DEGREE PROJECT

Change Management: A Key in Achieving Successful Cyber Security

A Multiple Case Study of Organizations in Sweden

Emma Ryttare

Industrial and Management Engineering, master's level
2019

Luleå University of Technology
Department of Business Administration, Technology and Social Sciences

LULEÅ UNIVERSITY OF TECHNOLOGY

ABSTRACT

Purpose – The purpose of this study is to enhance the understanding of how organizations can improve their cyber security with change management. To fulfill the purpose, the following research questions were developed: *RQ1: What are the key factors for effective change management in the context of cyber security?* and *RQ2: How can organizations manage these factors to improve cyber security?*

Method – A qualitative research method with an inductive approach was chosen. The empirical data collection was performed as a multiple case study with 16 semi-structured interviews with respondents from six organizations, and the data were analyzed through a thematic analysis.

Result – The findings of this study is gathered in a framework for successful cyber security culture change that highlights each essential activity for how to improve cyber security with change management. It also shows when and how these activities should be performed, when to consider each leadership characteristic, and what employee sensemaking needs that should be considered during the process.

Theoretical contribution – The study contributes to both cyber security literature and change management literature. It contributes to the cyber security literature by providing a processual model that illustrates the factors dependency of each other. Also, by adding the perspective of sensemaking, the study provides an overall picture, with both a leader and employee perspective, of how change management can be used to improve cyber security. Additionally, this study extends earlier change management literature by providing a sensemaking approach to the change process.

Managerial implications – The study contributes with valuable insights for management in practice by presenting a framework that can help CISO's, security consultants or other managers responsible for the organizations security to execute successful cyber security culture change. With the presented framework, they can plan, execute and sustain the change in the organization's cyber security culture.

Keywords: Cyber Security; Change Management; Sensemaking; Leadership

ACKNOWLEDGEMENTS

This master thesis was written by Emma Ryttare, during the spring of 2019, and is the final part of a master's degree in Industrial Engineering and Management with specialization in Innovation and Strategic Business Development at Luleå University of Technology.

First of all, I would like to express my greatest gratitude towards my supervisor at the university, Mats Westerberg. I am very thankful for all the feedback and support that I have received throughout the process, it has been invaluable. Secondly, thank you to my supervisor at one of the case organizations, Åsa Schwarz, for all the support and inspiration along the way. I also want to express a big thanks to all the interview respondents for sharing your ideas, knowledge, and experience with me. Lastly, thank you to the students at the university for providing me with valuable feedback for my thesis.

Stockholm, 2019-06-13

Emma Ryttare

TABLE OF CONTENT

1. INTRODUCTION

With the rise of digitalization and Internet of Things (IoT), organizations are getting more and more digitally connected. Nowadays, organizations are not only using IT as support for its business, instead, it is used as an integrated and central part of an organization's everyday operation (Poppensieker & Riemenschnitter, 2018). While organizations are becoming more digitalized, the threats of cyberattacks are a higher concern than ever before (Poppensieker & Riemenschnitter, 2018; Ransbotham, 2017; Syed, Padmanabhan, & Dixon, 2014; Jalali, 2018; PwC, 2017). Cyberhackers can nowadays reach far more vulnerable parts of an organization such as control systems or specific connected IoT devices (Poppensieker & Riemenschnitter, 2018). The cyberattacks can according to Jalali (2018) create devastating operational and financial consequences, moreover, it risks creating damage to the organization's reputation and facing consequences such as lawsuits. An organization that suffered from a serious cyberattack was the American retail store Target. In 2013, cyberhackers stole personal data from about 70 million customers and payment card numbers of around 40 million which lead to profits dropping, the organization's reputation was harmed, and the organizations CEO and CIO lost their jobs (Upton & Creese, 2014). A study presented by Bauer, Scherf and von der Tann (2017) reveals that risk managers consider risks of cyberattacks to be the biggest threat to their organization, and 75% of risk managers see cyber security as their number one priority. However, only 16% of the managers in the study believe that they are well prepared to deal with the cyber-risks. Therefore, organizations are in need to invest in cyber security in order to secure their operation from any current or future threats of cyberattacks.

Managing cyber security is defined by Spremic and Simunic (2018) as "to carefully design and implement basic protection to prevent common attacks, but also, innovative, smart and sophisticated security controls to detect and respond to advanced and emerging threats" (Spremic & Simunic, 2018, p. 2). For instance, cyber security initiatives could involve implementing new security systems, policies or guidelines. Even though investing in cyber security many organizations are still struggling with keeping their organization

secure. According to Lacey (2010), Pfleeger and Caputo (2012) and Safa et al. (2015) technological solutions are not enough to keep the organization safe. Many sources are arguing that the reason for the cyber security initiatives to be unsuccessful is the lack of focus on the human factor in security projects (Lacey, 2010; Orshesky, 2003; Pfleeger & Caputo, 2012; Stewart & Jürjens, 2017). The human factor involves how people interact and relate to security (Orshesky, 2003). Stewart and Jürjens (2017) argue that the human aspect is the most critical factor in managing security. For instance, cyberattacks are not only targeting the technological systems in an organization, and the concept of social engineering is a common issue for organizations. Social engineering describes the process in which cyberhackers targets people and influences them to reveal sensitive information (Mouton, Leenen & Venter, 2016). Hence, it is essential for organizations to focus on the people in the organization in order to prevent from these common cyberattacks. Furthermore, Orshesky (2003) mentions that a survey involving over 1000 organizations showed that the majority of the participating organizations failed to meet the tolerable standard for managing security and that they ignored to consider the human factor in security management. Ashenden and Sasse (2013) underline that information security is dependent on change management and the work of persuading the people in the organization to behave securely.

To illustrate the problem, imagine that an organization has worked with a project involving a new security policy. When the policy is finished, it is only emailed to everyone in the organization and it is expected that everyone in the organization commits to the new security policy. This kind of situation is common among organizations and makes it difficult for the people in the organization to be on board with the change since they have not gotten the chance to learn the new policy. According to D'Arcy and Greene (2014), a major challenge for organizations is to encourage the employees to comply with the security policies and procedures. If an organization lacks policy compliance, which according to Stewart and Jürjens (2017) is referred to as conforming to a rule or a policy, the policy will not be effective. In a study mentioned by Orshesky (2003), many of the participating organizations mentioned that they had documented security policies, however, less than 20% of the organizations responded that they had

fully implemented security policies that were involving the human factor. This requires organizations to focus on policy enactment, which according to Braun, Ball, Maguire, and Hoskins (2011) involves the translation and interpretation of policy ideas into contextualized practices. Additionally, Lacey (2010) states that there needs to be less emphasis on formal procedures and more focus on engagement with people. Thus, to improve cyber security large attention should be on change management (Da Veiga & Martins, 2015).

In a study from IBM, 87% of the respondents believed that there is not enough focus on change management for critical projects, such as cyber security projects (Jorgensen, Bruehl, & Franke, 2014). Change management is according to Duck (1993) described as "managing the conversation between the people leading the change effort and those who are expected to implement the new strategies, managing the organizational context in which change can occur, and managing the emotional connections that are essential for any transformation" (Duck, 1993, p. 110). In any kind of project, including cyber security projects, the people in the organization will struggle to be devoted to the change if they are not considered in the change. Levasseur (2001) makes the comparison to performing open-heart surgery and then leaving the patient to take responsibility for their own care from that point on. The author means that it is the same with change management, if you do not get the people committed to the change they will continue in the same pattern and the change initiative will not be effective. Hence, it is essential that organizations focus on change management in order for the cyber security initiatives to be successful (Ashenden & Sasse, 2013; Da Veiga & Eloff, 2007; Da Veiga & Martins, 2015; Soomro et al., 2016). One central aspect to consider for effective change management is to take the employees' sensemaking needs into consideration. Sensemaking is the process in which people interpret and make sense of activities in the change process in order to understand and deal with change successfully (Du Toit, 2007; Thurlow & Mills, 2009). Thus, it is important to consider the employees sensemaking needs in order for the employees to feel make sense of the change management process.

Change management is not an easy task and many organizations are struggling with achieving successful transformation projects. In fact, most change efforts fail. According to a McKinsey survey (McKinsey, 2008) with over 3000 managers around the world, only a third responded that their change effort was successful. Additionally, Kotter (2007) mentions that most fall in between success and failure while Burnes (2011) argues that there have in over 40 years been far more change initiatives that have failed than succeeded. The previous research of change management in the context of cyber security has mainly been focusing on certain individual aspects of change management. For example, several articles have studied how organizations can improve the cyber security by changing the employees' behavior (Hadlington, 2018; Pfleeger & Caputo, 2012; Pfleeger, Sasse & Furnham, 2014). Yet, this is only a part of change management and research which investigates the problem at the organizational level has not received much attention (Stewart & Jürjens, 2017). Additionally, Maglaras et al. (2018) and Parsons, Young, Butavicius, McCormac, Pattinson, and Jerram (2015) argue that there should be increased empirical research that investigates cyber security with regards to the people in the organization, also, Stewart and Kringas (2003) mention that empirical studies that intend to draw lessons from the experiences of change management are rare. Hence, the purpose of this study is to *enhance the understanding of how organizations can improve their cyber security with change management.*

To fulfill the purpose, the following research questions will guide the study:

RQ1: *What are the key factors for effective change management in the context of cyber security?*

RQ2: *How can organizations manage these factors to improve cyber security?*

The study will fulfill the purpose by performing a qualitative study and collecting empirical data from a multiple case study. By analyzing the collected data, a framework for how organizations can improve their cyber security with change management will be provided.

2. LITERATURE REVIEW

To fulfill the purpose of the study, this chapter provides a literature review comprising theory from previous research in both the field of change management and cyber security. The literature review aims to give a deeper understanding of the research field and to serve as a theoretical framework for the empirical data collection. The first section starts off with a review of literature in the area of cyber security and is then followed by a discussion of theories and models for effective change management. Next, the literature review combines the two areas and discusses change management in the context of cyber security. Lastly, a discussion on how the literature review connects to the research questions is provided.

2.1 Cyber security

Security is according to von Solms and van Niekerk (2013) the protection of assets from the different threats posed by certain vulnerabilities. In the literature field of security, there are several terms that are closely related to each other, *information security*, *information and communication technology (ICT) security* and *cyber security*. The article by von Solms and van Niekerk (2013) has provided an effort into clarifying the different terms and how they relate to each other. The authors state that ICT security involves the protection of the underlying technology while information security involves the protection of all information including the underlying technology. Cyber security, on the other hand, is a term that has been used differently among authors. Different interpretations and explanations have been given and B. von Solms and R. von Solms (2018) state that numerous articles argue that cyber security is the same as information security and can be used as a synonym to information security. However, according to von Solms and van Niekerk (2013), the term cyber security is not equivalent to the term information security, although, the authors state that the terms are closely related. The difference is according to the authors that cyber security is not just about protecting the information, it is also about protecting the people that function in cyberspace and any of their assets that can be reached through cyberspace. Therefore, the authors define cyber security as "the protection of cyberspace itself, the electronic information, the ICTs that

support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace" (von Solms & van Niekerk, 2013, p.101). Additionally, Pfleeger and Caputo (2012) mention that cyber security assures protection and prevention from cyberattacks by using a combination of innovative technology and an understanding of the human user. Similarly, B. von Solms and R. von Solms (2018) states that cyber security involves protecting from the risks that appear when an organization is in some way digitally connected. Furthermore, Spremic and Simunic (2018) describe the main objective for managing cyber security as "to carefully design and implement basic protection to prevent common attacks, but also, innovative, smart and sophisticated security controls to detect and respond to advanced and emerging threats" (Spremic & Simunic, 2018, p. 2).

With this discussion, the concept of cyber security will in this study be seen as an extension of information security. Literature from the information security field will also be used in the study since information security is a part of cyber security and thus the research in this area is seen as highly relevant for the present study. An overview of the different terms and how they differentiate from each other can be seen in Table 1.

Table 1. Descriptions of the terms in the security research field. Adapted from von Solms and van Niekerk (2013).

Term	***Description***
Security	The protection of assets from the different threats posed by certain vulnerabilities
ICT security	The protection of the underlying technology
Information security	The protection of all information including the underlying technology
Cyber security	The protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace

2.1.1 Cyber security governance

When managing cyber security, there is a need for controls to protect the organization from cyber threats. Cyber security governance, which is closely related to information security governance, is a concept that von Solms and von Solms (2018) describe as "the process of directing and controlling the protection of a company's digital information assets from the risks that are related to using the internet" (von Solms & von Solms, 2018, p. 6). von Solms (2006) states that information security governance can be seen as an overall approach for organizations to mitigate security risks. According to the article by Da Veiga and Eloff (2007) a comprehensive information security governance framework is divided into three components and consists of six main categories:

- Strategic:
    - Leadership and Governance
- Managerial and Operational:
    - Security Management and Organization
    - Security Policies
    - Security Program Management
    - User Security Management
- Technical:
    - Technology Protection and Operations (Da Veiga & Eloff, 2007).

