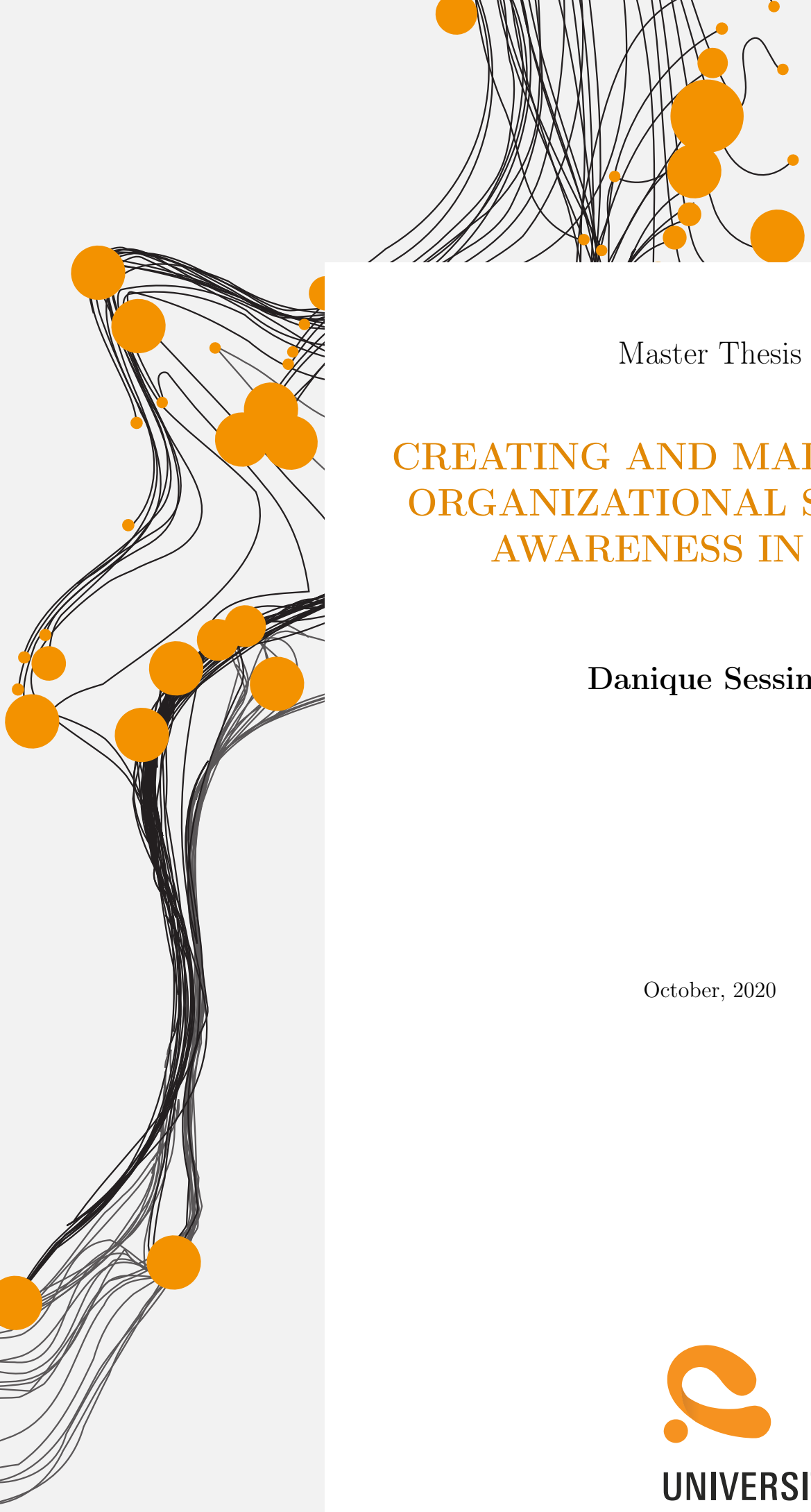

Master Thesis

CREATING AND MAINTAINING ORGANIZATIONAL SECURITY AWARENESS IN SMES

Danique Sessink

October, 2020

COFANO

UNIVERSITY OF TWENTE.

Master Thesis

Creating and Maintaining Organizational Security Awareness in SMEs

The investigation, design, and validation of an artifact for Cofano that treats the problem of creating and maintaining security awareness in SMEs.

