous research on cybersecurity awareness and confirmed by the people partaking in the project that no other similar artifact design solutions as this thesis provides have been constructed.

5.5 Ethical Considerations

It is essential to address ethical considerations in all forms of research, including design science research (DSR) projects as conducted within this thesis. Ethics addressed in scientific research often relate to the ethical aspects incorporated during the project, as mentioned in 3.4 in this thesis. However, discussing the ethics of DSR goes beyond that and should include ethical implications that may arise from utilizing the created artifacts (Johannesson and Perjons, 2014). The paper Myers and Venable (2014) addresses these implications by proclaiming that DSR projects must have significantly different ethical principles to adhere to compared to social science or behavioral researchers in Information Systems. This is because the artifacts in DSR can be utilized long after its invention by people who were not involved in creating it. This can result in the artifact being used in contexts other than intended, bringing future problems or harm (Myers and Venable, 2014). Ethical considerations that need to be addressed for this thesis' artifact relate to the information the guideline contains and how it is interpreted. For instance, as the guideline is developed to assist managers in large Swedish public organizations with their cybersecurity awareness (CSA) work, it is imperative that the included factors represent the correct informa-

tion and that organizations interpret them accurately. Public organizations may suffer if they follow a guideline that provides inaccurate information and implements poor suggestions and recommendations in their CSA initiatives. The repercussions of discovering that the guideline is more harmful than helpful to their awareness-raising efforts could be irreversible. This is because it requires a greater amount of time and effort to undo an action's negative consequences than it initially does to cause them. As a result, public organizations must rely on guidance that is based on reliable and correct information. If public organizations wish to follow this thesis guideline, they should carefully examine it beforehand to determine whether it will be beneficial or detrimental to their organization. It is important to note that misinterpretation of the guideline by public organizations could have negative consequences on their CSA initiatives. This could result in incorrect prioritization of areas, misallocating resources, and inappropriate reservation of resources for certain aspects. Therefore, it is crucial for organizations to properly understand and implement the guideline because public organizations may allocate excessive resources to the "wrong" areas and inadequate resources to the "right" ones. This may lead to the perception that any CSA initiative is a financial burden, resulting in negative feedback from significant stakeholders when such efforts fail to yield the expected outcomes. This negative perception can hinder the organization's progress toward enhancing its CSA, as organizations may choose not to invest further resources in raising awareness. Ultimately, this can result in the deterioration of their cybersecurity posture. In addition, if public organizations adopt the guideline, it could potentially have a negative impact on them if someone intends to harm the organizations and uses the guideline to do so. This is because the guideline outlines the activities that should be included in public organizations' efforts to raise CSA. Attackers could use this information to gain a better understanding of the factors that affect public organizations' CSA work, identify vulnerabilities, and use them to plan their attacks.

Therefore, as Myers and Venable (2014) mentions, it is important to consider the ethical principles of the artifacts being created. In addition, it is important to consider how the artifact can impact its surroundings and whether one wants to leave the world in a better or worse state after concluding the project. Researchers employing DSR should be proactive and agree on ethical principles instead of waiting until an event threatens their reputation. This paper, therefore, presents six ethical principles to which all researchers employing DSR should adhere. These principles include the public interest, informed consent, privacy, honesty and accuracy, property, and quality of the artifact. The first principle is the public interest, which entails researchers needing to identify every stakeholder that may be affected if a particular artifact is used. Researchers then need to critically assess what weighs the heaviest - the benefit or harm to stakeholders. Features in an artifact that can influence safety, health, democracy, empowerment, and emancipation for all must be evaluated to assess whether the artifact should have those capabilities. The second principle is informed consent, which entails that all DSR projects need to acquire informed consent from every person involved. The third principle is privacy, which entails ensuring adequate safeguards are in place to protect the privacy of those currently involved in the project and those utilizing or being impacted by the artifact in the future. The fourth principle is honesty and accuracy, and this entails that any inspiration from other sources should be acknowledged because plagiarizing ideas is not allowed, in addition to reporting any findings about the created artifact honestly. The fifth principle is property, which entails securing an agreement regarding ownership of the artifact at the beginning of the project. Furthermore, it also entails securing an agreement about ownership concerning information gathered during the project and establishing what privileges researchers have to publish findings. Lastly, the sixth principle is the quality of the artifact, and this entails guaranteeing the artifact is of sound quality, ensuring its design addresses risks such as safety-critical situations, and providing sufficient and rigorous

evaluation and testing to ensure the artifact is safe to use (Myers and Venable, 2014). This thesis addresses the public interest by speculating what could happen if public organizations were negatively affected using the guideline. Likewise, this thesis addresses informed consent in 3.4 for when interviews were conducted, addresses honesty and accuracy by never plagiarizing and always citing sources when inspiration has been taken from others, and addresses the quality of the artifact in 5.3. The remaining principles are not addressed due to not being suitable for the kind of artifact this thesis has developed.

6 | Conclusion

This chapter presents the conclusion to the thesis consisting of Revising Aims & Objectives, Revisiting Research Contributions, and Limitations & Future research.

6.1 Revisiting Aims & Objectives

The aim addressed in this thesis is the development of an artifact for cybersecurity awareness-raising by employing a design science research project. This guideline was aimed to provide managers in large Swedish public organizations with a complete and holistic overview of highly essential and relevant contributing factors for cybersecurity awareness-raising, presented in a single frame. This aim has been addressed by answering the thesis's research question consisting of one main objective and two sub-objectives. The two sub-objectives are answered first in this thesis, and by doing so, the main objective naturally becomes answered, and these are:

- What factors contribute to cybersecurity awareness-raising in large Swedish public organizations?
  - What factors contribute to cybersecurity awareness?
  - How can these contributing factors to cybersecurity awareness be described in a guideline for large Swedish public organizations?

The objective, "What factors contribute to cybersecurity awareness?" has been addressed in this thesis by conducting a rapid review based on good scientific literature that someway mentions how to increase cybersecurity awareness or contain the most critical factors organizations should focus on for cybersecurity awareness-raising. The rapid review included seventy-one extracted papers that were deemed relevant for the subject of cybersecurity awareness-raising. This is presented in full in section 4.1.1 - Method Development.