First of all, Da Veiga and Eloff (2007) describe Leadership and Governance as the category that involves commitment from the management and board of directors to protect information assets as well as executive level sponsorship for information security. Secondly, the category of Security Management and Organization covers legal and regulatory considerations and program organization (Da Veiga & Eloff, 2007). Program organization is what the authors refer to as information security organizational structure, design, composition and reporting structure, which also includes roles and responsibilities, and skills and experiences. Furthermore, Security Policies is the category that involves the policies, guidelines, procedures, and standards for information security which are essential in order to provide support and direction to the management (Da

Veiga & Eloff, 2007). Security policies propose the desired behavior of the employees (Osuagwu et al., 2015). According to Osuagwu et al. (2015), there are many standards and best practices currently established for information security and the authors mention that these standards can, for instance, be international standards such as ISO27001 and ISO27002, and other national guidelines and standards for different countries. The ISO/IEC 27000 family of standards is a group of popular standards that organizations are using to keep their information assets secure (ISO, n.d.).

In the category of Security Program Management, compliance, monitoring, and auditing are according to Da Veiga and Eloff (2007) essential factors for the management of information security. For instance, monitoring of both the employee behavior and technology is important to ensure compliance with information security policies (Da Veiga & Eloff, 2007). Compliance is according to Stewart and Jürjens (2017) referred to as the conforming to a policy or rule. The User Security Management category concerns aspects such as user awareness, education, training, trust, privacy, and ethical conduct. According to Osuagwu et al. (2015), education and training ensure that employees are trained to become aware of protecting information assets. The last category, Technology Protection and Operations, is according to Da Veiga and Eloff (2007) related to the traditional focus of information security which involves technical and physical controls in order to secure an organizations IT environment. Osuagwu et al. (2015) mention that technology controls could, for instance, be a thumbprint scanner or a firewall that can enhance an organizations information security. Conclusively, Da Veiga and Eloff (2007) state that change management should be involved when implementing any of the security governance components.

2.2 Change management

Change management is a concept that has been around for a long time and has received numerous definitions in the literature field. Moran and Brightman (2000) define change management as "the process of continually renewing the organization's direction, structure, and capabilities to serve the ever-changing needs of the marketplace, customers and employees" (Moran & Brightman, 2000, p. 73). Additionally, Duck (1993) describe

change management as "managing the conversation between the people leading the change effort and those who are expected to implement the new strategies, managing the organizational context in which change can occur, and managing the emotional connections that are essential for any transformation" (Duck, 1993, p. 110). Change management involves evolving from a current state to reach a desired state (Galli, 2018; Hussain et al., 2018) and the goal is according to Chou (2007) to achieve a better performance of the organization. The article by Yilmaz, Ozgen, and Akyel (2013) adds that organizational change is aimed at either increasing the performance or to adapt to the environment. From these definitions of change management, it is clear that organizational change requires a great focus on the people in the organization.

Leadership plays an essential role in change management (Page & Schoder, 2018; Rao, 2015). Rao (2015) define change leadership as "the process of neutralizing the anti-change forces and persuading the people to fall in line for the prosperity of the organization and its people" (Rao, 2015, p. 36). The article by Page and Schoder (2018) mentions that leadership is essential for creating the vision for change and to eliminate any obstacles that employees could be facing. A good change leader is according to Rao (2015) characterized as someone that clearly state the vision and cultivate hope, build trust and confidence, possess strong communication skills and empower and motivate the people in the organization.

2.2.1 Employee sensemaking and leader sensegiving

In order to understand change, one needs to understand which messages that have been received, how the messages have been interpreted and why, and how these are affecting behavior (Balogun, 2006). The people involved in the change process might experience the situation as unclear and ambiguous, hence, to create effective change it is essential to help the people involved to make sense of the context that they are working in (Tyler, 2005). This leads to the concept of sensemaking, and the related concept of sensegiving, which the literature field emphasize as important to consider for effective change management (Ala-Laurinaho, Kurki, & Simonsen Abildgaard, 2017; Apker, 2004; Balogun, 2006; Gioia & Chittipeddi, 1991; Kraft, Sparr, & Peus, 2018; Tyler, 2005).

Sensemaking is according to Weick, Sutcliffe and Obstfeld (2005) described as "a sequence in which people concerned with identity in the social context of other actors engage ongoing circumstances from which they extract cues and make plausible sense retrospectively, while enacting more or less order into those ongoing circumstances" (Weick et al., 2005, p. 409). Moreover, sensemaking is the process in which people interpret and make sense of activities in the change process in order to understand and deal with change successfully (Du Toit, 2007; Thurlow & Mills, 2009). Apker (2004) describe sensemaking as a key organizational practice and that it relates to change since change is a catalyst for social actors to be involved in sensemaking activities. Sensemaking is according to the article by Ala-Laurinaho et al. (2017) essential for the understanding of the social and psychological activities that occur during organizational change. Likewise, Gioia and Chittipeddi (1991) state that the acts of sensemaking and sensegiving constitute key processes involved in change management. The concept of sensegiving can be described as the effort by leaders to affect employees sensemaking (Kraft et al., 2018). It is according to Kraft et al. (2018) an essential leadership activity in organizational change.

To lead organizational change and to be able to cope with the peoples' sensemaking needs, there are several sensegiving activities that a leader could engage in. The article by Kraft et al. (2018) has investigated the employees' sensemaking needs during each phase of a change process adapted from Bullock and Batten (1985) which constitutes of four phases called *exploration*, *preparation*, *implementation*, and *evaluation*. The employees' sensemaking needs and the leaders respectively sensegiving actions during each phase are demonstrated in Table 2.

Table 2. Employee sensemaking needs and leader sensegiving for each phase. Reproduced from Kraft et al. (2018).

Phase in the change process	***Employee sensemaking***	***Leader sensegiving***
1. Exploration	Need for reassurance	Receptive sensegiving
2. Preparation	Need for orientation	Participative sensegiving
3. Implementation	Need for balance	Compensating sensegiving
4. Evaluation	Need for acknowledgement	Evaluative sensegiving

From this information, it is shown which sensegiving actions a leader should take, according to Kraft et al. (2018), in order to meet with the employees' sensemaking needs. In the first phase, *exploration*, the authors mention that employees experience concern and uncertainty about the situation and about what will really happen. Hence, it is essential for the leaders to relate to the employees' feelings and remove the fear of the fearful by signaling availability, providing stability and addressing concerns (Kraft et al., 2018). In the *preparation* phase, the employees feel the need for orientation to grasp the meaning of the change. According to Kraft et al. (2018), the leaders need to be participating in the employees' sensemaking and can, for instance, engage in discussions with the employees and ask the employees about their ideas and experiences. Also, it is important to create an environment of mutual trust (Kraft et al., 2018), and the article by Balogun (2006) state that change leaders should live the changes that they want others to adopt in order to provide a shared commitment and understanding. In the third phase, *implementation*, employees are experiencing a need for balance between the positive and negative aspects of the change. It is therefore important for the leaders to symbolize the benefits with the change and spread positive messages (Kraft et al., 2018). Lastly, in the *evaluation* phase, the employees feel a need for acknowledgement, and they evaluate their own part in the past change. Hence, the leaders should give and receive feedback, review success and challenges, and sustain the change environment by learning from mistakes and conveying confidence (Kraft et al., 2018). Similarly, the article by Balogun (2006) emphasizes that feedback is essential for sensemaking and states that organizations should use monitoring mechanisms to provide feedback on how the employees reacted to the change and why. The answer to why is according to the author important since it

supports change leaders to identify which actions and behaviors that need to be encouraged and which need to be changed or stopped.

2.2.2 Change management models

There are several processes and tools currently used by organizations for creating effective change management. According to Brisson-Banks (2010), Kurt Lewin's change management model is one of the earliest models and was first introduced in 1947 and breaks down change into three stages, *Unfreeze*, *Change*, and *Refreeze*. The first step *Unfreeze* is according to Levasseur (2001) the phase for organizations to unfreeze the current situation which according to Page and Schoder (2018) involves preparing the organization for the change and making sure that everyone in the organization, from senior managers to front-line workers, is informed of why the change is needed. The second stage called *Change* is where the organization move towards the new level and this is according to Page and Schoder (2018) the most challenging stage since it is now that the new process begins, and the comfortable and known way is over. In this step, the resistance from employees will start to appear since they are not used to the change and in order to ease the transition it is important to have resources available like for instance instructions, training or access to a manager to ask any questions that might appear (Galli, 2018). Lastly, the third step *Refreeze* includes making sure to stay at the new state and avoid that the organization returns to the prior state (Page & Schoder, 2018). In the refreezing stage it is according to Levasseur (2001) essential to work actively with the people in the organization to install, test, use, measure, and enhance the new system and the author mentions that it is for instance not tolerable to provide a report for the senior management and then expect that the people affected by the new change can implement the new system. The article by Burnes (2004) mentions that this model has received much criticism for being too simplistic since organizational change is more of an open-ended and continuous process. However, Page and Schoder (2018) mention that it is because of its applicability and simplicity that it remains relevant today. Additionally, the authors believe that the model serves as a foundation for effective change management.

Another well-known process used for effective change management is the model created by John P. Kotter in 1996 (Kotter, 2012). The model consists of eight steps for transforming an organization and leading organizational change (Kotter, 2007), and Kotter (2012) believes that it is essential to consider all of these eight steps in order for the change to be successful:

1) Establishing a sense of urgency
2) Forming a powerful guiding coalition
3) Creating a vision
4) Communicating the vision
5) Empowering others to act on the vision
6) Planning for and creating short-term wins
7) Consolidation improvements and producing still more change
8) Institutionalizing new approaches

In Table 3, an overview of the two models is provided to give an understanding of how they relate to each other.

Table 3. Lewin's and Kotter's change management models.

Lewin	***Kotter***
Unfreeze	Establishing a sense of urgency
	Forming a powerful guiding coalition
	Creating a vision
Change	Communicating the vision
	Empowering others to act on the vision
	Planning for and creating short-term wins
Refreeze	Consolidation improvements and producing still more change
	Institutionalizing new approaches

2.2.3 Comparing the different views and aspects for effective change management

The three-phase process by Lewin, the eight-step process by Kotter, and the aspects of sensemaking and sensegiving do all provide different views and essential aspects to consider for effective change management. The model by Lewin is, as Page and Schoder (2018) mentioned, a basis for change management and the model by Kotter provides a more detailed view of the change process. Page and Schoder (2018) state that large-scale change initiatives could benefit from both the simplicity of Lewin's model as well as the more detailed eight-stage process by Kotter. When it comes to the aspects of sensemaking and sensegiving, the focus is on the employees and how a leader can translate the activities in the change process in order for employees to understand and deal with change successfully (Du Toit, 2007; Thurlow & Mills, 2009).

When it comes to leading organizational change, there are similar aspects of Kotter's model and leader sensegiving. They are both providing suggestions on how organizations can lead change and how to engage and consider the employees in the change. Furthermore, one important aspect in employees sensemaking is communication (Balogun, 2006), which is an important part of Kotter's model as well. However, the model by Kotter emphasizes that the new vision created by the senior management should be communicated downwards to the people in the organization, while a sensemaking perspective provides a more bottom-up perspective where employees should be involved and included when working on creating the vision (Kraft et al., 2018). Moreover, in order for the organization to understand how employees react and respond to the change, the article by both Balogun (2006) and Kraft et al. (2018) emphasize the sensegiving action of giving and receiving feedback. This goes in line with both Lewin's and Kotter's models which also highlight this aspect in order to sustain the change and making sure the employees have understood and embraced the change. Overall, there are many existing models and theories used for effective change management, yet the ones described gives a comprehensive view of important aspects for organizations to consider when transforming their organization.

2.3 Combining change management practices with cyber security

The literature regarding change management to improve cyber security are scarce (Stewart & Jürjens, 2017), yet, there is current literature that discusses cyber security practices for specific aspects of the change process and also how to engage the people in an organization's cyber security. Therefore, this section will provide a comprehensive view of what the current literature has to say about how an organization can improve the cyber security with change management by considering the different perspectives of effective change management. An overview of the findings can be seen in Table 4.

Table 4. Key findings from the literature about change management in the context of cyber security.

Key findings	***Authors***
Senior management awareness	Alhogail & Mirza, 2014; Caldwell, 2016; Rothrock et al., 2018
Involvement of all employees	Alhogail & Mirza, 2014; Bevilacqua, 2017; Caldwell, 2016; Disparte & Furlow, 2017; Everett, 2010; Flowerday & Tuyikeze, 2016; Limba et al., 2017
Highlight security in a positive way	Bevilacqua, 2017; Caldwell, 2016; Limba et al., 2017; Parmar, 2013
Understanding of roles and consequences	Bevilacqua, 2017; Caldwell, 2016; Rothrock et al., 2018; Simmonds, 2018; Upton & Creese, 2014; Winnefeld Jr et al., 2015
Easy to ask questions	Bevilacqua, 2017; Caldwell, 2016; Winnefeld Jr et al., 2015
Customized training	Albrechtsen, 2007; Alhogail & Mirza, 2014; Caldwell, 2016; Dutta & McCrohan, 2002; Jenkins, 2012; Mansfield-Devine, 2017; Pfleeger et al., 2014; Upton & Creese, 2014
Interactive learning	Albrechtsen, 2007; Alhogail & Mirza, 2014; Bevilacqua, 2017; Caldwell, 2016; Jenkins, 2012; Mansfield-Devine, 2017
Feedback channels	Bevilacqua, 2017; Blau, 2017; Caldwell, 2016; Mansfield-Devine, 2017; Upton & Creese, 2014
Rewards	Alhogail & Mirza, 2014; Bevilacqua, 2017; Caldwell, 2016; Lacey, 2010; Mansfield-Devine, 2017
Effective measurements	Bevilacqua, 2017; Caldwell, 2016; Upton and Creese, 2014
Continuous change efforts	Alhogail & Mirza, 2014; Blau, 2017; Caldwell, 2016; Everett, 2010; Jenkins, 2012; Mansfield-Devine, 2017

Organizations need to start at the very top and make sure that ***the board and management understand*** the need for change (Alhogail & Mirza, 2014; Caldwell, 2016; Rothrock, Kaplan, & van der Oord, 2018). The article by Caldwell (2016) emphasizes that the change starts from the top of the organization and that it is important that senior managers create a culture that is sympathetic to security messages. Furthermore, when planning for the new change, one important aspect is to make sure that ***all employees are involved*** in the change (Alhogail & Mirza, 2014; Bevilacqua, 2017; Caldwell, 2016; Disparte & Furlow, 2017; Everett, 2010; Flowerday & Tuyikeze, 2016; Limba, Plèta, Agafonov, & Damkus, 2017). According to Caldwell (2016), the vulnerabilities can be where you least expect them which makes it important to change every employees' security-related behavior. Additionally, Flowerday and Tuyikeze (2016) highlight that the employees should be involved and considered early in the process in order for difficulties to be identified before, for example, the new security policy is implemented.