Author

Name:	Danique Sessink
Programme:	Master Computer Science
Specialization:	Cyber Security
Faculty:	Electrical Engineering, Mathematics and Computer Science (EEMCS)
E-mail:	d.a.m.sessink@alumnus.utwente.nl

Assessment Committee

Chair and first supervisor:	Dr. Maya Daneva Services, Cybersecurity & Safety (SCS)
Examiner:	Dr. Faiza Bukhsh Datamanagement & Biometrics (DMB)
Daily supervisor:	Leon de Vries Services, Cybersecurity & Safety (SCS) Cofano
Advisory member:	Joey Osseman Cofano

Abstract

Usually, employees are the weakest link within an organization when it comes to cyber security. To prevent security-attacks in an organization, each employee should be able to recognize security threats and know how to mitigate them. For that reason, cyber security awareness amongst employees is an important organizational concern. Within the company Cofano, it is hard to create security awareness and consistently maintain it throughout the year. The research in this master thesis aims to design and validate an artifact for Cofano that treats the problem of creating and maintaining security awareness in SMEs with regard to ISO 27001 and with preservation of corporate culture.

To achieve this research goal, a design science research methodology was chosen. First, a problem investigation was done through interviewing the problem stakeholders within Cofano. From the conducted interviews, improvement possibilities for Cofano on the area of security awareness could be extracted. Next, an artifact was designed based on literature from a research topics paper combined with the interview results. The artifact, together with explanatory notes, contains what Cofano has to do in order to achieve a higher level of security awareness within the organization. Finally, this artifact was validated by using expert opinions and perceptions. The results indicate that the artifact provides a clear overview of all steps Cofano can undertake to reach a higher level of security awareness. In addition, it contains all steps needed for improvement of security awareness amongst employees.

The results of this research aid Cofano in improving the level of security awareness amongst the employees while corporate culture is preserved, and the ISO 27001 standard is respected. Future directions could be implementing the artifact at Cofano and evaluating this implementation. In addition, the application of this research to other, similar companies could be investigated as to determine the usability of the proposed artifact at companies in a similar business sector as that of Cofano.

Acknowledgements

Throughout writing this thesis, I have received support from many people. These people helped me see past obstacles and inspired me to keep pushing forward. Hereby, I would like to thank all of them for their continuous support.

First, I would like to thank my supervisor Maya for her help in shaping and sharpening this research. Next, I would like to thank my daily supervisor Leon for his valuable feedback and useful discussions. Furthermore, I would like to thank my company supervisor Joey for providing me with insights into the security of Cofano.

I would also like to thank all of my colleagues at Cofano for their time, support, discussions, and distractions. I am happy to get the opportunity to continue working with all of you.

Last but definitely not least, I want to thank my friends, family, father and mother, sister, and especially my boyfriend Dennis for providing the much-needed distractions during this thesis.

Love,

Danique

Contents

Part I

Background

Chapter 1

Introduction

> "*In every chain of reasoning, the evidence of the last conclusion can be no greater than that of the weakest link of the chain, whatever may be the strength of the rest.*" — Thomas Reid

A chain is only as strong as its weakest link. Within an organization this is no different. Usually, employees are the weakest link within an organization when it comes to cyber security [4, 8, 19, 26]. To prevent an organization against security-attacks, an employee should be able to recognize security threats and know how to mitigate them. For that reason, cyber security awareness amongst employees is an important organizational concern. If employees are made aware of the various forms of security threats, they can identify them and the weakest link in the chain can be strengthened.

International information security standards exist to enhance the security within an organization, such as ISO/IEC 27001. The ISO/IEC 27001 standard requires organizations to organize cyber security awareness training to educate their employees. In order to change the way employees act and behave with regard to information security, an information security culture should be an integral part of the organizational culture [23, 44].

This chapter is the introduction to this research. In section 1.1, definitions are presented to establish and clarify the meaning of the concepts used in the research. In addition, background on security awareness, ISO 27001 and corporate culture

is presented in sections 1.1.1, 1.1.2 and 1.1.3. The context of this research is presented in section 1.2. Based on this information, a research goal is identified, which is stated in section 1.3. To achieve this goal, research questions have been created, which are presented in section 1.4. Finally, the first chapter is concluded by providing an outline for the thesis which can be found in section 1.5.

1.1 Concepts and Definitions

1.1.1 Security Awareness

Amankwa et al. present a working definition of information security awareness (ISA) based on several definitions in existing literature [2]. In their paper, they describe how the following three attributes are important for information security according to the National Institute of Standards and Technology (NIST): focus, purpose, and method [42]. Based on these attributes, Amankwa et al. define information security awareness as: "*any endeavour to focus employees' attention on information security in order to ensure that all employees understand their roles and responsibilities in protecting the information that is in their possession by using print or electronic media*" [2]. The working definition of information security of Amankwa et al. will be used in this paper.