The objective, "How can these contributing factors to cybersecurity awareness be described in a guideline for large Swedish public organizations?" has been addressed in this thesis by developing a guideline based on the factors identified in the literature as contributors to cybersecurity awareness. In addition to incorporating people retaining expert knowledge on cybersecurity awareness that works at large Swedish public organizations into the design science research process of developing the guideline. Demonstrating and evaluating the guideline based on experts' knowledge of cybersecurity awareness and the inner workings of large Swedish public organizations allows the guideline to be verified and validated as beneficial to large Swedish public organizations. The process of developing the guideline is presented in full in Chapter 4 - Result.

The objective, "What factors contribute to cybersecurity awareness-raising in large Swedish public organizations?" has been addressed in this thesis by concluding the two design cycles in the design science research process and by communicating the final result of the developed guideline. The final results establish what factors contribute to cybersecurity awareness-raising in large Swedish public organizations. These are presented in full in section 4.3 - Communication of the Final Results.

6.2 Revisiting Research Contributions

This thesis produces valuable contributions to society and the scientific community by presenting a novel application of existing knowledge as a guideline. The guideline contributes valuable knowledge to society by developing a guideline specifically aimed at large Swedish public organizations to assist them in their cybersecurity awareness efforts. The guideline contributes valuable knowledge to the scientific community by presenting a new perspective and application on existing knowledge of cybersecurity awareness that has not previously been done.

6.3 Limitations & Future Research

This thesis has certain limitations that must be acknowledged because limitations of a thesis design refer to the systematic bias researchers unintentionally create (Price and Murnan, 2004). Limitations are imposed restrictions on the thesis that are closely associated with the chosen research strategy, budget constraints, and other factors. It is essential to acknowledge them as they may impact the thesis's results and conclusions (Theofanidis and Fountouki, 2018). This thesis encounters several limitations that greatly affect it, which are associated with methodology and time. This thesis result and conclusion are affected by time constraints which influence the design science research process by not being able to include more design cycles than two. Restricting the number of design cycles to two hinders the guideline from being further developed and improved. This may result in a guideline that is unfinished or underdeveloped. For instance, the guideline may provide even more valuable results or a different conclusion if allowed time to include a third or even a fourth design cycle to enhance further and improve it. However, this is often impossible in reality as all projects are restricted by time. Therefore, it is not uncommon in design science research to conclude the process before everyone is completely satisfied with the artifact. Concluding the design science research process after two design cycles may produce deficiencies in the guideline's solution; nonetheless, those deficiencies can be further addressed in future research.

This thesis presents opportunities for future research to develop further and improve the guideline. Currently, the guideline produces a comprehensive and complete overview of highly relevant contributing factors for cybersecurity awareness-raising aimed at large Swedish public organizations. However, there are opportunities for other researchers to move away from this highly abstract umbrella work and delve deeper into each area and its factors. For example, other researchers could focus on further developing the guideline to provide users with a practical and detailed 'how-to-do' list of suggested activities and exercises for each presented cybersecurity awareness-raising factor. Suppose managers want to incorporate the principal factor 'User participation, engagement, and motivation' into their organization's cybersecurity awareness efforts. In that case, they can be provided with more specific suggestions and recommendations for ways to do so. Furthermore, if managers want to concentrate on creating a 'relaxed and humorous

atmosphere,' they can be provided with detailed suggestions specific to that factor, etc. It is important to note that despite being provided with detailed suggestions for activities and exercises, organizations must tailor the suggestions to their environment. Providing in-depth suggestions for each factor is meant to provide further assistance on what an organization should include and prioritize in their cybersecurity awareness efforts, not be presented with exact steps they can blindly follow. Additional opportunities for future research could include altering the perspective or target audience of the guideline usability from the current public organizations to private ones. For example, researchers could develop and evaluate the guideline further by including experts from Swedish private organizations to determine whether the guideline is useful or applicable solely to public organizations or if the guideline can be useful for private organizations' cybersecurity awareness work as well. This could lead to a change in perspective for what target audience should utilize the guideline.

Bibliography

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, 33(3):237–248.

Abawajy, J. and Kim, T.-h. (2010). Performance analysis of cyber security awareness delivery methods. In *Security Technology, Disaster Recovery and Business Continuity: International Conferences, SecTech and DRBC 2010, Held as Part of the Future Generation Information Technology Conference, FGIT 2010, Jeju Island, Korea, December 13-15, 2010. Proceedings*, pages 142–148. Springer.

Abu-Amara, F. and Tamimi, H. (2021). Cyber shield security awareness program. In *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, pages 422–425. IEEE.

Adelola, T., Dawson, R., and Batmaz, F. (2015). The urgent need for an enforced awareness programme to create internet security awareness in nigeria. In *Proceedings of the 17th International Conference on Information Integration and Web-based Applications & Services*, pages 1–7.

Ahlan, A. R. and Lubis, M. (2011). Information security awareness in university: maintaining learnability, performance and adaptability through roles of responsibility. In *2011 7th International Conference on Information Assurance and Security (IAS)*, pages 246–250. IEEE.

AL-Nuaimi, M. N. (2022). Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review. *Global Knowledge, Memory and Communication*.

Al-Otaibi, A. F. and Alsuwat, E. S. (2020). A study on social engineering attacks: Phishing attack. *Int. J. Recent Adv. Multidiscip. Res*, 7(11):6374–6380.

Al Sabbagh, B. (2019). *Cybersecurity incident response: a socio-technical approach*. PhD thesis, Department of Computer and Systems Sciences, Stockholm University.

Alahmari, A. and Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pages 1–5. IEEE.

Alahmari, S., Renaud, K., and Omoronyia, I. (2022). Moving beyond cyber security awareness and training to engendering security knowledge sharing. *Information Systems and e-Business Management*, pages 1–36.

Alanazi, M., Freeman, M., and Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, 136:107376.

Albrechtsen, E. and Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study. *Computers & Security*, 29(4):432–445.

Aldawood, H. and Skinner, G. (2018). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)*, pages 62–68. IEEE.

Aldawood, H. and Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—pitfalls and ongoing issues. *Future Internet*, 11(3):73.