When creating the vision of the change and the plan for how to communicate the message to everyone, Limba et al. (2017) underline the importance of communicating the message so that everyone in the organization understands. In order for the employees to understand why there is a need to change, Caldwell (2016) mentions a key aspect as not communicating security issues in a negative way, by for example mentioning when something goes wrong. Instead, the author believes that it is more effective to ***highlight security success stories***. This is supported by Parmar (2013) which believes that it is important not to promote fear and rather encourage and motivate the employees. However, there are also articles emphasizing the importance of making sure the employees ***understand their roles and the consequences*** with security (Bevilacqua, 2017; Caldwell, 2016; Rothrock et al., 2018; Simmonds, 2018; Upton & Creese, 2014; Winnefeld Jr, Kirchhoff, & Upton, 2015). Additionally, Winnefeld Jr et al. (2015) underlines that every employee in the organization needs to understand that they are held accountable and are responsible for the things they can control. Similarly, Upton and Creese (2014) mention that employees need to understand what behaviors are acceptable and what is not. This can according to Upton and Creese (2014) be done by communicating to the employees that protecting the organization also protects their own

jobs, which creates an understanding of what the change means for them personally. These two aspects, *highlight security in a positive way* and *understanding of roles and consequences*, might seem a bit contradictory. However, comparing these findings with the change management literature about sensemaking and sensegiving, the article by Kraft et al. (2018) discusses that an employee sensemaking need is to receive a balance of the positive and negative aspects of the change. Hence, it might therefore be suitable to not only highlight security success stories but to also compensate by communicating the consequences of a security incident and as a leader try to find a balance in between.

Numerous articles emphasize the importance of having a security culture where every employee feels comfortable with talking and ***asking questions about security*** (Bevilacqua, 2017; Caldwell, 2016; Winnefeld Jr et al., 2015). Bevilacqua (2017) highlights that everyone in the organization should be able to raise any concern about security without hesitation. Additionally, this can be related to the sensemaking literature which underlines that employees have more questions about the change when they are in the middle of the change process and that it therefore is important for leaders to interact with the employees to provide the opportunity for them to ask questions and get updates on the changes (Balogun, 2006).

There are several articles that underline the importance of training programs in order for the employees to get knowledge of how to increase its cyber security thinking and protect the organization from any future potential violations (Albrechtsen, 2007; Alhogail & Mirza, 2014; Caldwell, 2016; Dutta & McCrohan, 2002; Jenkins, 2012; Mansfield-Devine, 2017; Pfleeger, Sasse, & Furnham, 2014; Upton & Creese, 2014). With regards to training and education for the employees, there are different ways to conduct it. Caldwell (2016) believes the best training is when organizations are using blended learning where e-learning modules are complemented by coaching, mentoring and classroom training in order for the training to get through to every employee. Likewise, the article by Upton and Creese (2014) underlines that organizations should perform ***customized training*** which takes into account the specific violations and threats a particular operation might encounter. Several articles emphasize that demonstrations and

hands-on activities are included in effective training and education programs (Albrechtsen, 2007; Alhogail & Mirza, 2014; Bevilacqua, 2017; Caldwell, 2016; Jenkins, 2012; Mansfield-Devine, 2017). The article by Albrechtsen (2007) states that the most effective way involves a user-involving approach by for example having information security workshops. Similarly, Jenkins (2012) argues for ***interactive learning*** where the employees, for example, get pop-up alerts that warn them when sending an email that has an unsafe attachment that can violate the organization's security policy. The author believes that the employees then become more cyber security conscious and learns to think once more before sending of the email. Mansfield-Devine (2017) highlights that when training the employees, organizations should not just tell the employees what to do but rather to focus on giving them real insight about the threat and learning them what to do about it. Approaches such as SMS messages, email updates, hackathons are all ways of getting the employees involved in the cyber security process (Caldwell, 2016).

An important part that several articles have highlighted is the importance of creating ***feedback channels*** in order to identify gaps in the training and processes (Bevilacqua, 2017; Blau, 2017; Caldwell, 2016; Mansfield-Devine, 2017; Upton & Creese, 2014). The article by Blau (2017) highlights that feedback should be built in to make sure the employees learn when they make a mistake and can avoid the misstep in the future. For example, organizations can send out fake phishing emails to the employees on a regular basis (Blau, 2017; Caldwell, 2016; Upton & Creese, 2014). Phishing attacks are according to Upton and Creese (2014) a way to trick employees of clicking a link in an email that downloads malware. These attacks are hard to detect and therefore to send out fake phishing emails occasionally can be a way to test if the employees have learned to detect phishing attacks (Blau, 2017; Caldwell, 2016; Upton & Creese, 2014). When relating this to the sensemaking literature, which also emphasizes that feedback is an important part, Balogun (2006) underlines that it is essential to also get an answer to why and not just get feedback on how the employee behaves. For leaders to develop an understanding of why, makes it possible for them to identify which behaviors should be encouraged and which should be changed (Balogun, 2006).

Alhogail and Mirza (2014) highlight that organizations should identify small wins and give ***rewards*** to acknowledge employees' efforts and contributions in the change process. According to the authors, rewards can be methods such as promotion, peer recognition and appreciation of good performance. Nevertheless, Mansfield-Devine (2017) mentions that there is a debate to be had whether an organization should reward employees for the right cyber security behavior or to punish them for unsafe behaviors. However, most of the findings in the literature claim that rewarding positive behavior is the right choice (Alhogail & Mirza, 2014; Bevilacqua, 2017; Caldwell, 2016; Lacey, 2010). This can be related to the strategic framework by Simons (1995) which is called levers of control. For instance, Sheehan (2006) explains that the framework involves a need for both boundary controls that shows which actions employees are not allowed to take, as well as diagnostic controls that rewards and motivates employees' achievements, in order for the organization to be successful (Sheehan, 2006). Hence, the most effective solution might be to reward the employees' positive behavior while at the same time ensure that there are boundaries in place that employees should not violate.

Several articles state that in order to reinforce and sustain a change, organizations should use ***effective measurements*** (Bevilacqua, 2017; Caldwell, 2016; Upton and Creese, 2014). The article by Caldwell (2016) underlines that it is important to perform effective measurements and assessment in order to make sure that the training has worked. However, the author mentions that it is all too often that organizations are using measurements that are activity-based that for example only shows how much percentage of the employees completed an e-learning module. The best measurement is output based where the actual employee cyber security behavior before and after the training is measured (Caldwell, 2016). In order to sustain the change organizations should make it to an ongoing process (Alhogail and Mirza, 2014; Blau, 2017; Caldwell, 2016; Everett, 2010; Jenkins, 2012; Mansfield-Devine, 2017). The article by Caldwell (2016) mentions that in order to change the behaviors of the employees, the training needs to be repeated at consistent and frequent intervals. Alhogail and Mirza (2014) highlight that new security risks appear every year and that it is therefore needed to conduct ***continuous efforts*** in order for an organization to be secure against any future potential cyber security incident.

2.4 Literature review's connection to the research questions

The literature review has provided valuable insights to fulfill the purpose of the study. First of all, the concept of cyber security is a term that in previous research has been used in different ways and situations. Thus, a discussion about the concept of cyber security and the closely related concepts have been provided in order to give the reader an understanding of the research area. Also, the explanation of the various concepts eases the answering of the research questions since it gives a clear view of what the study aims to investigate. Additionally, a discussion about relevant actions that organizations take when working towards improving the cyber security works as a basis towards answering the research questions since it helps to create a fundamental understanding of the research context. Furthermore, the literature review describes the concept of change management and discusses different views and theories of effective change management. This helps to answer the research questions since it provides knowledge of what key factors are required for effective change management and it also compares different views for how organizations should manage these factors.

The literature review combines change management practices with cyber security and views what previous literature has to say about change management in a cyber security context. Also, it integrates the different learnings of effective change management from the change management literature in order to get a comprehensive view of the research field. This helps to gain knowledge into answering the research questions since it discusses what previously has been done in the research area and gives an indication of important aspects to consider in order to fulfill the purpose of the study. Conclusively, the overall understanding that the literature provides for *how organizations can improve their cyber security with change management* serves as a foundation for the empirical data collection.

3. METHOD

This chapter covers the chosen methods that were used to fulfill the purpose of the study. The first section includes the research approach that was taken for the study and a discussion of the case selection and unit of analysis. Furthermore, a section presenting the data collection is provided. The method chapter then continues with a discussion of the data analysis. Lastly, the qualitative improvement measures that have been taken for the study are discussed.

3.1 Research approach

To fulfill the research purpose, a qualitative approach for the study was chosen. A qualitative research approach allows the research questions to be relatively open (David and Sutton, 2016), which prevents the study to be guided in a certain direction. Furthermore, an inductive approach was taken in this study in order to explore the data and develop theories from it (Saunders, Lewis & Thornhill, 2009). However, the study has been involving some deductive elements as well, in order to be able to use the existing theory to shape the results of the study (Saunders et al., 2009), which was used when developing the interview questions for the data collection. The research has been an iterative process since new learnings have appeared during the course which has provided valuable insights to improve the study further (Edmondson & McManus, 2007).

3.2 Case selection

The study was performed at a Scandinavian consultancy firm, which in this study will be referred to as Alpha, at the company's head office in Stockholm, Sweden. The organization is helping clients in various industries and have one specific part of the organization specialized in cyber security and another part specialized in change management. The study was conducted as a multiple case study with 6 participating organizations, including Alpha, in Sweden. An overview of the different organizations can be seen in Table 5. The organizations were chosen in order to get a wide spread of the data collection and therefore, various industries and types of organizations were

chosen. The organizations chosen were all in the client network of Alpha which the study was performed for.

Table 5. Overview of organizations that the participating respondents in the study were from.

Organization	***Industry***	***Type***	***Description***
Alpha	Consultancy	Private	A consultancy firm in Sweden with IT and management related projects.
Beta	IT	Independent	An independent non-profit Swedish institution in the IT industry.
Gamma	Energy	Private	An electricity network distributor in Sweden.
Delta	Transportation	Public	An organization providing public transport in a large city in Sweden.
Epsilon	Municipality	Public	A municipality in a large city in Sweden.
Zeta	Telecom	Private	A large telecom operator in Sweden.

In order to maximize the understanding of how organizations can improve cyber security with change management, a purposeful sampling method was chosen (Onwuegbuzie & Leech, 2007). With this sampling method, a wide range of organizations and respondents were purposively selected in order to get a multiple perspective of the research area.

3.3 Data collection

The empirical data was collected by performing interviews with respondents from six different organizations. Interviews were chosen as the main source of data because of the study's qualitative character (Onwuegbuzie & Leech, 2007). The various types of respondents were Chief Information Security Officers (CISOs) and consultants specialized in cyber security or change management, and other employees at the different case organizations. The respondents with roles of CISOs and consultants were chosen based on their long work experience in the area. The snowball sampling method was used to reach other employees in the case organizations (Onwuegbuzie & Leech, 2007). After interviewing the CISOs at the organizations they were recommending employees in their organization to interview.

The process for data collection was divided into three phases in order to get a comprehensive understanding of the research area. Phase *one* can be described as the exploratory phase where one unstructured interview with a security specialist and informal discussions with security consultants at Alpha were conducted to gain knowledge into the research field. Additionally, other types of data were also collected in this phase, for instance, documents, news articles and video lectures were provided by the supervisor at Alpha in order to achieve an understanding of the research problem and context. Also, during this phase additional literature research was made to refine the theoretical framework. In the *second* phase, which can be described as the in-depth phase, 16 semi-structured interviews were conducted with the targeted respondents at the different case companies. All of the interviews in this stage were recorded and transcribed in order to be able to analyze and find codes from the data set. The length of the interviews varied between 20-60 minutes and was performed face-to-face when possible. The *third* phase can be described as the confirmation phase, where one unstructured interview was performed to validate the findings from the second phase. The interview in this phase was not transcribed however notes were taken during the interview.