1.1.2 ISO 27001 and Security Awareness

The information security standard ISO 27001 aids an organization in creating an Information Security Management System (ISMS). The ISMS provides an organization with a structured approach for dealing with the security of assets and information. The ISO 27001 standard also contains controls for human resource security, in Annex A.7. The second part of this Annex, A.7.2, has the objective of ensuring that employees and contractors understand and are aware of their responsibilities with regard to information security during employment. Control A.7.2.2 is about awareness, education, and training with regard to information security. In this control, it is stated that all employees of the organization and, where relevant, contractors, should receive appropriate information security awareness education and training, and supplementary training of organizational policies and procedures, pertinent to their role within the company.

1.1.3 Corporate Culture and Security Awareness

Corporate culture, or organizational culture, is about the divergence between formal business processes and values, beliefs, assumptions, and experience of the employees [30]. With regard to information security, culture can also be defined as "*the behaviour of an organization to protect data, information and knowledge*" [35]. As a system of learned behaviour, organizational culture has significantly affected the information security process [44]. Between organizational culture (OC) and information security awareness (ISA), there is a mediator variable: security culture (SC) [41]. Between organizational culture and security culture, as well as between security culture and information security awareness, a strong, positive linear relationship exists, as depicted in figure 1.1.

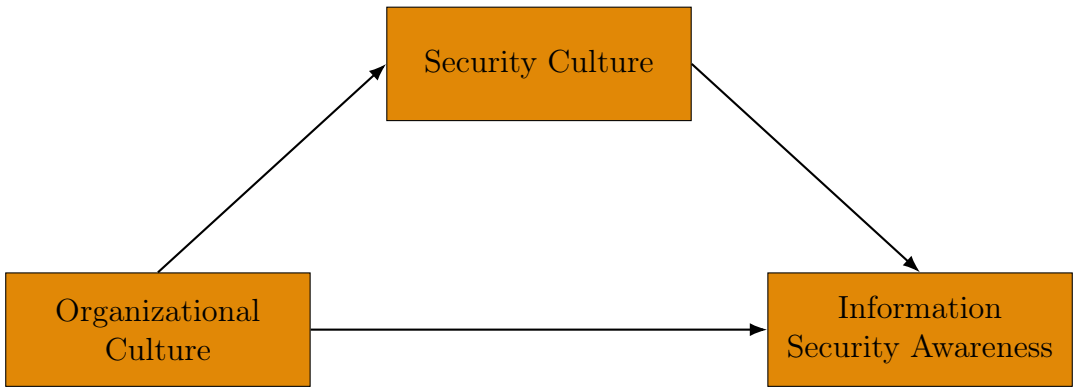

Figure 1.1: The relationship between OC, SC, and ISA [41]

Since the impact of organizational culture on employees is significant, integrating information security culture in organizational culture is needed as to guide the behaviour of employees with regard to information security [3, 6, 11, 17, 23, 39]. However, if security awareness needs to be improved within the organization, the focus should be on the security culture instead of the organizational culture. Changing the security culture would cost less time and resources than changing the organizational culture, since security culture is only a part of the organizational culture. As a result of improving the security culture, the organizational culture may be positively impacted.

1.2 Context

Cofano Software Solutions is a software company that offers Software as a Service (SaaS) for the logistics sector. In 2018, Cofano decided to pursue the ISO/IEC 27001 certification to show their customers that information security is highly prioritized within the organization. Annually, an audit needs to be conducted to maintain this certification. The workload prior to such an audit is high for the employees of Cofano that are concerned with managing information security, as the level of security awareness does not remain the same throughout the year. According to a security officer of Cofano, an increase in the reporting of security issues is noticed, as well as an increase in security awareness amongst employees around the date of the audit. Currently, an audit always needs extra preparation, whereas this should not be the case and Cofano should always be ready for an audit. Therefore, Cofano desires a reduction of the workload prior to the audit by creating security awareness amongst employees and keeping it at the same level throughout the year.

1.3 Research Goal

Within Cofano, it is hard to create security awareness and maintain it at the same level throughout the entire year. Therefore, the following research goal has been formulated:

Design and validate an artifact for Cofano that treats the problem of creating and maintaining security awareness in SMEs with regard to ISO 27001 and with preservation of corporate culture.

1.4 Research Questions

In order to achieve the research goal, we have to answer the following research questions:

RQ1: What are the challenges Cofano currently experiences from the perspective of security awareness and Cofano's organizational culture?

- **RQ1.1:** Who are the stakeholders and what are their goals?
- **RQ1.2:** What is Cofano currently doing to resolve the challenges? If applicable and known, what are the shortcomings of the approaches that were tried out?

RQ1.3: What are the effects if the challenges are not treated and how do these detract from stakeholder goals?

RQ2: What artifact can be designed that treats the problem Cofano is experiencing?

RQ2.1: What are the available treatments?

RQ2.2: What are the concepts and components of available treatments that treat the problem?