Alkhazi, B., Alshaikh, M., Alkhezi, S., and Labbaci, H. (2022). Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. *IEEE Access*, 10:132132–132143.

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences*, 12(5):2589.

Alshaikh, M., Maynard, S. B., and Ahmad, A. (2021). Applying social marketing to evaluate current security education training and awareness programs in organisations. *Computers & Security*, 100:102090.

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in saudi arabia. *Heliyon*, 7(1):e06016.

Aman, W. and Al Shukaili, J. (2021). A classification of essential factors for the development and implementation of cyber security strategy in public sector organizations. *International Journal of Advanced Computer Science and Applications*, 12(8).

Amjad, H. A. R., Naeem, U., Zaffar, M. A., Zaffar, M. F., and Choo, K.-K. R. (2016). Improving security awareness in the government sector. In *Proceedings of the 17th International Digital Government Research Conference on Digital Government Research*, pages 1–7.

Arbanas, K., Spremic, M., and Zajdela Hrustek, N. (2021). Holistic framework for evaluating and improving information security culture. *Aslib Journal of Information Management*, 73(5):699–719.

Bada, M. and Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (smes). *Information & Computer Security*, 27(3):393–410.

Bakari, J. K., Tarimo, C. N., Yngström, L., Magnusson, C., and Kowalski, S. (2007). Bridging the gap between general management and technicians–a case study on ict security in a developing country. *Computers & Security*, 26(1):44–55.

Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance*, 28:24–31.

Braun, V. and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101.

Bélanger, F., Maier, J., and Maier, M. (2022). A longitudinal study on improving employee information protective knowledge and behaviors. *Computers & Security*, 116:102641.

Cain, A. A., Edwards, M. E., and Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications*, 42:36–45.

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security*, 2016(6):8–14.

Chang, L. Y. and Coppel, N. (2020). Building cyber security awareness in a developing country: lessons from myanmar. *Computers & Security*, 97:101959.

Chaudhary, S., Kompara, M., Pape, S., and Gkioulos, V. (2022). Properties for cybersecurity awareness posters' design and quality assessment. In *Proceedings of the 17th International Conference on Availability, Reliability and Security*, pages 1–8.

Chowdhury, N., Katsikas, S., and Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, 113:102551.

Chumaera, M. M., Ayu, M. A., et al. (2022). Assessing students' information security awareness through the knowledge, attitude, and behavior model. In *2022 IEEE 8th International Conference on Computing, Engineering and Design (ICCED)*, pages 1–6. IEEE.

Chung, M. (2020). Signs your cyber security is doomed to fail. *Computer Fraud & Security*, 2020(3):10–13.

Cieslinska, K. (2007). The basic roles of manager in business organization. *Roczniki Akademii Rolniczej w Poznaniu. Ekonomia*, 6.

Coffey, J. W. et al. (2017). Ameliorating sources of human error in cybersecurity: technological and human-centered approaches. In *The 8th International Multi-Conference on Complexity, Informatics, and Cybernetics, Pensacola*, pages 85–88.

Cone, B. D., Irvine, C. E., Thompson, M. F., and Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers & security*, 26(1):63–72.

Cone, B. D., Thompson, M. F., Irvine, C. E., and Nguyen, T. D. (2006). Cyber security training and awareness through game play. In *Security and Privacy in Dynamic Environments: Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22–24 May 2006, Karlstad, Sweden 21*, pages 431–436. Springer.

Dahabiyeh, L. (2021). Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information & Computer Security*, 29(5):836–849.

Dawson, M., Bacius, R., Gouveia, L. B., and Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*, 26(1):69–75.

de Bruijn, H. and Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1):1–7.

Denscombe, M. (2014). *The good research guide: for small-scale social research projects*. McGraw-Hill Education (UK).

Draw.io (2023). Features of draw.io.

Drevin, L., Kruger, H. A., and Steyn, T. (2007). Value-focused assessment of ict security awareness in an academic environment. *Computers & Security*, 26(1):36–43.

Eurostat (2016). Glossary: Enterprise size.

Fielding, J. (2020). The people problem: how cyber security's weakest link can become a formidable asset. *Computer Fraud & Security*, 2020(1):6–9.

Fielding, J. (2021). Building a culture of security. *Computer Fraud & Security*, 2021(2):20.

Filipczuk, D., Mason, C., and Snow, S. (2019). Using a game to explore notions of responsibility for cyber security in organisations. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–6.

Furnell, S. and Rajendran, A. (2012). Understanding the influences on information security behaviour. *Computer Fraud & Security*, 2012(3):12–15.

Furnell, S. and Vasileiou, I. (2017). Security education and awareness: just let them burn? *Network Security*, 2017(12):5–9.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., and Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, 30(1):28–38.

Gcaza, N. and Von Solms, R. (2017). Cybersecurity culture: an ill-defined problem. In *Information Security Education for a Global Digital Society: 10th IFIP WG 11.8 World Conference, WISE 10, Rome, Italy, May 29-31, 2017, Proceedings 10*, pages 98–109. Springer.

Georgiadou, A., Michalitsi-Psarrou, A., and Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. *Computers & Security*, 129:103199.

Grant, M. J. and Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health information & libraries journal*, 26(2):91–108.

Grassegger, T. and Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, 181:59–66.

Gregor, S. and Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS quarterly*, pages 337–355.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7):e00346.

Hall, M. (2016). Why people are key to cyber-security. *Network Security*, 2016(6):9–10.

Haney, J. M. and Lutters, W. G. (2018). "it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. In *SOUPS@ USENIX Security Symposium*, pages 411–425.

Hart, S., Margheri, A., Paci, F., and Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95:101827.

Hasan, N., Rana, R. U., Chowdhury, S., Dola, A. J., and Rony, M. K. K. (2021). Ethical considerations in research. *Journal of Nursing Research, Patient Safety and Practise (JNRPSP) 2799-1210*, 1(01):1–4.

Hevner, A., Chatterjee, S., Hevner, A., and Chatterjee, S. (2010). Design science research in information systems. *Design research in information systems: theory and practice*, pages 9–22.

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian journal of information systems*, 19(2):4.