An overview of the semi-structured interviews conducted in the second phase of the interview process can be seen in Table 6.

Table 6. Overview of semi-structured interviews conducted in the second phase.

Respondent	***Position***	***Organization***	***Type of interview***	***Date***	***Duration***
R1	Change management consultant	Alpha	Face-to-face	2019-03-14	45 min
R2	CISO	Beta	Face-to-face	2019-03-18	60 min
R3	CISO	Gamma	Face-to-face	2019-03-19	30 min
R4	CISO	Delta	Face-to-face	2019-03-20	30 min
R5	Security consultant	Alpha	Face-to-face	2019-03-22	45 min
R6	Security consultant	Alpha	Skype	2019-03-22	30 min
R7	Security consultant	Alpha	Phone	2019-03-25	40 min
R8	Security consultant	Alpha	Face-to-face	2019-03-28	45 min
R9	Risk manager	Gamma	Phone	2019-04-09	20 min
R10	Group manager IT	Delta	Phone	2019-04-10	30 min
R11	CISO	Zeta	Phone	2019-04-11	30 min
R12	Division manager	Gamma	Phone	2019-04-12	20 min
R13	CISO	Epsilon	Phone	2019-04-12	30 min
R14	Risk manager	Zeta	Phone	2019-04-15	20 min
R15	Internal auditor	Delta	Phone	2019-04-15	20 min
R16	Division manager IT	Delta	Phone	2019-04-16	25 min

3.4 Data analysis

The analysis of the empirical data collection was performed through a thematic analysis. A thematic analysis was chosen since it according to Braun and Clarke (2006) is beneficial when summarizing key features from a large amount of data. Also, it is according to the author a preferable method when aiming to find similarities and differences in the data set and to capture the psychological and social interpretations of the data. The thematic analysis was performed in six steps, adapted from Braun and Clarke (2006):

1) Familiarize with data
2) Generate initial codes
3) Search for themes
4) Review themes
5) Define and name themes
6) Produce the report

First, the analysis started by familiarizing with the data which involved transcribing the collected data and writing down the initial ideas that appeared when studying the transcribed interviews. Secondly, the initial codes were created by taking every segment of the data set and converting these to various codes. The aim was to create as many potential codes as possible in order to not exclude any code right away that might appear to be of high relevance to the analysis later on. The initial coding was done digitally, by marking each part in the documents and moving it to another text document where the data extract received a headline based on a code name.

In the third step, the themes were generated. This was done by sorting the different codes into clusters that were related to each other. The clustering was done by color marking each of the codes that were similar and gathering these in the same color category. After creating these initial themes, step four involved reviewing these themes in order to combine some of the themes that were similar and removing those that not had sufficient data to support them. The remaining themes were then named and defined by considering what each theme involve and what aspects it captures. Step three to five involved an iterative process in order for the themes to be refined and clearly defined before starting step six, producing the report. In the last step, the result chapter was produced and sorted based on the final themes. The themes were discussed and analyzed, and a final thematic map involving the themes and codes is presented in order to provide an outline of the findings. Also, representative quotes for each code were summarized under each theme. These quotes were extracted from the transcribed interviews and translated from Swedish to English.

3.5 Quality improvement measures

To ensure high quality and trustworthiness of the study, there are some quality improvement measures that were taken into consideration throughout the research process. The study was evaluated by using the four measures called, *credibility*, *transferability*, *dependability*, and *confirmability* (Lincoln & Guba, 1985).

To achieve ***credibility*** of the study, i.e. to ensure that the study tests or measures what is really intended (Shenton, 2004), triangulation was performed by collecting data from a wide range of informants with contrasting perspectives in order to be able to verify and compare the different viewpoints to each other. In addition, credibility was achieved by frequent feedback and debriefing sessions with supervisors and opponents. Also, well-established research methods were used in the study to ensure high credibility of the research process. For example, the thematic analysis used to analyze the collected data is a widely used method for analysis in qualitative studies (Braun & Clarke, 2006). The second criteria, ***transferability***, i.e. the extent to which the findings can be applied to other situations (Shenton, 2004), was achieved by providing background information of the different case organizations and interviews. For example, the number of participants and the length of interviews are presented in Table 5 and Table 6 in order to ensure transferability. To achieve the third measure, ***dependability***, i.e. to use techniques to show that similar results would be obtained if the research was repeated in the same context and by using the same research methods (Shenton, 2004), a detailed description of the research process was provided by explaining step by step how the data collection and analysis was performed. The last criteria, ***confirmability***, i.e. the qualitative researcher's objectivity in the study (Shenton, 2004), was ensured through triangulation in order to reduce the influence of investigator bias where the result reflects the researchers own thoughts and ideas instead of the informants.

4. ANALYSIS AND FINDINGS

This chapter presents and analyzes the findings from the collected data. It is divided into two sections, the first one answers RQ1 by providing the key factors for effective change management in the context of cyber security, and the second section answers RQ2 by analyzing the relation between all the essential factors and providing a framework for how organizations can manage these factors to improve cyber security.

4.1 Key factors for effective change management in the context of cyber security

From the analysis, a thematic map was created with the identified codes and themes, see Figure 1. The themes have been identified as key factors to consider for effective change management in a cyber security context and each theme will be discussed in the following sections.

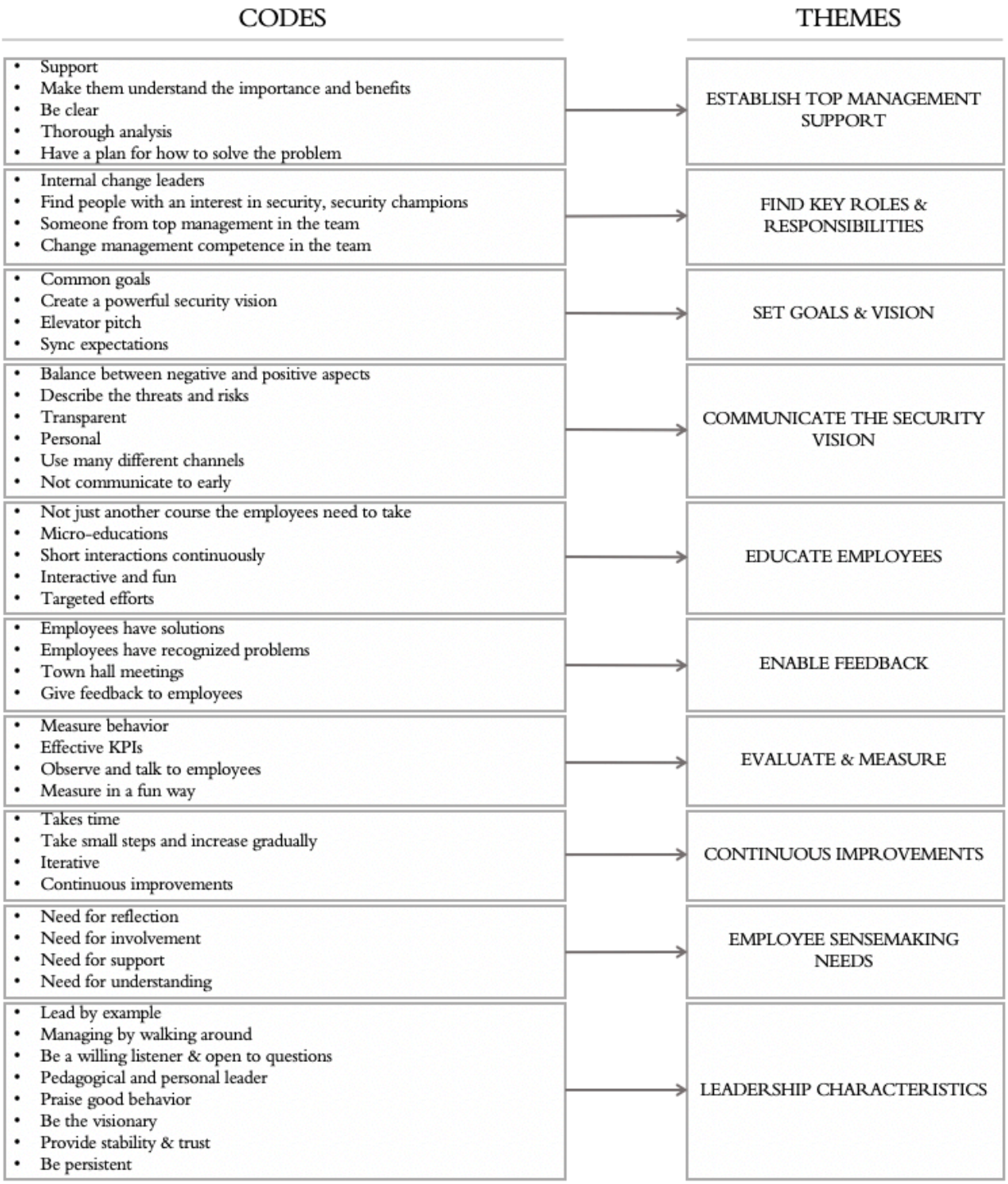

Figure 1. Thematic map

4.1.1 Establish top management support

The theme 'Establish top management support' highlights that it is essential with support from top management and discusses how to establish support and engagement from the top management. Table 7 summarizes the findings for this theme.

Table 7. Representative quotes for the theme 'Establish top management support'

Resp.	***Representative quotes***	***Code***
R1	*I think the biggest challenges are somewhere to bring along the top management, that is where it starts*	Support
R7	*What I think is most important is that you get the top management to understand what security is, that you usually have to start from the top and get a buy-in from the management*	
R4	*It starts with the top, that is where I put the most effort*	
R7	*That you actually can make money from it, many are still seeing it as an unnecessary hurt, as a fire insurance that one must have because everyone else has it, that one has not understood and no one has been sufficiently clear and explained the benefits with, it is only seen as a cost*	Make them understand the importance and benefits
R7	*Explain in such a simple way that they understand these questions and that they then understand them so they feel that they dare to tackle them, otherwise it will just be a directive or that others do this, and it is quite easy, and then you do not go through a change at all except on the paper*	Be clear
R3	*You create another type of credibility with the top management if you have done an analysis and go and present the analysis and say that we have these business branches, we have these protection values within the organization that we must protect, and we can explain why they are important*	Thorough analysis
R13	*We cannot just go out and present that we have a problem, we must also be able to present the solution to it, so then I have to develop the solution first how is this meant to be handled*	Have a plan for how to solve the problem

Top management plays an important role in the organization's cyber security since it is with the top management that it all starts, and they are the ones that provide resources and decides how much the organization should invest in cyber security. Establishing top management ***support*** is something that the respondents have expressed as one of the biggest challenges as well as the most important aspect when working with security. It is essential that the top management understand the ***importance and benefits*** of working with security and engage in the organization's security initiatives. Hence, in order to effectively being able to sell in all the good effects of working with cyber security and create an awareness and support from top management, the respondents have expressed some key aspects that should be considered. First, it is important to ***be clear*** and communicate with the top management on a level that they understand. As one respondent explains:

> *"The important thing is to connect these questions to something that is concrete ... if you are doing a lot of jargon and talk about as ehh they got in through a vishing attack and like that, then there is no one in a management group who will understand or be interested of these issues"* - R4

It is therefore important to speak in terms of how it affects the business and how it damages the organization's goals rather than using cyber security terms that require some fundamental knowledge of the area. Another essential aspect expressed by respondents is the importance of a ***thorough analysis*** that can convince the top management about the importance of cyber security. For instance, respondent 3 explained that if you have done a thorough analysis that can prove why it is needed and also ***have a plan and solution*** of the problem, then it shows reliability which will help them understand the importance of investing in cyber security.

4.1.2 Find key roles & responsibilities

The theme 'Find key roles & responsibilities' includes what roles and responsibilities are needed for effective change management in a cyber security context. Table 8 presents the codes and their representative quotes for this theme.

Table 8. Representative quotes for the theme 'Find key roles & responsibilities'

Resp.	***Representative quotes***	***Code***
R1	*We want to create internal change leaders … a way to create internal change leaders is to involve key people early in the project as, for example, the project group, start to identify ambassadors in the organization that could take different streams*	Internal change leaders
R5	*In this secure development world, you talk about security champion, like someone that is a bit interested in security, you create some kind of virtual forum to train them and then maybe you meet some day every month and talk security and then that person becomes the representative in the group or team for security*	Find people with an interest in security, security champions
R1	*It is not uncommon for the steering committee to consist of just members from the top management, because we really get them to understand: what are we doing? And why should we do what we do? And what effects does it bring?*	Someone from top management in the team
R11	*I just got one in my team, a program manager who is also a specialist in change management*	Change management competence in the team

To achieve a successful change in the organization's cyber security culture, it is essential to create key roles and responsibilities, and as some respondents called it, security champions. It is important to find people in the organization that can help to lead this journey forward especially if it is a large organization, since then there need to be people in each division that can help communicate and lead the change. This should be done by finding the people in the organization with an interest in security and train these into

becoming ***internal change leaders*** and responsible for cyber security in each division. These do necessarily not have to be the ones with most knowledge or power, but someone that has the ***interest*** to learn more about security. As one respondent described:

> *"If you can find someone who thinks these are interesting questions and also are skilled in the organization then it is better than shaking out information security representatives and forcing them into the organization and train them"* – R4

The respondents believe that it will not be successful if you force someone to be responsible for the security, for instance, if the security champion is not excited about communicating security to the other employees then it will reflect towards the employees as well. Another aspect that is highlighted as effective, is to include a member of the ***top management in the team*** leading the change effort. If someone from the top management is included in the change initiative, it increases the understanding of cyber security at the top management and it also reflects onto the employees how essential cyber security is for the organization. Moreover, if possible, the team leading the security change effort should include someone with experiences and ***knowledge of change management***. Respondent 11 mentioned that they had included a specialist in change management in their team that could help lead the cyber security culture change effort. This could be an effective way of making sure that there is change management competence inside the team.