RQ2.3: How do these contribute to the stakeholder goals?

RQ3: What is the applicability of the proposed artifact?

RQ3.1: To what extent is the proposal useful for the practitioners in the field?

RQ3.2: To what extent is the proposal usable at Cofano? Can the practitioners apply it in the context for which the artifact was envisioned?

1.5 Outline

The thesis is structured as follows: chapter 2 describes the methodology that is used during the research in detail. Chapter 3 corresponds to RQ1 and presents the results from the interviews. Additionally, this chapter identifies improvement possibilities. Chapter 4 corresponds to RQ2 and outlines the design for a solution for creating security awareness. Chapter 5 corresponds to RQ3 and validates that solution. Chapter 6 discusses the results and limitations of the research. Finally, the thesis is concluded with chapter 7, in which the research questions are answered, and future work is discussed.

Part II

Method

Chapter 2

Approach and Methodology

In this chapter, the approach and methodology of the research will be presented. In section 2.1, we discuss the method for the research. Next, in section 2.2, we focus on the approach of the problem investigation. Consequently, in section 2.3 we discuss how the treatment design has been established. Finally, in section 2.4, we discuss the approach for the treatment validation.

2.1 Method

In order to achieve the research goal in section 1.3, we will make use of the Design Science Methodology as discussed by Wieringa [40]. Design science research revolves around the interaction between an artifact and a context and can be split up into two parts: design and investigation. The first part requires a real-world change, whereas the second part is about answering knowledge questions.

A design cycle consists of three steps which can be iterated over many times. The first step is the problem investigation, the second step is the treatment design and the third and final step is the treatment validation. The design cycle is part of a larger cycle, namely the engineering cycle, as depicted in figure 2.1. In this cycle, the results of the design cycle are implemented and evaluated. In this research, we will only focus on the first three steps of the engineering cycle, namely the problem investigation, the treatment design, and the treatment validation.

For the first step, the problem investigation, we will investigate what must be improved and why. The most important question is: what are the challenges Cofano currently experiences with regard to security awareness? In order to answer that

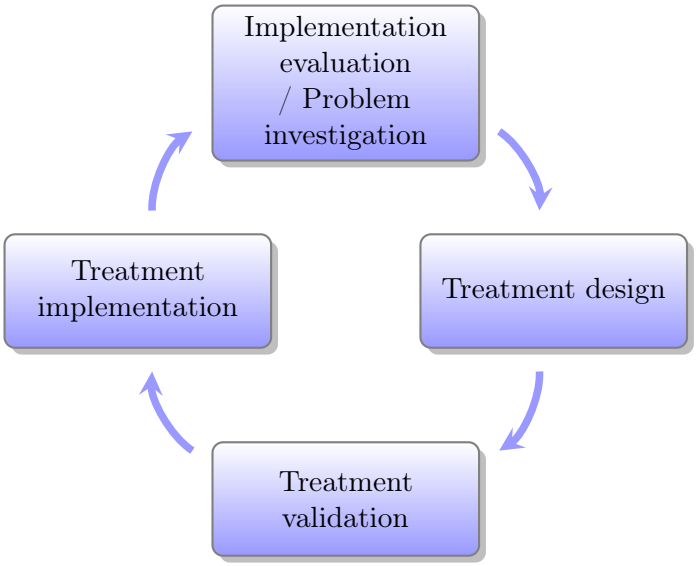

Figure 2.1: The engineering cycle

question, the stakeholders of the problem will be investigated. Moreover, we will look into what Cofano is currently doing to resolve the challenges they encounter. Additionally, we investigate the effects of leaving the challenges untreated. Semi-structured interviews are conducted with the stakeholders to get more practical insight in the problem and gather ideas for the treatment design. The approach for the problem investigation is presented in section 2.2. Consequently, the results from the problem investigation are discussed in chapter 3.

For the second step, the treatment design, we will design an artifact which could treat the problem. To achieve this, we have to find out what the available treatments are. Next, we need to determine what concepts and components of these available treatments could treat Cofano's problem. Consequently, we need to investigate how these concepts and components contribute to the goals of the stakeholders. The approach for the treatment design can be found in section 2.3. Additionally, the proposed solution is discussed in chapter 4.

For the third step and final step, the treatment validation, we will look into the applicability of the designed artifact. With a group of practitioners, we will look at the usefulness of the proposed artifact. In addition, we will investigate to what extent the artifact is usable at Cofano and if practitioners can apply it in the context for which the artifact was envisioned. The approach for the treatment validation is presented in section 2.4. Moreover, the expert evaluation is presented in chapter 5.