Hooper, V. and McKissack, J. (2016). The emerging role of the ciso. *Business Horizons*, 59(6):585–591.

IPPF (2014). Assessing organizational governance in the public sector. In *The Institute of Internal Auditors Global*.

Jeong, J., Mihelcic, J., Oliver, G., and Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. In *2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, pages 338–345. IEEE.

Johannesson, P. and Perjons, E. (2014). *An introduction to design science*, volume 10. Springer.

Jouaibi, R., Gaylard, A. K., and Lee, B. (2022). Employee cyber-security awareness training (csat) programs in ireland's financial institutions. In *2022 Cyber Research Conference-Ireland (Cyber-RCI)*, pages 1–4. IEEE.

Kalhoro, S., Rehman, M., Ponnusamy, V., and Shaikh, F. B. (2021). Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. *IEEE Access*, 9:99339–99363.

Kävrestad, J. (2022). *Context-Based Micro-Training: Enhancing cybersecurity training for end-users*. PhD thesis, University of Skövde.

Kävrestad, J., Gellerstedt, M., Nohlberg, M., and Rambusch, J. (2022). Survey of users' willingness to adopt and pay for cybersecurity training. In *Human Aspects of Information Security and Assurance: 16th IFIP WG 11.12 International Symposium, HAISA 2022, Mytilene, Lesbos, Greece, July 6–8, 2022, Proceedings*, pages 14–23. Springer.

Kemper, G. (2019). Improving employees' cyber security awareness. *Computer Fraud & Security*, 2019(8):11–14.

Khader, M., Karam, M., and Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, 12(10):417.

Khando, K., Gao, S., Islam, S. M., and Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security*, 106:102267.

Ki-Aries, D. and Faily, S. (2017). Persona-centred information security awareness. *computers & security*, 70:663–674.

Korovessis, P., Furnell, S., Papadaki, M., and Haskell-Dowland, P. (2017). A toolkit approach to information security awareness and education. *Journal of Cybersecurity Education, Research and Practice*, 2017(2):5.

Kovačević, A., Putnik, N., and Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access*, 8:125140–125148.

Kovačević, A. and Radenković, S. D. (2020). Sawit—security awareness improvement tool in the workplace. *Applied Sciences*, 10(9):3065.

Larsen, K. R., Lukyanenko, R., Mueller, R. M., Storey, V. C., VanderMeer, D., Parsons, J., and Hovorka, D. S. (2020). Validity in design science research. In *Designing for Digital Transformation. Co-Creating Services with Citizens and Industry: 15th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2020, Kristiansand, Norway, December 2–4, 2020, Proceedings 15*, pages 272–282. Springer.

Li, L., Xu, L., He, W., Chen, Y., and Chen, H. (2016). Cyber security awareness and its impact on employee's behavior. In *Research and Practical Issues of Enterprise Information Systems: 10th IFIP WG 8.9 Working Conference, CONFENIS 2016, Vienna, Austria, December 13–14, 2016, Proceedings 10*, pages 103–111. Springer.

Li, Y. and Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports*, 7:8176–8186.

Lindgreen, A., Di Benedetto, C. A., and Brodie, R. J. (2021). Research quality: What it is, and how to achieve it. *Industrial Marketing Management*, 99:A13–A19.

Loukis, E. and Spinellis, D. (2001). Information systems security in the greek public sector. *Information management & computer security*, 9(1):21–31.

Mansfield-Devine, S. (2017). Raising awareness: People are your last line of defence. *Computer Fraud & Security*, 2017(11):10–14.

March, S. T. and Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems*, 15(4):251–266.

Marshall, M. N. (1996). Sampling for qualitative research. *Family practice*, 13(6):522–526.

Mohajan, H. K. et al. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series*, 17(4):59–82.

Myers, M. D. and Venable, J. R. (2014). A set of ethical principles for design science research in information systems. *Information & Management*, 51(6):801–809.

Neigel, A. R., Claypoole, V. L., Waldfogle, G. E., Acharya, S., and Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers & Security*, 92:101731.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA-Journal of Business and Public Administration*, 9(3):71–88.

Nohlberg, M. (2008). *Securing information assets: understanding, measuring and protecting against social engineering attacks*. PhD thesis, Institutionen för data-och systemvetenskap (tills m KTH).

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., and Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (hais-q). *Computers & security*, 42:165–176.

Paterson, O. (2021). Training is the foundation of security. *Computer Fraud & Security*, 2021(8):10–13.

Peffers, K., Rothenberger, M., Tuunanen, T., and Vaezi, R. (2012). Design science research evaluation. In *Design Science Research in Information Systems. Advances in Theory and Practice: 7th International Conference, DESRIST 2012, Las Vegas, NV, USA, May 14-15, 2012. Proceedings 7*, pages 398–410. Springer.

Peffers, K., Tuunanen, T., and Niehaves, B. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, 24(3):45–77.

Pollock, T. (2017). Reducing human error in cyber security using the human factors analysis classification system (hfacs). In *2017 Ksu Conference on Cybersecurity Education, Research and Practice*.

Power, R. and Forte, D. (2006). Case study: a bold new approach to awareness and education, and how it met an ignoble fate. *Computer Fraud & Security*, 2006(5):7–10.

Price, J. H. and Murnan, J. (2004). Research limitations and the necessity of reporting them. *American journal of health education*, 35(2):66.

Quayyum, F., Cruzes, D. S., and Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30:100343.

Ramluckan, T., Martins, B. v. N. I., et al. (2020). A change management perspective to implementing a cyber security culture. In *ECCWS 2020 20th European Conference on Cyber Warfare and Security*, page 442.

Reegård, K., Blackett, C., and Katta, V. (2019). The concept of cybersecurity culture. In *29th European Safety and Reliability Conference*, pages 4036–4043.

Reeves, A., Calic, D., and Delfabbro, P. (2021). "get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training. *Computers & security*, 106:102281.

Renaud, K. (2018). Cooking up security awareness & training. *Network Security*, 2018(5):20–20.

Riel, M. (1998). Education in the 21st century: Just-in-time learning or learning communities. In *fourth annual conference of the emirates center for strategic studies and research, Abu Dhabi*.