4.1.3 Set goals & vision

The theme 'Set goals & vision' underlines the importance of forming security goals and vision to achieve effective organizational change. In Table 9 below are the codes and representative quotes for this theme presented.

Table 9. Representative quotes for the theme 'Set goals & vision'

Resp.	***Representative quotes***	***Code***
R3	*We have a number of stated goals in the business plan to reduce the number of incidents*	Common goals
R7	*One has to find something in common that is strong enough to make people move*	Create a powerful security vision
R1	*We stop with some kind of workshop on the purpose description and there they get to practice on a type of elevator pitch so that you really own it*	Elevator pitch
R1	*Change takes time, if you want to do it for real then it takes time, so here we need to sync expectations*	Sync expectations

From the interviews, there is no doubt that creating goals and vision is an essential aspect to consider. It essential to set up goals and visions that are aligned with the organizations overall vision. Organizations should create short-term goals during the change process but also overall ***goals that are common*** for the whole organization. Also, the whole organization should be striving for the same security vision. In the words of one respondent:

> *"One has not spent time and resources on the actual strategic work and how to get together the security work with the organization's overall goals and vision … much is about understanding and finding common goals and ideas"* – R7

The respondents underline that organizations should create a ***powerful security vision*** that is convincible. The vision should be created in the way that it can be communicated clearly by everyone leading the change effort. It is essential that even the top management know the vision and are able to describe it. Hence, this could require some workshops around the vision where they can practice an ***elevator pitch***, to be able to easily tell the security vision whenever encountering an employee. When forming the vision, it is essential to ***sync everyone's expectations***. This change is not something that can be done in a rush, everyone needs to be aware of that creating a cyber security culture change will take time in order to be done thoroughly.

4.1.4 Communicate the security vision

The theme 'Communicate the security vision' describes how to communicate the security vision towards the people in the organization. Table 10 summarizes the main findings for this theme.

Table 10. Representative quotes for the theme 'Communicate the security vision'

Resp.	***Representative quotes***	***Code***
R7	*To just highlight positive and these bits, you miss a great deal and then you do not get the right understanding and people feel misled and many get tired of it, and if you only bring out consequences and are negative then it is harder to motivate people, so you have to have both*	Balance between positive & negative aspects
R3	*We try to describe the threats as well as incidents that occurred both internally in the organization and externally to motivate actions*	Describe the threats and risks
R8	*Consciously raise the risks of information you are sitting on and to do it in a way that does not mean that the employee thinks it is a hassle to live up to what you want to introduce*	
R7	*It should be transparent and clear, you should not hide anything, you should open your cards and just be honest and show how it is without distorting anything*	Transparent
R9	*That they get feedback to their everyday life … for example if you take other types of organizations, then it will not really be as down to earth for them*	Personal
R4	*Differentiated delivery methods, to sit like a half day or something and learn about information security, yes it may work the first time but then it is not reasonable, people do not have the time and desire ... so to use as many different ways as possible*	Use many different channels
R1	*To not go out and communicate externally too early because it is not always the case that it gets as one said to be communicated and then it just gets the other way, it has the opposite effect*	Not communicate too early

When it comes to communicating the security vision towards the people in the organization, there are some aspects that the interviews have emphasized to be essential in order for the communication to be effective. First, when communicating it is important to ***balance the positive and negative aspects*** of security. The threats are an effective way to make the employees understand that cyber security is serious, and they understand why this is needed. However, to just talk about ***threats and incidents*** will not be effective since the employees can feel scared or receive a negative view of security. As respondent 1 highlighted, this is only extrinsic motivation for employees, which means that they do it since they are asked to do it and that they feel that they can lose their job if they do not do this, and this only creates short-term wins. To make a lasting change in the employees' security behavior you need to focus on capture the employees' inner (intrinsic) motivation instead. The controls are important as a basis, but you need to communicate the positive aspects of the change by highlighting success stories and talk in terms of what can be positive about the change for the employees. Therefore, a balance between the negative and positive aspects of cyber security is believed to be the most effective. Positive aspects can, for instance, be success stories and competitive advantages,

and negative aspects such as the potential risks and threats. This is something that the literature also discussed, for instance, Kraft et al. (2018) mentioned that there needs to be a balance between the negative and positive aspects of the change for a change initiative to be successful. A quote from respondent 7 summarizes this well:

> *"To just highlight positive and these bits, you miss a great deal and then you do not get the right understanding and people feel misled and many get tired of it, and if you only bring out consequences and are negative then it is harder to motivate people, so you have to have both"* – R7

Another essential part concerning communication is ***transparency***. In order for employees to achieve an understanding of why cyber security is important, organizations should not try to hide internal incidents or threats. It is important to tell the employees about incidents that were happening or almost happening in their organization since it makes the employees feel more involved and they understand why there needs to be a change. This is according to the respondents a difficult thing to live up to when it comes to cyber security since top management are usually afraid of incidents getting leaked to the press. However, this is a risk that should be taken since the employees will not feel involved and understand if they not get informed about what is happening in their organization. As one respondent expressed:

> *"That you dare to talk about things that have really happened to ourselves that were not so great because people have much easier to grasp why it is important ... so transparency about what has happened and that it was not good, and what we do because it should not happen again"* - R5

Another aspect concerning communication is to make it ***personal*** and relatable for the employees, this goes in line with transparent communication, that it is effective to talk about things that have happened or almost happened inside their organization, rather than something happening to an external organization. If they get an understanding of what is in it for them personally, they can have it easier to understand why this needs to be done and why this is important. Furthermore, it is according to the respondents effective to ***use many different channels*** to get the security message out there. This could, for instance, be intranets, tv-screens, and newsletters, in order for the employees to receive regular information of security that can make the employees pay attention and

become more aware of cyber security. In order for the communication to be successful, it is essential to ***not start communicating too early***. The respondents expressed that there needs to be support for the employees before they receive information about the change. They need to know whom to turn to with questions and concerns, otherwise the employees might feel confused or insecure about what is happening which can have a negative effect on the communication.

4.1.5 Educate employees

The theme 'Educate employees' includes how to educate the employees in the organization and enhance their understanding of cyber security. Table 11 presents the representative quotes for each code.

Table 11. Representative quotes for the theme 'Educate employees'

Resp.	***Representative quotes***	***Code***
R4	*A university course in information security 101, it was like this is how information security works, but the problem is that yes for some people who are interested and find it fun to learn more, they will think yes how fun and exciting, but for most others it is just another education they need to take*	Not just another course the employees need to take
R14	*I think that you raise awareness quite well with these short small parts, and because you can make them shorter in various topics and of what is most relevant right now so you can focus on that*	Micro-educations
R5	*Micro-awareness training, I think this was a pretty good idea ... everyone has such a short attention span, it is so short nowadays so maybe it is micro-mails that is the way to convey awareness*	
R4	*short interactions involved in other programs based on how the tasks look for these target groups*	Short interactions continuously
R10	*At all security workshops that are made is it the employees who sit and classifies*	Interactive and fun
R2	*We do not have any one-size-fits-all education, it is more targeted efforts*	Targeted efforts
R3	*Now we start to add some targeted education to different target groups*	

Educating the people in the organization to enhance the knowledge and awareness of cyber security is an essential part and is what several respondents expressed as the key factor for changing the employees' cyber security behavior. In order for the education to be effective, respondents highlight the importance of ***not making it to just another course*** that employees need to take. The respondents believe that the traditional way of having a long lecture may be effective the first time introducing the employee to security, however, to really make a lasting change in employees security behavior the most effective way is ***micro-educations*** that enables ***short interactions*** frequently. This can be

done in different ways and channels and the respondents believe that making it ***fun and interactive*** is an effective way of educating the employees. This can, for instance, be as one respondent mentioned, gamification-educations, where the employees can compete against each other in a fun and interactive way to learn about cyber security. In the words of respondent 4.

> *"Short interactive gamification courses, like that kind of parts, printed material, or information campaigns on the TV screens that sit a little here and there or short lectures, we have these breakfast seminars sometimes"* – R4

Furthermore, making ***targeted efforts*** where the education material is tailored for a specific target group in the organization is a key aspect to consider when educating the people in the organization in order to make sure that all roles get the knowledge they need.

4.1.6 Enable feedback

The theme 'Enable feedback' highlights the importance of giving and receiving feedback. Table 12 provides an overview of the findings for this theme.

Table 12. Representative quotes for the theme 'Enable feedback'

Resp.	***Representative quotes***	***Code***
R13	*Many of the employees are sitting on a lot of good ideas and solutions for how to solve the security problems we have… so there is a risk that we believe that it is only we in the information security area who are experts on this and that we should come up with all the solutions*	Employees have solutions
R10	*I really believe it mostly been us employees that based on the environment for example the transport department which has suffered, then you have like: shit, we deal with the same type of information and does not make it better at all*	Employees have recognized problems
R11	*We are going to have some occasions, simply public meetings, where we sit and then get the people to come and talk directly with us and make suggestions and stuff*	Town hall meetings
R1	*Reinforce progress for each individual, yes but fantastic now I saw that you have made three deviation reports here against previous zero*	Give feedback to employees

Creating feedback channels that make it easy for employees to give suggestions and provide solutions, is an essential activity to enhance the employees' security behavior. One respondent mentioned that it is important to not think that it is only themselves in the security division that are the experts in the organization, the employees know their area well and might have great ***solutions*** for how the security could be improved in that area. As one employee mentioned:

"I really believe it mostly been us employees that based on the environment for example the transport department which has suffered, then you have like: shit, we deal with the same type of information and does not make it better at all" – R10

The employees created the awareness, they ***realized*** that something needed to be done made the top management aware of the problem and realized that resources were needed to solve the security issue. Thus, with feedback from employees, the solutions to security related problems can be provided and the employees will feel more involved in cyber security. Hence, the organization should have feedback channels in place in order for the change to be effective. Respondent 11 mentioned that in their organization one way to receive feedback were ***town hall meetings***, where the people involved in the project could sit and everyone could come and give feedback and talk to them about anything concerning security. Furthermore, the employees do also need to receive feedback in order for them to change and improve their cyber security behavior. Hence, it is essential to ***provide the employees with feedback*** on how they are performing and behaving in order for them to reflect their own part of the change.

4.1.7 Evaluate & measure

The theme 'Evaluate & measure' underlines the importance of effective measurements and to evaluate the results of the change initiative. An overview of the findings for this theme can be seen in Table 13.

Table 13. Representative quotes for the theme 'Evaluate & measure'

Resp.	***Representative quotes***	***Code***
R2	*This year I will do what to call it an attitude measurement, there is a company that has developed a model for benchmarking of the security culture*	Measure behavior
R3	*Advantages of doing the education per business area is that you can measure and set up key figures in a different way than just having the quantitative and see that a number of employees have taken to the education*	Effective KPIs
R1	*You need to find some different tools to start quantifying the journey itself and in order to do so you need to set up important key figures in the form of KPIs*	
R7	*It is about the fact that when creating measurement numbers, what is the actual effect here*	
R2	*Walk around and ask how much they know and can*	Observe and talk to employees
R3	*Me and a couple of my colleagues usually go around and look at this without saying anything but observe how it has affected*	
R1	*We usually go on a group level, what is the sense, again in the project team, ear-to-rails behavior of those who are leaders and ambassadors, how is the talking out there, so in that way are we sniffing in pretty much*	
R2	*I have tried to make it a bit fun to answer questions where I have omitted, for example, the safety manual speaks about the minimum length of our passwords it is… so point point, you can fill in there*	Measure in a fun way

A key factor to create a cyber security culture is to evaluate the result of the effort. This means that effective measurements need to be put in place. As realized from the interviews, this is something that the case organizations have not come far with and needs to be improved more. To perform effective measurements, it is essential to ***measure the change in behavior*** before and after the change. In the words of one respondent:

> *"We want to change a behavior not the actual thing, we want to change a behavior, that they should think in a different way"* – R13

As another respondent expressed, when they come to you to ask questions and shows interest in these questions that is a good indicator of a successful effort, since then it starts becoming a part of the security culture. Also, to ***set up KPIs*** that quantifies the journey is an effective way of evaluating the results of the initiative. When it comes to measuring the success of the education, a fact-based questionnaire might be useful right after but to really evaluate and measure the result of the change effort, it is essential to measure the effect, to measure the change in employees' behavior. This can be done in several ways, for instance, to be present and ***observe and talk to the employees*** on a group level, you can receive a good idea of the effect. Additionally, it is good the measure the behavior by asking questions which finds out of if they understand why they need to behave

securely for instance why they need to change passwords. When measuring the behavior, it is preferable to try to make it ***in a fun and engaging way***, so it is not only a standard questionnaire that the employees need to do. One respondent highlighted that in their organization they were trying to make the tests in a fun way, which for example could be to fill in the missing pieces in a statement.