In the fourth step, the treatment implementation, the problem is treated with the designed artifact. Finally, in the implementation evaluation, it is evaluated if the treatment has been successful. The steps from the engineering cycle can now be repeated again to see if the problem still exists. The focus of this research is on the problem investigation, the treatment design, and the treatment validation.

2.2 Problem Investigation

2.2.1 Initial Stakeholder Analysis

For this research, it is important to identify the stakeholders of the problem, as they could supply useful information that possibly contributes to treating the problem. According to Wieringa [40], a stakeholder is someone that experiences effects when the problem is treated. These effects do not necessarily have to be positive and could even be negative for some cases. Nevertheless, treating the problem should result in a positive effect for at least some of the stakeholders.

The stakeholders of this research are as follows:

- **Cofano** - sponsor
- **Cofano employees** - end users of the artifact
- **SMEs** - functional beneficiary

Cofano as organization is the sponsor of the research, as it provides the budget for developing an artifact that will be useful to the company. In addition, the employees of Cofano are the end users of the artifact and will be the ones that benefit from the use of it. Moreover, SMEs who want to create and maintain security awareness with regard to ISO 27001 and with preservation of corporate culture are the functional beneficiaries, as they could benefit from this research and the artifact it will produce.

Since the focus of this research lies on Cofano and their problem with security awareness, we will mainly focus on the second group of stakeholders: the employees. As each member of this group of stakeholders is involved with security awareness in a different way, we can break the group down into more specific groups of stakeholders. The breakdown of these groups was discussed during a pilot interview with an expert of Cofano, who is part of the management team. The result of breaking down the group of stakeholders that are Cofano employees looks as follows:

- Management Team

- Security Officers
- Lead Developers
- Developers
- Infrastructure Team
- Supporting Staff
- Students

The management team consists of the owner of the company and the two managers of operations of Enschede and Sliedrecht. Next, the security officers of Cofano are two developers: one in Enschede and one in Sliedrecht. These officers do not only handle the security matters of Cofano, but they are also lead developers next to this function. At Cofano, six lead developers are in charge of the various project teams. Consequently, the developers, a group of about 25 people, are members of these project teams. The infrastructure team, consisting of two members, handles all infrastructure within Cofano. Additionally, we have the group of supporting staff, consisting of seven members with various tasks. Two of them are concerned with sales, marketing and product and project management. One of them is a service desk employee. Another employee is concerned with HR and office management related issues, whereas a different employee is concerned with legal issues. Additionally, Cofano has a consultant who is involved in the implementation process of Cofano's products. Moreover, one employee is concerned with client and product management.

Finally, we have the stakeholder group of students. These employees are doing an internship or graduation at Cofano. They are not considered for the investigation, because they work on their own laptop and do not have access to Cofano's sensitive data.

2.2.2 Qualitative Interviews

As part of the problem investigation, qualitative interviews were done with the problem stakeholders, since more practical insight in the problem was needed. In the interview, we wanted to find out more about:

- Who the stakeholders are and what their goals are
- What challenges they encounter, how they are resolved, and what the possible

shortcomings are of this approach

- What the effects are if the problem is not treated

Not only would these interviews help us gaining more insight into the problem, the results from the interviews can also aid in creating a treatment for Cofano's problem.

The interview questionnaire consisted of 17 questions, divided in five parts, and can be found in appendix B. The first part contained questions about general information of the participant, such as name, location of Cofano they work at, role/function within Cofano, tasks within Cofano and if they were in contact with customers or not.

The second part consisted of questions about the participants' security knowledge. Questions were asked about what the participant thought security was, what their perception was of the security within Cofano, what they thought Cofano's goals where on the area of security, and what they thought security awareness was.

After the second part, the participant received the definition of security awareness, as well of some examples. Hence, every interviewee could answer the remainder of questions with the same knowledge. In the third part, questions about security awareness perception, importance and obtaining security awareness were asked.

Consequently, in the fourth part, participants were asked about their involvement in security within Cofano, as well as their goals. In addition, participants were asked if they thought any problems with regard to security awareness existed.

Finally, in the fifth part, participants were asked if they encountered any challenges with regard to security awareness. Additionally, they were asked what they thought the effects could be of not addressing security awareness within Cofano.

2.2.3 Sample Size

After the interview questionnaire was created, a number of participants needed to be interviewed. Usually, in qualitative research, sample size is determined based on achieving saturation. Saturation is achieved when no new information is discovered and should be a guiding principle in choosing the sample size, according to Mason [25]. Creswell and Poth indicate how Polkinghorne recommends having a sample size between 5 - 25 for phenomenological studies [9, 27]. Based on the structure and content of the interview, as well as participant homogeneity, Guest

et al. recommends a sample size of 12 participants [15]. In other words, each participant needs to be asked a similar set of questions, or data saturation cannot be achieved. Otherwise, a new piece of information will come to light in each new interview.