Rohan, R., Funilkul, S., Pal, D., and Chutimaskul, W. (2021). Understanding of human factors in cybersecurity: A systematic literature review. In *2021 International Conference on Computational Performance Evaluation (ComPE)*, pages 133–140. IEEE.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., and Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*.

Ruighaver, A. B., Maynard, S. B., and Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & security*, 26(1):56–62.

Safa, N. S. and Maple, C. (2016). Human errors in the information security realm–and how to fix them. *Computer Fraud & Security*, 2016(9):17–20.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53:65–78.

Sardar, T. and Wahsheh, L. A. (2020). Design of a cyber security awareness campaign to be implemented in a quarantine laboratory. *Journal of Computing Sciences in Colleges*, 35(9):11–18.

Scholefield, S. and Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. In *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings 21*, pages 191–203. Springer.

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., and von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, 119:102756.

Singh, D., Mohanty, N. P., Swagatika, S., and Kumar, S. (2020). Cyber-hygiene: The key concept for cyber security in cyberspace. *Test Engineering and Management*, 83:8145–8152.

Solomon, A., Michaelshvili, M., Bitton, R., Shapira, B., Rokach, L., Puzis, R., and Shabtai, A. (2022). Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowledge-Based Systems*, 246:108709.

Stahl, S. (2006). Beyond information security awareness training: it's time to change the culture. *Inf. Secur. Manag. Handb*, 3(3):285.

Stenfors, T., Kajamaa, A., and Bennett, D. (2020). How to... assess the quality of qualitative research. *The clinical teacher*, 17(6):596–599.

Syafrizal, M., Selamat, S. R., and Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, 12(3):417–432.

Szumski, O. (2018). Cybersecurity best practices among polish students. *Procedia Computer Science*, 126:1271–1280. Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 22nd International Conference, KES-2018, Belgrade, Serbia.

Tariq, M. A., Brynielsson, J., and Artman, H. (2014). The security awareness paradox: A case study. In *2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2014)*, pages 704–711. IEEE.

Tasevski, P. (2016). It and cyber security awareness-raising campaigns. *Information & Security*, 34(1):7–22.

Theofanidis, D. and Fountouki, A. (2018). Limitations and delimitations in the research process. *Perioperative Nursing-Quarterly scientific, online official journal of GORNA*, 7(3 September-December 2018):155–163.

Tirumala, S., Valluri, M. R., and Babu, G. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI)*, pages 1–6. IEEE.

Tolah, A., Furnell, S. M., and Papadaki, M. (2021). An empirical analysis of the information security culture key factors framework. *Computers & Security*, 108:102354.

Tonkin, A., Kosasih, W., Grobler, M., and Nasim, M. (2022). Simulating cyber security management: A gamified approach to executive decision making. In *37th IEEE/ACM International Conference on Automated Software Engineering*, pages 1–8.

Trim, P. R. and Lee, Y.-I. (2019). The role of b2b marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, 83:224–238.

Tschakert, K. F. and Ngamsuriyaroj, S. (2019). Effectiveness of and user preferences for security awareness training methodologies. *Heliyon*, 5(6):e02010.

Tu, C. Z., Yuan, Y., Archer, N., and Connelly, C. E. (2018). Strategic value alignment for information security management: A critical success factor analysis. *Information & Computer Security*.

Uchendu, B., Nurse, J. R., Bada, M., and Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109:102387.

Vaishnavi, V. K. (2007). *Design science research methods and patterns: innovating information and communication technology*. Auerbach Publications.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38:97–102.

Wang, Y., Qi, B., Zou, H.-X., and Li, J.-X. (2018). Framework of raising cyber security awareness. In *2018 IEEE 18th International Conference on Communication Technology (ICCT)*, pages 865–869.

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management*, 24(1):43–57.

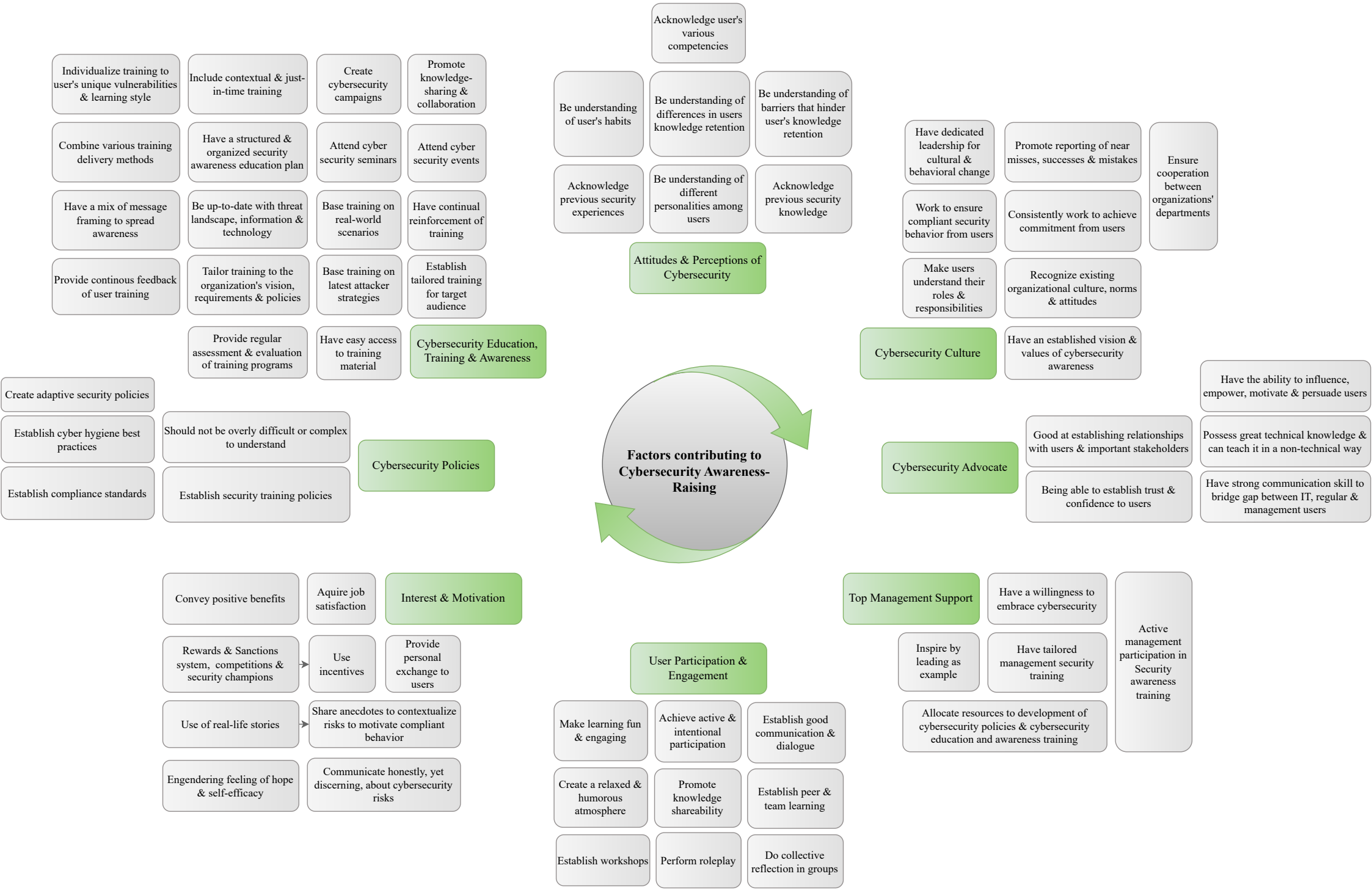
Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., and Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66:102520.