4.1.8 Continuous improvements

The theme 'Continuous improvements' describes the cyber security change process and highlights what efforts are needed to sustain the change. Table 14 presents the representative quotes for each code of the theme.

Table 14. Representative quotes for the theme 'Continuous improvements'

Resp.	***Representative quotes***	***Code***
R13	*It takes time to change an organization, to change a behavior in the organization*	Takes time
R2	*It is a long-term work that needs dedicated resources, is not something you do with your left hand, it is really something that is a long-term work*	
R1	*Another thing that is very important is that change takes time, if you want to do it for real it takes time*	
R13	*You need to walk around in that circle and build the spiral outwards in a controlled manner so that you do not create panic in the organization*	Take small steps and increase gradually
R2	*It should fall naturally into the job that you have every day, so we have cut this elephant into appetizing pieces*	
R10	*You might start gradually and expand, instead of starting with everything at once*	
R1	*Key factors associated with when it actually goes well is when you dare to be a little bit iterative, that you dare to change a bit throughout the process*	Iterative
R2	*It builds a lot on continuous improvements, you can always be a little little bit better*	Continuous improvements

An aspect that the respondents have emphasized clearly, is that this change ***takes time***. In order for organizations to improve their cyber security with change management, their organizational culture needs to be changed and become integrated with cyber security. Cyber security is not only another project, it should be integrated into the organization's culture. The result of the change effort should be a cyber security culture where all people in the organization have a security thinking and security falls in naturally in all employees' everyday work. Moreover, to create this cyber security culture change, the respondents highlight that it is essential to ***take small steps*** and build a little at a time. It is better to start small and then continue with improvements continuously. Additionally, it is

important to remember that change takes time. It is an ***iterative*** process that requires ***continuous improvements*** to really create a successful cyber security culture and sustain the change into the employees' cyber security behavior. As one respondent emphasized:

"It builds a lot on continuous improvements, you can always be a little little bit better" – R2

This aspect goes in line with the existing literature and Alhogail and Mirza (2014) highlighted a worthy argument for why this is an important aspect. The authors underline that new security risks appear every year and that it is therefore needed to conduct continuous efforts in order for an organization to be secure against any future potential cyber security incident.

4.1.9 Employee sensemaking needs

To create a lasting change in the employees' behavior and make them more security conscious, it is essential to understand how the employees make sense of the change. Therefore, from the interviews, the following employee sensemaking needs were identified, see Table 15.

Table 15. Representative quotes for the theme 'Employee sensemaking needs'

Resp.	***Representative quotes***	***Code***
R13	*The employees should have the time and opportunity to actually also engage in information security issues … if you are doing your other tasks at 100% when will you have time to take care of this? When will you have time to stop and reflect?*	Need for reflection
R7	*That you actually listen to the input and take care of it so that people feel like they are involved*	Need for involvement
R13	*An important part when you develop the controls, when you produce material and so on, to not ignore the employees, but to actually involve them much earlier*	
R14	*Even if they have no idea, that they at least know where to go to get help*	Need for support
R13	*We cannot just educate them and scare them and say this is how you should do, and then there is no support behind it all, we have to make sure there is support first*	
R12	*To create an awareness that you should understand why you need to do something*	Need for understanding

Need for reflection. It is essential to give the employees time to evaluate their own part, everything they have learned about security, and the feedback they have received. If they

do not get time to evaluate what they have learned and what it means for them, it is hard for them to change behavior because it can be difficult to grasp and easily be forgotten. One respondent described this aspect well:

> *"The employees should have the time and opportunity to actually also engage in information security issues ... if you are doing your other tasks at 100% when will you have time to take care of this? When will you have time to stop and reflect?"* – R13

To fulfill this need, the key factors *communicate the security vision*, *educate employees*, and *enable feedback*, are essential for organizations to consider. The employees need to have the time to reflect what they have been informed of and educated in when it comes to cyber security. Also, to provide the employees with feedback where the employees have the opportunity to reflect how well they have done and how they can improve will help them fulfill their sensemaking need for reflection.

Need for involvement. Employees have a need to feel involved in order for them to be positive towards security. Even if one respondent highlighted that it is important to remember that every employee does not want to be actively involved, yet, even if they do not want to be actively engaged in the organization's cyber security efforts, they want to feel like a part of it and have a feeling of involvement. Therefore, to fulfill this need, it is essential as a leader to listen, ask them, get suggestions and feedback from the employees and actually take the employees thoughts and experiences into consideration. Also, to find the people in the organization that can have key roles and responsibilities in the organization's cyber security efforts, the employees that have an interest in cyber security can get involved and hence fulfill their sensemaking need for involvement.

Need for support. It is important that the employees know whom to turn to, to get help and ask questions. It should be easy to be able to ask any questions and therefore, there needs to be available support established since the employees will just continue in the same pattern if they do not get the answer to questions they have. As one respondent stated:

> *"Even if they have no idea, that they at least know where to go to get help"* – R14

This sensemaking need relates to the key factors, *communicate the security vision* and *educate employees*. The employees need support when they get information and education about cybersecurity in order for them to fully understand and feel motivated to change.

Need for understanding. The employees understanding and knowledge about cyber security are lacking and therefore there is resistance towards the change. They need to understand why this is happening and also to understand what to do and have the knowledge to do the right thing. Hence, this is where clear communication and education serve as fundamental aspects to handle this need. Also, when creating the security vision, it is essential to consider that all employees need to understand the vision.

4.1.10 Leadership characteristics

One critical aspect in order to change the organization's cyber security culture is to have effective leaders that lead the change effort. Based on the interviews with the respondents, some essential leadership characteristics are identified, see Table 16.

Table 16. Representative quotes for the theme 'Leadership characteristics'

Resp.	***Representative quotes***	***Code***
R13	*It is important that the top management not only say this but that they actually also lead by example … even them in their priorities and that they prioritize in the same way as they want their employees to prioritize, because if it shows that the top management chooses to prioritize financial issues ahead of quality- and information security questions, then the employees will do the same*	Lead by example
R2	*I am very much security and managing by walking around, so you go around the office all the time and talk to people and make sure you are present*	Managing by walking around
R1	*To come to a group and say now you should do completely differently, without creating room for dialogue where they get put words of their fears and maybe also hopes, then you miss what the group actually possess*	Be a willing listener & open to questions
R8	*Some kind of responsiveness from the security side regarding the implementation phase*	
R1	*We also talk about personal leadership, leaders are important in such a way that they need somehow to enhance the progress for each individual*	Pedagogical & personal
R2	*Try to strengthen in their self-esteem and in their professional role, that you can do this, you know how to do it, and you do not have to worry that something should go wrong*	
R1	*Fantastic, now I saw that you did three deviation reports here against the previous zero, to just reinforce these behaviors when going in the right direction*	Praise good behavior
R7	*Find something in common that is strong enough to make people change*	Be the visionary
R1	*Be able to sell in 30 seconds why we do what we are doing and what effects it will lead to, and why others should join in*	
R2	*I have worked so long with these questions and I am extremely much out and talking, last year I believe I had around 75 presentations over the year and I believe that it reflects on to my authority internally*	Provide stability & trust
R12	*To work with information security, it is not just a project, it is something that must be implemented in everything, so it is important to think about persistence there*	Be persistent

First, a leader should ***lead by example*** and this does not only refer to the people leading the security initiative, this is also something concerning the very top management. The top management's attitude toward security will reflect the entire organization's priorities. In the words of one respondent:

> *"I believe that the best example is parenting, if you want your child to do different, you say do not eat candy on Tuesday and Wednesday and then you sit and just gormandize chips and candy right in front of them, they will not buy it"* – R1

This leadership characteristic is strongly related to the key factors, *establish top management support* and *find key roles & responsibilities*. It is the top management and the key people involved in the change that needs to lead by example in order for the employees to feel motivated to follow the cyber security initiatives. Another leadership

characteristic that has been identified as essential is to ***manage by walking around***. This requires that the leader is present and observe and talk to the employees in the organization. The respondents highlighted that there needs to be a leader that interacts with employees and that is present and visible. This relates to the key factors, *communicate the security vision*, *enable feedback*, and *evaluate & measure*. A leader should walk around and talk to employees when communicating the security vision and receiving suggestions and feedback from employees. Also, it is essential to observe and talk to the people in the organization to measure and evaluate how well the employees have responded to the change. Furthermore, it is essential that a leader has good listening skills and is ***open to the employees' questions***. Every employee should be able to feel like they can ask any question and not be afraid that any question might be too stupid to ask. Just like one respondent expressed:

> *"When they dare to ask questions is a good sign that they understand, that they have some kind of trust for you and dare to ask questions, and it is a bit of how you represent security, that you are truly open to receive questions and that no questions are stupid questions"* – R5

This is essential when communicating and receiving and giving feedback to the employees. Furthermore, to create a successful cyber security culture, the respondents highlighted that a leader needs to be ***pedagogical and personal*** towards the people in the organization**.** The respondents expressed that in order for the employees to respond well to the change, a leader needs to be pedagogical and strengthen the employees' inner motivation. This is essential when educating the employees and communicating towards the employees. Additionally, it is important to ***praise good cyber security behavior*** and acknowledge and encourage the employees when they do something well for the organization's cyber security. This can be done when measuring and evaluating the results of the change effort when noticing that an employee has improved their cyber security behavior to acknowledge and praise them for it. Furthermore, the respondents highlight that a leader needs to ***be the visionary*** and be able to sell in the vision to everyone in the organization and make the employees committed and believe in the security efforts. To achieve this, a leader should try to reach out to everyone and create a vision that the employees can relate to and that is strong enough for everyone to receive an ambition to

change. Also, it is essential that the key people involved in the effort can be the visionary and deliver the security vision towards the employees in the organization.

Another identified leadership characteristic is to ***provide stability and trust***. For a leader to be able to provide stability and trust it is essential to have a knowledge and understanding of cyber security and a well-thought-out plan for the process, in order for the employees to be calm and trust that the change effort will be successful. One respondent mentioned that the reason they had a good cyber security culture was that as a leader she had great experience and knowledge in the area which made the employees respect and trust her in the cyber security effort. Moreover, this leadership characteristic is important when communicating the security vision and educating the employees about cyber security. Lastly, it is essential that a leader can ***be persistent*** when working with security change management. As the respondents have highlighted, it is a long-term process that builds on continuous improvements. Therefore, to be aware of that change does not happen right away and that it requires continuous efforts, is an important aspect for successful cyber security culture change.

4.1.11 Relations between the different key factors

Based on the findings, it is clear that the leadership characteristics and employee sensemaking needs strongly correlates with the other key factors. Hence, to illustrate the relation between the different key aspects, and show specifically which leadership and employee sensemaking need that should be considered for each factor, a spreadsheet is presented, see Figure 2. This provides an understanding of how the different factors relate to each other.

		Main activities							
		Establish top management support	Find key roles & responsibilities	Set goals & vision	Communicate the security vision	Educate employees	Enable feedback	Evaluate & measure	Continuous improvements
Employee sensemaking needs	Need for reflection				X	X	X		
	Need for involvement		X				X		
	Need for support				X	X			
	Need for understanding			X	X	X			
Leadership characteristics	Lead by example	X	X						
	Be the visionary		X	X					
	Managing by walking around				X		X	X	
	Be a willing listener & open to questions				X		X		
	Pedagogical & personal				X	X			
	Praise good behavior							X	
	Provide stability & trust				X	X			
	Be persistent								X

Figure 2. Spreadsheet of how the key factors relate to each other

4.2 An emerging framework for successful cyber security culture change

Emerging from the analysis is a framework that provides a visualization of the empirical findings, see Figure 3. The framework shows the relation between the findings and visualizes the process of how it should be managed to create a successful cyber security culture change. The process is divided into three phases, *prepare for change*, *change*, and *sustain change*. Also, the framework highlights each essential activity and shows when and how they should be performed, when to consider each leadership characteristic, and what employee sensemaking needs that should be considered during the process. The circular arrow in the end illustrates the iterative and continuous process that is required in order to sustain the change in the organization's cyber security culture.