Initially, we decided on a sample size of 10-15 participants. The actual size would depend on when saturation was attained. After 13 interviews saturation was achieved, since in the last two interviews no more new information was shared. Therefore, the sample size of this research is 13 participants.

2.2.4 Interview Materials and Participants

Interviews were done with 13 of the stakeholders to gain more insight in the challenges Cofano is currently experiencing from the perspective of security awareness. Nine of these participants are employed at the office in Enschede, the other four participants work from the office in Sliedrecht. In table 2.1 the number of stakeholders per stakeholder group is listed, as well as the amount and percentage of interviewees per stakeholder group. As can be seen in table 2.1, the total amount of interviewees is higher than the 13 interviews done. This is because some of the Cofano employees are a member of several stakeholder groups at the same time. For example, the security officers are also lead developers, and some of the lead developers are part of the management team. Hence, this was considered when interviewing the stakeholders, as they were asked about their tasks within Cofano. In addition, we identified in which of the stakeholder groups (one or multiple) the interviewees fit, which can be found in table 2.2.

Stakeholder group	**Amount**	**Number of interviewees**	**Percentage**
Management Team	3	3	100.0 %
Security Officers	2	2	100.0 %
Lead Developers	6	4	66.7 %
Developers	25	5	20.0 %
Infrastructure	2	1	50.0 %
Supporting Staff	7	2	28.6 %
Total	45	17	37.9 %

Table 2.1: Number of stakeholders and interviewees per group

First, a pilot interview was conducted with one of the stakeholders. The purpose of this interview was to see if any improvements could be made to the interview questions. Additionally, the pilot interview would give an indication of the time it would take to conduct such an interview. The interview guide for the pilot

Group/Participant	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Management Team													
Security Officers													
Lead Developers													
Developers													
Infrastructure													
Supporting Staff													

Table 2.2: Identification of stakeholder group(s) for interviewees

interview can be found in appendix A. During this interview, feedback was given that highlighted possible improvements. The feedback could be bundled in the following three improvement points:

- Additional general information could be useful, such as location and customer contact
- Information about the security knowledge is needed
- A definition of security awareness needs to be provided, so interviewees have the same level of knowledge at some point during the interview

All of these improvements were suggested to enable better judgement of answers about security awareness problems, challenges, and effects. For example, if an interviewee did not think there was something problematic in the field of security awareness, it could be because they were not involved in security awareness in any way. Accordingly, the interview was adapted in such a way that it now includes two additional questions about general information. Moreover, some extra questions were added that aid in gaining insight into the security knowledge of the interviewee. In addition, after the knowledge questions were asked, a definition of security awareness and some examples were given. As a result, every interviewee could answer the remainder of questions with the same knowledge. The improved interview guide can be found in appendix B. The improvements made to the interview did not invalidate the data gathered from the pilot interview, since the additional required questions identified by the expert were immediately answered by the expert himself during the pilot interview. Consequently, these results could be used during the research. All interviews were conducted in Dutch.

After the pilot interview was adapted, interviews were held with the other 12 stakeholders. The interviews took place in the same week and were held in the office, through video meetings or through phone calls and lasted no longer than

half an hour. The participants were told no preparation was needed and that the subject of the interview was security. At the start of the interview, the interviewer asked the participant if he or she agreed to the interview being recorded for processing purposes. Since all participants consented to the interviewer recording the interview, the interviewer only made brief notes of outstanding answers during interviews.

Once all interviews were conducted, the interviews were processed. The interviewer listened to all recordings and manually transcribed each interview.

2.2.5 Data Analysis

For the analysis of the interviews a systematic approach for qualitative content analysis (QCA) by Kuckartz was used [21]. Kuckartz describes that a QCA usually consists of the following six steps:

1. Preparing the data
2. Forming the main categories
3. Coding the data
4. Compiling text passages and forming subcategories
5. Perform analyses based on category and present results
6. Report and document

In the first phase, the data is prepared. The conducted interviews were manually transcribed to ensure the completeness of the interview data. On a few occasions, some interpretation was needed since the audio was distorted, but no extensive interpretation was needed in any case. The interpretation was based on the context and the researcher's knowledge. Consequently, an initial read-through was performed on the interview transcripts. A word cloud was constructed from the contents of the interview, from which stop words were excluded based on an extensive Dutch list of stop words created by Eijkemans [13]. The word cloud can be found in appendix C.