Zhang, Z., Wenzhuo Li, W., and Abdous, M. (2021). Cybersecurity awareness training programs: a cost-benefit analysis framework. *Industrial Management & Data Systems*, 121(3):613–636.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., and Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1):82–97.

A | Appendix: Guideline's First Draft in Design Cycle One

This Appendix presents a complete picture of the guideline's first draft developed during design cycle one.


Factors contributing to Cybersecurity Awareness-Raising
Cybersecurity Education, Training & Awareness
Individualize training to user's unique vulnerabilities & learning style
Include contextual & just-in-time training
Create cybersecurity campaigns
Promote knowledge-sharing & collaboration
Combine various training delivery methods
Have a structured & organized security awareness education plan
Attend cyber security seminars
Attend cyber security events
Have a mix of message framing to spread awareness
Be up-to-date with threat landscape, information & technology
Base training on real-world scenarios
Have continual reinforcement of training
Provide continous feedback of user training
Tailor training to the organization's vision, requirements & policies
Base training on latest attacker strategies
Establish tailored training for target audience
Provide regular assessment & evaluation of training programs
Have easy access to training material
Attitudes & Perceptions of Cybersecurity
Acknowledge user's various competencies
Be understanding of user's habits
Be understanding of differences in users knowledge retention
Be understanding of barriers that hinder user's knowledge retention
Acknowledge previous security experiences
Be understanding of different personalities among users
Acknowledge previous security knowledge
Cybersecurity Culture
Have dedicated leadership for cultural & behavioral change
Promote reporting of near misses, successes & mistakes
Ensure cooperation between organizations' departments
Work to ensure compliant security behavior from users
Consistently work to achieve commitment from users
Make users understand their roles & responsibilities
Recognize existing organizational culture, norms & attitudes
Have an established vision & values of cybersecurity awareness
Cybersecurity Advocate
Have the ability to influence, empower, motivate & persuade users
Good at establishing relationships with users & important stakeholders
Possess great technical knowledge & can teach it in a non-technical way
Being able to establish trust & confidence to users
Have strong communication skill to bridge gap between IT, regular & management users
Cybersecurity Policies
Create adaptive security policies
Establish cyber hygiene best practices
Should not be overly difficult or complex to understand
Establish compliance standards
Establish security training policies
Interest & Motivation
Convey positive benefits
Aquire job satisfaction
Rewards & Sanctions system, competitions & security champions
Use incentives
Provide personal exchange to users
Use of real-life stories
Share anecdotes to contextualize risks to motivate compliant behavior
Engendering feeling of hope & self-efficacy
Communicate honestly, yet discerning, about cybersecurity risks
User Participation & Engagement
Make learning fun & engaging
Achieve active & intentional participation
Establish good communication & dialogue
Create a relaxed & humorous atmosphere
Promote knowledge shareability
Establish peer & team learning
Establish workshops
Perform roleplay
Do collective reflection in groups
Top Management Support
Have a willingness to embrace cybersecurity
Active management participation in Security awareness training
Inspire by leading as example
Have tailored management security training
Allocate resources to development of cybersecurity policies & cybersecurity education and awareness training

B | Appendix: Interview Questions in Design Cycle One

This Appendix presents this thesis' interview questions used to gather information and feedback from interviewees during the first design cycle.

Interview Questions for Design Cycle 1

Part 1

Background about the interviewees

1) Do you work within a large Swedish public organization?
   a) What is your role in this workplace?
   b) For how long have you been in that role?
   c) What are the typical responsibilities that come with that position?
   d) What prior experiences with cybersecurity awareness do you have?
2) How confident are you when it comes to your knowledge of cybersecurity awareness? Please rate yourself on a scale of 1 to 10, where 1 means you have little to no understanding, and 10 means you have a strong and thorough understanding.
   a) Could you explain the reasoning behind the rating you have selected?

Part 2

Explore interviewees' thoughts, knowledge and experience about cybersecurity awareness.

1) Why do you think working with cybersecurity awareness is so important?
2) How do you think organizations should work with cybersecurity awareness in the present day?
3) In your opinion, what do you consider to be the greatest challenges in that work?
4) What are the possible solutions to overcome these challenges?
5) What do you consider to be the most important factors that contribute to the increase of cybersecurity awareness?
6) Would you say it is possible to rank the named factors in order of their importance, from most to least important?
   a) [No] How come?
   b) [Yes] Please explain the reasoning behind your ranking.
7) Is there a model, framework, or guideline in your organization that assists with your cybersecurity awareness tasks?
   a) [Yes] Could you provide me with information about that aid?
   b) [No] What should this aid look like and what content should it have?