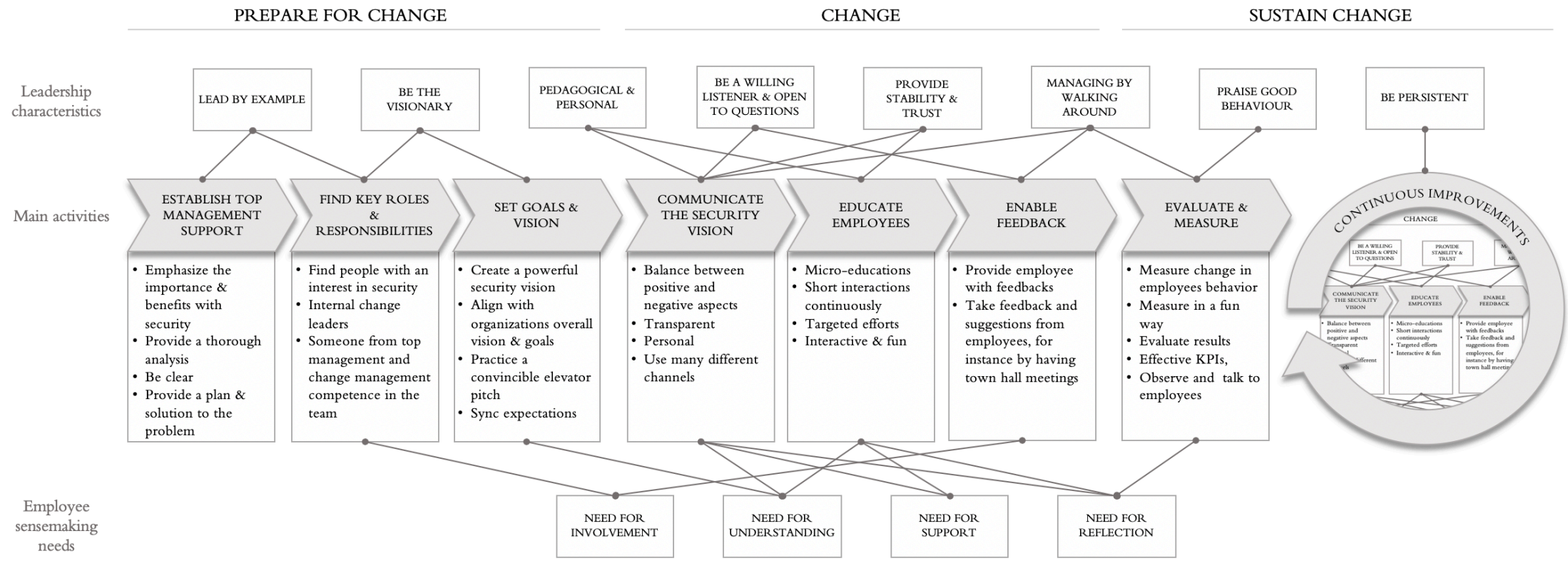

Figure 3. A framework for successful cyber security culture change

5. DISCUSSION AND CONCLUSION

This study has contributed with a broader understanding of how organizations can improve their cyber security with change management, by providing a framework that illustrates the key factors for effective change management in a cyber security context and how these factors should be managed. Since the threats of cyberattacks are a higher concern than ever before (Poppensieker & Riemenschnitter, 2018; Ransbotham, 2017; Syed, Padmanabhan, & Dixon, 2014; Jalali, 2018; PwC, 2017), and the reason for cyber security initiatives to be unsuccessful is the lack of focus on the human aspect (Lacey, 2010; Orshesky, 2003; Pfleeger & Caputo, 2012; Stewart & Jürjens, 2017), it is clear that change management plays an important role for organizations when aspiring to achieve successful cyber security. Hence, this study contributes with essential insights to the literature of cyber security and change management, as well as practical implications for managers and consultants working in various industries with cyber security.

5.1 Theoretical contributions

The results of this study contribute to existing theories and research in several ways. First, in the cyber security literature, several scholars have highlighted key factors for how to use change management to improve cyber security (e.g. Caldwell, 2016; Limba et al. 2017). The results from this study add empirical insights on what key factors should be considered for effective change management in a cyber security context and also shows how these identified factors should be managed. Hence, the study adds with an extra dimension to how to manage organizational cyber security change by providing a processual model that illustrates the factors dependency of each other.

Secondly, the cyber security literature that focuses on change management is scarce, and not enough focus has been on the human aspects of cyber security (Lacey, 2010; Orshesky, 2003; Pfleeger & Caputo, 2012; Stewart & Jürjens, 2017). This study contributes to the cyber security literature by enhancing the understanding of how change management can be used in a cyber security context. Also, by adding the perspective of sensemaking, the study provides an overall picture, with both a leader and

employee perspective, of how change management can be used to improve cyber security.

Lastly, the result of this study extends earlier change management literature by providing a sensemaking approach to the change process. Similar to current change management models (e.g. Kotter's & Lewin's models), the result of this study goes in line with existing theories of change management, however, these models are not including the employee sensemaking perspective. For instance, the model by Kotter consists of eight steps for leading organizational change (Kotter, 2007), but these steps do not provide an understanding of how the employees make sense of the change and how a leader should handle these needs. Moreover, the results of this study highlight that both a leader and employee perspective need to be taken for effective change management. Therefore, the framework from this research provides an extra dimension towards change management by contributing with both a top-down and bottom-up perspective on change management.

5.2 Practical implications

The study contributes with valuable insights for management in practice. Since most change efforts fail (Burnes, 2011), and organizations are struggling with creating successful cyber security projects that take the human factor into consideration (Lacey, 2010; Orshesky, 2003; Pfleeger & Caputo, 2012; Stewart & Jürjens, 2017), the presented results can help CISO's, security consultants or other managers responsible for the organizations security to execute successful cyber security culture change. With the presented framework, they can plan, execute and sustain the change in the organization's cyber security culture. It can be functioned as a starting point for organizations when planning on using change management to improve their cyber security. For instance, they can use the framework as guidelines to comprehend what essential aspects that should be considered for each activity in the change. Also, it is a tool for managers to evaluate their own role as a change leader and receive an understanding of what important characteristics a cyber security leader needs to take in order to provide a lasting change in the employees' cyber security behavior. Additionally, this provides managers with an

understanding of the employees' sensemaking needs and how they should be met during the change.

An example for how it can be viewed is that if a manager was planning on performing education towards the people in the organization about cyber security, the manager can see how the education should be performed to be effective. Also, the manager can understand that as a leader it is essential to show stability and trust, and also be pedagogic and personal towards the employees during the education. Additionally, the manager can take into consideration that employees have a need for reflection, involvement, and understanding in order for the education to be effective.

5.3 Limitations and future research

The study provides a number of contributions for theory and practice, however, the study comes with some limitations that need to be acknowledged. First, the study is limited to the context of cyber security. Yet, the change management principles resulting from this study could possibly be adjusted to fit other contexts as well. Therefore, a suggestion for future research could be to apply this framework to other contexts that need increased attention to change management. Another limitation of the study is that the data collection has only been performed on organizations based in Sweden. Although the change process would probably be similar to organizations in other countries, it would be interesting to investigate other countries further in detail since different countries organizational cultures can vary. Thus, to perform a similar study, but with empirical data collected from another country, would be an interesting idea for future research.

This study is limited to having a qualitative character. Hence, it would also be interesting to complement the study with a quantitative research approach that can for instance test the framework's potential in practice. Furthermore, the study is limited to the number of respondents and a suggestion for future research could be to focus on interviewing a larger number of respondents and case organizations, as well as other roles in an

organization, to provide even more perspectives of how change management can be used to improve cyber security.

REFERENCES

Ala-Laurinaho, A., Kurki, A-L., & Simonsen Abildgaard, J. (2017). Supporting Sensemaking to Promote a Systemic View of Organizational Change – Contributions from Activity Theory. *Journal of Change Management, 17*(4), 367-387. doi: 10.1080/14697017.2017.1309566

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security, 26*(4), 276-289. doi: 10.1016/j.cose.2006.11.004

Alhogail, A., & Mirza, A. (2014). A framework of information security change. *Journal of Theoretical and Applied Information Technology, 64*(2), 540-549.

Apker, J. (2004). Sensemaking of change in the managed care era: a case of hospital-based nurses. *Journal of Organizational Change Management, 17*(2), 211-227. doi: 10.1108/09534810410530629

Ashenden, D., & Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security, 39*(B), 396-405. doi: 10.1016/j.cose.2013.09.004

Balogun, J. (2006). Managing Change: Steering a Course between Intended Strategies and Unanticipated Outcomes. *Long Range Planning, 39*(1), 29-49. doi: 10.1016/j.lrp.2005.02.010

Bauer, H., Scherf, G., & von der Tann, V. (2017). Six ways CEOs can promote cybersecurity in the IoT age. Retrieved 2018-11-29 from https://www.mckinsey.com/featured- insights/internet-of-things/our-insights/six-ways- ceos-can-promote-cybersecurity-in-the-iot-age

Bevilacqua, B. (2017). How Facebook's Annual "Hacktober" Campaign Promotes Cybersecurity to Employees. *Harvard Business Review.*

Blau, A. (2017). Better Cybersecurity Starts with Fixing Your Employees' Bad Habits. *Harvard Business Review.*

Bowen, G. A. (2006). Grounded Theory and Sensitizing Concepts. *International Journal of Qualitative Methods, 5*(3), 12-23. doi: 10.1177%2F160940690600500304

Bullock, R. J., & Batten, D. (1985). It's just a phase we're going through: A review and synthesis of OD phase analysis. *Group and Organization Management, 10*(4), 383–412. doi: 10.1177/105960118501000403

Burnes, B. (1996). No such thing as ... a "one best way" to manage organizational change. *Management Decision, 34*(10), 11-18. doi: 10.1108/00251749610150649

Braun, A., Ball, S. J., Maguire, M., & Hoskins, K. (2011). Taking context seriously: towards explaining policy enactments in the secondary school, *Discourse: Studies in the Cultural Politics of Education, 32*(4), 585-596. doi: 10.1080/01596306.2011.601555

Braun V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. doi: 10.1191/1478088706qp063oa

Brisson-Banks, C. V. (2010). Managing change and transitions: a comparison of different models and their commonalities. *Library Management, 31*(4/5), 241-252. doi: 10.1108/01435121011046317

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security, 2016*(6), 8-14. doi: 10.1016/S1361-3723(15)30046-4

Chou, D. C. (2007). Field development in change management: how information systems contribute to the process of organisational change. *International Journal of Information Systems and Change Management, 2*(1), 100-106. doi: 10.1504/IJISCM.2007.013884

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security, 22*(5), 474-489. doi: 10.1108/IMCS-08-2013-0057

Da Veiga, A., & Eloff J. H. P. (2007). An Information Security Governance Framework, *Information Systems Management, 24*(4), 361-372, doi: 10.1080/10580530701586136

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

David, M., & Sutton, C. D. (2016). Samhällsvetenskaplig metod (1. ed.) Lund: Studentlitteratur.

Disparte, D., & Furlow, C. (2017). The Best Cybersecurity Investment You Can Make Is Better Training. *Harvard Business Review.*

Dubois, A., & Gadde, L. E. (2002). Systematic combining: an abductive approach to case research. *Journal of business research, 55*(7), 553-560. doi: 10.1016/S0148-2963(00)00195-8

Duck, J. D. (1993). Managing change: the art of balancing. *Harvard Business Review*, *71*(6), 109–118.

Du Toit, A. (2007). Making sense through coaching. *Journal of Management Development, 26*(3), 282-291. doi: 10.1108/02621710710732164

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review, 45*(1), 67-87. doi: 10.2307/41166154

Edmonson, A. C., & McManus, S. E. (2007). Methodological fit in management field research. *Academy of Management Review, 32*(4), 1155–1179. doi: 10.5465/AMR.2007.26586086

Everett, C. (2010). Embedding security: when technology is no longer enough. *Computer Fraud & Security, 2010*(11), 5-7. doi: 10.1016/S1361-3723(10)70143-3

Flowerday S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*(2016), 169-183. doi: 10.1016/j.cose.2016.06.002

Galli, B. J. (2018). Change Management Models: A Comparative Analysis and Concerns. *IEEE Engineering Management Review, 46*(3), 124-132. doi: 10.1109/EMR.2018.2866860

Gioia, D. A., & Chittipeddi, K. (1991). Sensemaking and sensegiving in strategic change initiation. *Strategic Management Journal, 12*(6), 433-448. doi: 10.1002/smj.4250120604

Hadlington, L. (2018). Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269-281. doi: 10.5281/zenodo.1467909

Hussain, S. T., Lei, S., Akram, T., Haider, M. J., Hussain, S. H., & Ali, M. (2018). Kurt Lewin's change model: A critical review of the role of leadership and employee involvement in organizational change. *Journal of Innovation & Knowledge, 3*(3), 123–127. doi: 10.1016/j.jik.2016.07.002

Jorgensen, H. H., Bruehl, O., & Franke, N. (2014). *Making change work …while the work keeps changing.* Somers: IBM Corporation.

ISO. (n.d.). ISO/IEC 27000 family – Information security management systems. Retrieved 2019-02-07 from https://www.iso.org/isoiec-27001-information-security.html

Jalali, S. (2018). The Trouble With Cybersecurity Management. *MIT Sloan Management Review.*

Jenkins, C. (2012). Towards "social" security. *Computer Fraud & Security, 2012*(8), 18-20. doi: 10.1016/S1361-3723(12)70084-2

Kotter, J. P. (2007). Leading change: Why Transformation Efforts Fail. *Harvard Business Review.*

Kotter, J. P. (2012). Leading Change: With a New Preface by the Author John P. Kotter. Boston: Harvard Business Review Press.

Kraft, A., Sparr, J. L., & Peus, C. (2018). Giving and Making Sense About Change: The Back and Forth Between Leaders and Employees. *Journal of Business and Psychology, 33*(1), 71-87. doi: 10.1007/s10869-016-9474-5

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security, 18*(1), 4-13. doi: 10.1108/09685221011035223

Levasseur, R. E. (2001). People Skills: Change Management Tools—Lewin's Change Model. *Interfaces, 31*(4), 71–73. doi: 10.1287/inte.31.4.71.9674

Limba, T., Plèta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues, 4*(4), 559-573. doi: 10.9770/jesi.2017.4.4(12)

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Thousand Oaks: SAGE Publications.