In the second phase, categories are constructed. The set of main categories was created based on the interview questions that were asked. For the first coding cycle, the following 16 categories were constructed:

- Location
- Role/Position
- Tasks
- Contact with customer
- Security definition
- Security perception
- Perceived goals
- Security awareness definition
- Security awareness perception
- Security awareness importance
- Obtaining security awareness
- Involvement in security awareness
- Goals security awareness
- Problems and improvements security awareness
- Security awareness challenges
- Effects not addressing security awareness

In the third phase, the text segments that correspond to the categories are coded accordingly. For coding the text segments, the software MAXQDA was used [1], which is the same software as used by Kuckartz [21]. The guidelines of Kuckartz and Rädiker [22] are used for analyzing the data with MAXQDA.

In the fourth phase, the text segments are paraphrased and will be used to form subcategories inductively. Only text segments that are relevant for the research are paraphrased. For the creation of the subcategories, a similar process to that of open coding was used, as described by Strauss and Corbin [37]. This is data-driven since the text segments are used to form subcategories. The codes of the subcategories were words that described which topic the interviewee was talking about. A paraphrase could have multiple subcategories: as many as were fit for the topics of that paraphrase. For the category *Security definition*, the following subcategories were created:

- Policy
- CIA
- Training/education
- Physical
- Access control and user roles
- Information classification
- Intellectual property
- Security of data
- Security of applications
- Security of infra

- Hardware
- Social engineering
- Software security

All codes for categories and subcategories can be found in appendix D.

After coding, the Creative Coding tool of MAXQDA was used to see if anything in the current coding scheme could be re-organized or higher-level concepts could be developed. Codes were grouped together based on similarity, to form a paragraph together. However, forming paragraphs did not only depend on creative coding, but was also done if a paragraph was deemed too long. The re-organized coding scheme resulted in a paragraph classification per category for chapter 3. To illustrate the creative coding process, creative coding for the category security definition can be found in appendix E.

Consequently, in the fifth phase, the coded data was analyzed. For this, the paraphrased text passages are combined to enable for a more abstract view of the results. In the sixth and final phase, the results were reported and documented. The results are presented in chapter 3.

2.3 Treatment Design

For the treatment design, research has already been done on available treatments in a preliminary investigation for this thesis. From literature research in this preliminary investigation, a framework and model that could serve as good candidates in the development of a framework for SMEs such as Cofano were identified. The available treatments are mapped to Cofano and the mapping is validated by an expert on the area of security within Cofano. Consequently, concepts and components that could treat the problem are taken from the available treatments and their contribution to the stakeholder goals is discussed. Finally, the artifact design is presented, which is a combination from the interview data and the available treatments.

2.4 Treatment Validation

According to Wieringa, a straightforward method to validate a treatment is by expert opinions [40]. Experts are asked to give their opinions about the proposed artifact in a short interview. The interview questions are based on a modified version of the original Technology Acceptance Model (TAM) by Davis [10]. The adapted model by Jones et al. includes employee adaption of security measures and is depicted in figure 2.2 [18].

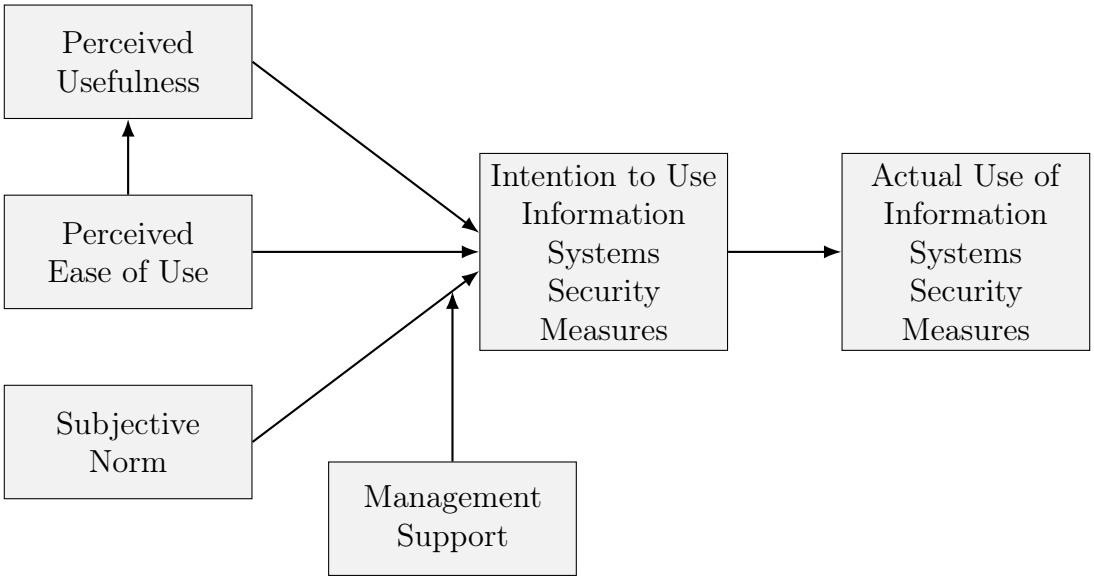

Figure 2.2: Modified Technology Acceptance Model [18]

In the expert interview, two experts from Cofano are asked about the perceived ease of use of the artifact, perceived usefulness of the artifact and intention to use the artifact within Cofano. The expert interview can be found in appendix F.