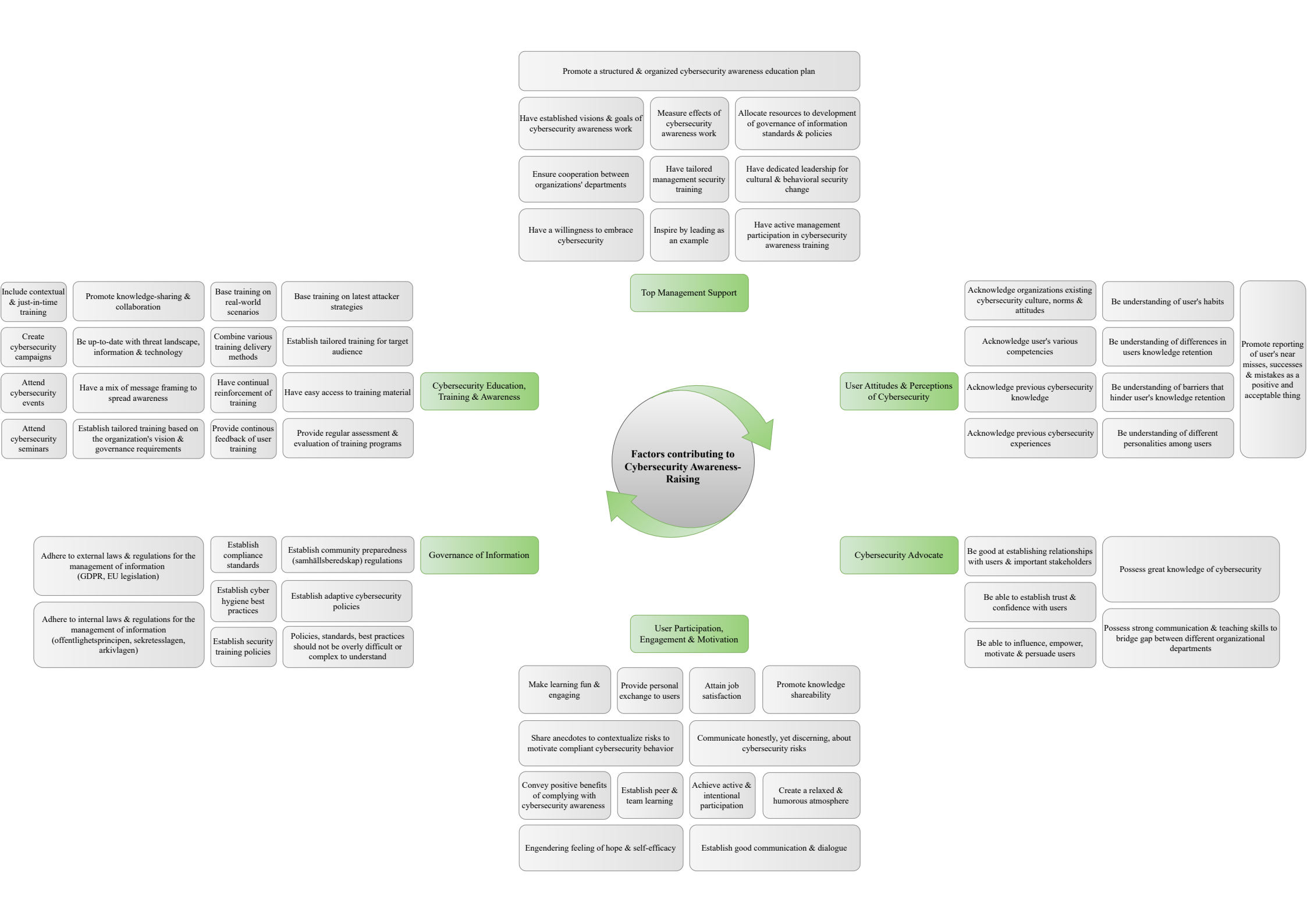
Part 3

Demonstration of the guidelines first draft and retrieval of feedback.

1) What are your initial impressions of this guideline?
2) Do you believe this guideline would be useful for a large Swedish public organization like yours?
    a) In what way would it be useful?
3) Do you have any suggestions for additional information that you would like to see included in the guideline?
4) Do you see any issues with this guideline that should be addressed and potentially removed?
5) Do you think there is anything in this guideline that should be relocated?
6) Is it comprehensible to understand?
    a) If not, how can I render it so?
7) Is it a good layout?
    a) If not, how can I render it so?

C | Appendix: Guideline's Second Draft in Design Cycle Two

This Appendix presents a complete picture of the guideline's second draft developed during design cycle two.


Factors contributing to Cybersecurity Awareness-Raising
Top Management Support
Promote a structured & organized cybersecurity awareness education plan
Have established visions & goals of cybersecurity awareness work
Measure effects of cybersecurity awareness work
Allocate resources to development of governance of information standards & policies
Ensure cooperation between organizations' departments
Have tailored management security training
Have dedicated leadership for cultural & behavioral security change
Have a willingness to embrace cybersecurity
Inspire by leading as an example
Have active management participation in cybersecurity awareness training
Cybersecurity Education, Training & Awareness
Include contextual & just-in-time training
Promote knowledge-sharing & collaboration
Base training on real-world scenarios
Base training on latest attacker strategies
Create cybersecurity campaigns
Be up-to-date with threat landscape, information & technology
Combine various training delivery methods
Establish tailored training for target audience
Attend cybersecurity events
Have a mix of message framing to spread awareness
Have continual reinforcement of training
Have easy access to training material
Attend cybersecurity seminars
Establish tailored training based on the organization's vision & governance requirements
Provide continous feedback of user training
Provide regular assessment & evaluation of training programs
User Attitudes & Perceptions of Cybersecurity
Acknowledge organizations existing cybersecurity culture, norms & attitudes
Be understanding of user's habits
Promote reporting of user's near misses, successes & mistakes as a positive and acceptable thing
Acknowledge user's various competencies
Be understanding of differences in users knowledge retention
Acknowledge previous cybersecurity knowledge
Be understanding of barriers that hinder user's knowledge retention
Acknowledge previous cybersecurity experiences
Be understanding of different personalities among users
Governance of Information
Adhere to external laws & regulations for the management of information (GDPR, EU legislation)
Adhere to internal laws & regulations for the management of information (offentlighetsprincipen, sekretesslagen, arkivlagen)
Establish compliance standards
Establish community preparedness (samhällsberedskap) regulations
Establish cyber hygiene best practices
Establish adaptive cybersecurity policies
Establish security training policies
Policies, standards, best practices should not be overly difficult or complex to understand
Cybersecurity Advocate
Be good at establishing relationships with users & important stakeholders
Possess great knowledge of cybersecurity
Be able to establish trust & confidence with users
Possess strong communication & teaching skills to bridge gap between different organizational departments
Be able to influence, empower, motivate & persuade users
User Participation, Engagement & Motivation
Make learning fun & engaging
Provide personal exchange to users
Attain job satisfaction
Promote knowledge shareability
Share anecdotes to contextualize risks to motivate compliant cybersecurity behavior
Communicate honestly, yet discerning, about cybersecurity risks
Convey positive benefits of complying with cybersecurity awareness
Establish peer & team learning
Achieve active & intentional participation
Create a relaxed & humorous atmosphere
Engendering feeling of hope & self-efficacy
Establish good communication & dialogue