Maglaras, L. A., Kim, K., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., … Cruz, T. J. (2018). Cyber security of critical infrastructures. *ICT Express, 4*(1), 42-45. doi: 10.1016/j.icte.2018.02.001

Mansfield-Devine, S. (2017). Raising awareness: people are your last line of defence. *Computer Fraud & Security, 2017*(11), 10-14. doi: 10.1016/S1361-3723(17)30082-9

McKinsey. (2008). McKinsey Global Survey Results: Creating organizational transformations. *McKinsey Quarterly.*

Moran, J. W., & Brightman, B. K. (2000). Leading organizational change. *Journal of Workplace Learning, 12*(2), 66-74. doi: 10.1108/13665620010316226

Mouton, F., Leenen, L., & Venter, H.S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*(2016), 186-209. doi: 10.1016/j.cose.2016.03.004

Orshesky, C. M. (2003). Beyond technology – The human factor in business systems, *Journal of Business Strategy, 24*(4), 43-47. doi: 10.1108/02756660310494872

Osuagwu, E. U., Chukwudebe, G. A., Salihu, T., & Chukwudebe, V. N. (2015). Mitigating social engineering for improved cybersecurity. *2015 international conference on cyberspace governance,* 91-100. doi: 10.1109/CYBER-Abuja.2015.7360515

Page, L., & Schoder, J. (2018). Making change last: leadership is the key. *Journal of Business Strategy*. doi: 10.1108/JBS-01-2018-0003

Parmar, B. (2013). Employee negligence: the most overlooked vulnerability. *Computer Fraud & Security, 2013*(3), 18-20. doi: 10.1016/S1361-3723(13)70030-7

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. *Journal of Cognitive Engineering and Decision Making, 9*(2), 117-129. doi: 10.1177/1555343415575152

Pfleeger, S. L., Sasse, M. A., & Furnham, A. (2014). From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Homeland Security & Emergency Management, 11*(4), 489-510. doi: 10.1515/jhsem-2014-0035

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597-611. doi: 10.1016/j.cose.2011.12.010

Poppensieker, T., & Riemenschnitter, R. (2018). A new posture for cybersecurity in a networked world. Retrieved 2018-11-29 from https://www.mckinsey.com/business- functions/risk/our-insights/a-new-posture-for- cybersecurity-in-a-networked-world

Prosci. (n.d). The History and Future of Change Management. Retrieved 2019-01-06 from https://www.prosci.com/resources/articles/change- management-history-and-future

PwC. (2017). *Strengthening Digital Society against Cyber Shocks: Key Findings from the Global State of Information Security Survey 2018.* Retrieved from the website of PwC: https://www.pwc.com/us/en/cybersecurity/informati on-security-survey/strengthening-digital-society- against-cyber-shocks.html

PwC. (2018). The Global State of Information Security® Survey 2018. Retrieved 2018-11-29 from https://www.pwc.com/us/en/services/consulting/cyb ersecurity/library/information-security-survey.html

Ransbotham, S. (2017). Safeguard Your Organization's IoT Initiatives. *MIT Sloan Management Review*.

Rao, M. S. (2015). The tools and techniques of effective change management: Why some reformers succeed while others fail. *Human Resource Management International Digest, 23*(1), 35-37. doi: 10.1108/ HRMID-12-2014-0163

Rothrock, R. A., Kaplan, J., & van der Oord, F. (2018). The Board's Role in Managing Cybersecurity Risks. *MIT Sloan Management Review.*

Safa, N. S., Sookhak, M,. von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78. doi: 10.1016/j.cose.2015.05.012

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (Fifth.ed.). Edinburgh: Pearson Education Limited.

Sheehan, N. T. (2006). Want to improve strategic execution? Simons says levers. *Journal of Business Strategy, 27*(6), 56-64. doi: 10.1108/02756660610710364

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information, 22*(2), 63-75. doi: 10.3233/EFI-2004-22201

Simmonds, M. (2018). Instilling a culture of data security throughout the organisation. *Network Security, 2018*(6), 9-12. doi: 10.1016/S1353- 4858(18)30055-2

Simons, R. (1995). Levers of Control: How Managers Use Innovative Control Systems to Drive Strategic Renewal. Harvard Business School Press, USA.

von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security, 25*(3), 165-168. doi: 10.1016/j.cose.2006.03.004

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

von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information & Computer Security, 26*(1), 2-9. doi: 10.1108/ICS-04-2017-0025

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225. doi: 10.1016/j.ijinfomgt.2015.11.009

Spremic, M., & Simunic, A. (2018). Cyber Security Challenges in Digital Economy. *Proceedings of the World Congress on Engineering, 1.* 341-346

Stewart, H., & Jürjens, J. (2017). Information security management and the human aspect in organizations. *Information & Computer Security, 25*(5), 494-534. doi: 10.1108/ICS-07-2016-0054

Stewart, J., & Kringas, P. (2003). Change Management – Strategy and Values in Six Agencies from the Australian Public Service. *Public Administration Review, 63*(6), 675-688. doi: 10.1111/1540-6210.00331

Syed, A., Padmanabhan, V., & Dixon, J. (2014). *Why cybersecurity is a strategic issue.* Retrieved from the website of Bain & Company: https://www.bain.com/insights/why-cybersecurity- is-a-strategic-issue/

Thurlow, A., & Mills, J. H. (2009). Change, talk and sensemaking. *Journal of Organizational Change Management, 22*(5), 459-479. doi: 10.1108/09534810910983442

Tyler, C. (2005). Metaphor and Management: making sense of change. *Management in Education, 19*(3), 28–32. doi: 10.1177/08920206050190030701

Upton, D. M., & Creese, S. (2014). The Danger from Within. *Harvard Business Review.*

Venus, M., Stam, D., & van Knippenberg, D. (2018). Research: To Get People to Embrace Change, Emphasize What Will Stay the Same. *Harvard Business Review.*

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science, 16*(4), 409-421. doi: 10.1287/orsc.1050.0133

Winnefeld Jr, J. A., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity's Human Factor: Lessons from the Pentagon. *Harvard Business Review.*

Yilmaz, S., Ozgen, H., & Akyel, R. (2013). The impact of change management on the attitudes of Turkish security managers towards change. Journal of Organizational Change Management, 26(1), 117-138. doi: 10.1108/09534811311307941

van Zadelhoff, M. (2016). The Biggest Cybersecurity Threats Are Inside Your Company. *Harvard Business Review.*

APPENDIX

Appendix 1. Interview guide for CISO

Background

- What is your position at the organization?
- How long have you worked here?
- How long have you worked with security?
- What are your main job tasks?

General questions about security projects

- Can you tell me a bit about how you work with security in the organization? What major changes in security have occurred during the last years at the organization?
- How have you been steering the project/projects/security initiatives? What was your role in this? Who was involved?
- What did the project/security initiatives result in?
- Do you believe it was successful?
    - If yes, why do you think it became so successful? What do you define as a successful project?
    - If no, why do you think it was not?
- What have been the greatest challenges?
- What could have been improved?
- What do you think is important to get every employee to have cyber security thinking in their everyday job?
- Do you believe there is a security culture at the organization?

Change management

- How do you work with change management in security projects? Like, how do you work with getting all the employees motivated to change?
- What do you think should be improved when it comes to change management in security projects?
- Did you experience any resistance from the employees that this change was going to happen?
    - If yes, how did you handle it?
    - If no, what makes you think it was not any resistance?
- How was the support from top management? How were they involved in this? In what way?
- How does the communication work? How do you communicate with every employee in the organization? Through which channels? In what way?
- Did you use any kind of training and education for the employees in order for them to understand?

- Do you think the employees had enough education and training?
    - If yes, why do you think so?
    - If no, what could have been done better? Why was there no more education?
- If some employees felt like they did not understand or that they had any questions, was there anyone present that could answer the questions?
    - If yes, how did that work?
    - If no, why not?
- How did you work with getting all employees motivated? Did you use some kind of incentives?
    - If yes, what kind of incentives?
    - If no, why not?
- Do you believe that all people in the organization had understood this?
    - If yes, why do you think so?
    - If no, what do you think could have been better in order for them to understand?
- Do you evaluate that everyone had learned and understood all of this? How?
- How do you work with feedback?
    - For example, how does the management know what needs to be done better and how can the employees give feedback to the management?
    - How does the management give feedback to the employees of what can be done better?
- Do you believe that cyber security is a natural part of the organization that you have done the consultancy work for? Like, has it become a natural part of the organization's culture?
    - If yes, what do you think have done that it became like this?
    - If no, why do you think it hasn't been so? What do you think is important for it to be so?

Other questions:

- What do you believe are the key factors create successful change management?
- Do you think there is any difference between private and public organizations? In what way?
- Is there anything else that I have not mentioned that you think could be useful when it comes to change management in security projects?

Closing questions:

- Is there anyone else that you would recommend me to talk to in the organization about this?
- Would it be okay if I get back to you if any new questions appear during the process?

Appendix 2. Interview guide for Consultant

Background

- What is your position at Alpha?
- How long have you worked with security?
- What are you currently working on/what kinds of projects are you currently involved in?

General questions about security projects

- Can you give an example of how the work has been done when you been working with security at a client?
- How have you been steering the project/projects? What was your role in this? Who was involved?
- What did the project result in?
- Do you believe it was successful?
    - If yes, why do you think it became so successful? What do you define as a successful project?
    - If no, why do you think it wasn't?
- What have been the greatest challenges?
- What could have been improved? What could have been done better from the client's side?

Change management

- How do you work with change management in security projects? Like, how do you work with getting all the employees motivated to change?
- What do you think should be improved when it comes to change management in security projects?

In the beginning of the project:

- Did you experience any resistance from the employees that this change was going to happen?
    - If yes, how did you handle it?
    - If no, what makes you think it was not any resistance?
- How was the support from top management? How were they involved in this? In what way?

During the project:

- How was this communicated to every employee in the organization? Through which channels? In what way?
- Did you use any kind of training and education for the employees in order for them to understand?

- Do you think the employees had enough education and training?
    - If yes, why do you think so?
    - If no, what could have been done better? Why was there no more education?
- If some employees felt like they did not understand or that they had any questions, was there anyone present that could answer the questions?
    - If yes, how did that work?
    - If no, why not?
- How did you work with getting all employees motivated? Did you use some kind of incentives?
    - If yes, what kind of incentives?
    - If no, why not?

After the project:

- Do you believe that all people in the organization had understood this?
    - If yes, why do you think so?
    - If no, what do you think could have been better in order for them to understand?
- Do you evaluate that everyone had learned and understood all of this? How?
- How do you work with feedback?
    - For example, how does the management know what needs to be done better and how can the employees give feedback to the management?
    - How does the management give feedback to the employees of what can be done better?
- Do you believe that cyber security is a natural part of the organization that you have done the consultancy work for? Like, has it become a natural part of the organization culture?
    - If yes, what do you think have done that it became like this?
    - If no, why do you think it hasn't been so? What do you think is important for it to be so?

Other questions:

- What do you believe are the key factors create successful change management?
- Do you think there is any difference between private and public organizations? In what way?
- Is there anything else that I have not mentioned that you think could be useful when it comes to change management in security projects?

Closing questions:

- Would it be okay if I get back to you if any new questions appear during the process?

Appendix 3. Interview guide for Employee

Background

- What is your position at the organization?
- How long have you worked here?
- What are your main job tasks?

General questions about security

- How do you experience the security at the organization? Do you believe that the organization works a lot with security?
- Would you say that you are involved in the organization's security initiatives?
    - If yes, in what way?
    - If no, would you like to be more involved? How?
- (If the respondent has been in the organization for a long time) How do you think the security has changed the last years? Has it improved or is it still the same? What kind of big changes around the cyber security have you noticed in the organization?
- Would you say that you think about security when you perform your job?
    - If yes, what makes you have this security-thinking?
    - If no, why do you think you do not do it?
- Is there any security initiative that the organization has taken that you experience is an obstacle for your daily job tasks? Like, have it made your job tasks difficult in some way?
    - If yes, in what way? What do you think would make it easier? Did you become informed about it etc.?
- How has the top management worked in order to strengthen the security thinking? What kind of initiatives have they taken to strengthen the security thinking?
    - What has worked well?
    - What has not worked so well?
    - How should it have been done?
- Do you feel like you are motivated to think about security/ to be security conscious?
    - If yes, why? What do you believe would do to make you even more security-conscious?
    - If no, why not? What makes you think that you would be motivated to be more security-conscious?
- Do you believe that you have a good understanding of security? Do you for example believe that you know and understand the organization's security policy?
- How would you like to be informed if there is happening anything new when it comes to security in the organization? (Especially when it concerns your own work)
- Have you been educated in security?
    - What kind of education?
    - How did you experience it?
    - How do you feel that you learn best? By having traditional lectures, online courses, etc.?

    - What do you believe could have been improved?
- Do you experience that there is someone that you can ask questions and talk to about this?
    - If yes, who can you talk to?
    - If no, who would you have wanted to turn to? In what way?
- How do you experience that everyone in the organizations attitude towards security is?
    - If good, what do you think is the reason for having such a good security culture?
    - If not so good, what do you think is the reason that the security culture is not that good in the organization?
- How do you think that the organization can be better in getting everyone in the organization more security-conscious? What do you wish could be improved when it comes to the organization's security efforts?
- Have you done something, have you contributed to strengthening the organization's security?
- Do you have any other reflections about this that you would like to share?