D | Appendix: Interview Questions in Design Cycle Two

This Appendix presents this thesis' interview questions used to gather information and feedback from interviewees during the second design cycle.

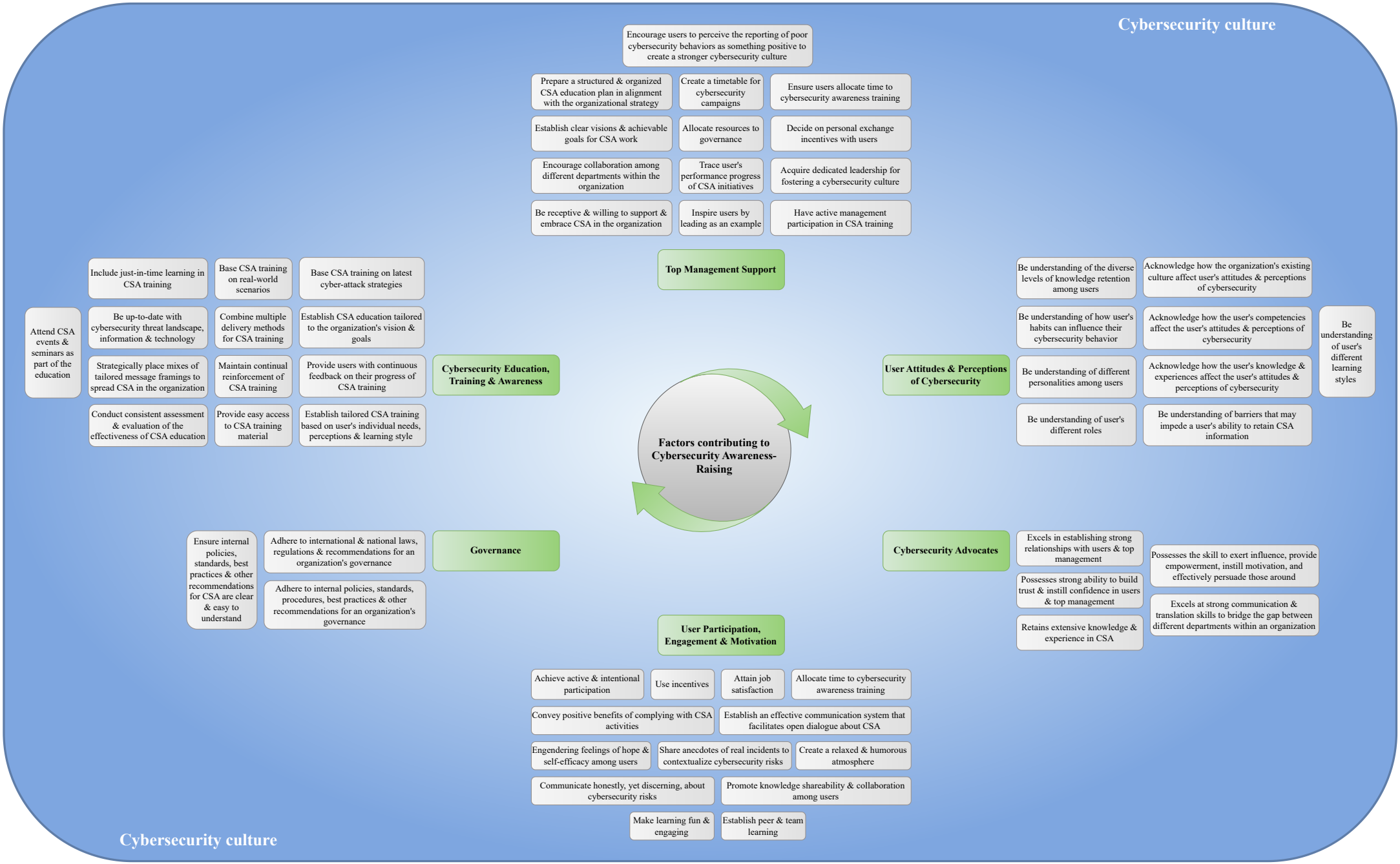
Interview Questions for Design Cycle 2

Part 1

Reconciliation regarding changes made for the guideline's second draft.

1) What do you think about the changes that were implemented in the guideline?
2) Do you think the revised guideline is an improvement or a decline from the previous version?
    a) In what way?
3) Do you believe that the sub-factors in the guideline are distinctly delimited to each green principal factor?
4) Do you have any suggestions for additional information that you would like to see included in the guideline?
5) Do you see any issues with this guideline that should be addressed and potentially removed?
6) Do you think there is anything in this guideline that should be relocated?
7) Is it comprehensible to understand?
    a) If not, how can I render it so?
8) Is it a good layout?
    a) If not, how can I render it so?

E | Appendix: Guideline's Final Result

This Appendix presents a complete picture of the guideline's final result. This is the third and final draft.

Cybersecurity Awareness (CSA)