The experts both have the function of *Manager Operations* and are members of the management team of Cofano. One is based in Sliedrecht and the other is based in Enschede. Both experts are lead developers. Additionally, the first expert is a security officer.

Part III

Results

Chapter 3

Problem Investigation: Findings From the Interviews

> "*Social engineering: the greatest vulnerability is that people are way too nice - if people were assholes, companies would be a lot safer.*"
> — Developer Cofano

This chapter presents the results of the interview-based qualitative study, which serves the purpose of a problem analysis as discussed by Wieringa [40]. The interviews take the perspective of Cofano employees and reflect what they think about Cofano's security awareness. In what follows, each section with the exception of section 3.1 and section 3.15, contains solely the view of employees of Cofano. The sections are based of the categories created whilst coding, as can be read in section 2.2.5. To emphasize, this chapter is about the opinions and experiences of the employees that came up during the interview questions. Hence, it might be the case that some information is listed in other sections than expected.

In the following sections, the concepts, perceptions, and goals of the employees with regard to Cofano's security and security awareness are discussed. In addition, the importance of security awareness as viewed by the employees is presented, as well as how they think security awareness is currently obtained amongst employees within Cofano. The involvement and personal goals of the employees with regard to security awareness are examined, as well as the challenges and problems they think are encountered in this area. Furthermore, it is discussed what employees

think that will happen if security awareness is not addressed within Cofano. This is followed by a section listing the general remarks the employees had during the interviews. Next, the improvement possibilities that could be extracted from the interviews are presented. Consequently, the validity of the results is discussed. Finally, the chapter is concluded with a summary.

3.1 Interviewee Position within Cofano

To clarify which interviewee said what during the interview and what their role is within Cofano, we will make use of abbreviations of roles whenever an interviewee has multiple roles. The following codes will be used:

- **M** to indicate a member of the **m**anagement team
- **S** to indicate a **s**ecurity officer
- **L** to indicate a **l**ead developer

To demonstrate, if an interviewee is labeled by the following: interviewee (MSL), it means this interviewee is a member of the management team, a security officer, and a lead developer. Usually, the most important role is indicated, with the abbreviation behind it, for example: security officer (MSL), or lead developer (ML), or security officer (SL). If possible, the common role is defined, for example, if we talk about the management team, we talk about the general member of the management team (one role), the security officer (MSL) and the lead developer (ML). Furthermore, if we talk about three lead developers, and one or more of those has or have multiple roles, it is indicated as: three lead developers (ML, MSL). In other words, two of these three lead developers have multiple roles. If no abbreviation is used behind the role, then it concerns an employee with only one role. It is not necessary to indicate a developer, infrastructure or supporting staff member with an abbreviation, since all interviewees that have those roles within Cofano do not have any other roles. An overview of the roles of the interviewees is listed in table 2.2.

3.2 The Concept of Security

According to the interviewees, security is a broad concept. The interviewees mention a variety of topics when thinking of security. These topics can be visualized in a mind map, which is depicted in figure 3.1. The colors in the mind map stand for the various topics or concepts the interviewees mention during the interviews.

Figure 3.1: The concept of security: a mind map

The connection of the concepts represents the flow of one concept to the other. For example, you have the top-level concept *security*, then you have the first level concept *level of security*, and the second level concepts *training* and *education*. The second level concepts are for the benefit of the first level concept: *training* and *education* contribute to the *level of security* amongst employees.

Usually, when you talk about information security, it is about the confidentiality, integrity, and availability (CIA) of data, as indicated by a security officer (MSL) and two developers. To ensure the CIA of data, it is important to prevent and limit unauthorized access, according to the employee that handles the infrastructure of Cofano. To do so, one needs to enforce access control and implement user roles for applications, according to a developer and two members of the supporting staff. Additionally, a lead developer, two developers, a member of the supporting staff and a member of the management team think it is important that the applications, that are provided by Cofano, are secure. The lead developer and another developer indicate that you should code in such a way that your application cannot be used in another way than the intended use. The lead developer thinks, at a human level, you have to try to make an application invulnerable to social engineering. A management team member indicates that Cofano's infrastructure should be secure as well.

The three members of the management team and a developer think it is important to protect the intellectual property and most important asset of the company. In case it is a software company, the most import asset is the source code. The security officer (MSL) indicates that the company's ideas and strategies are also important, but still less important than protecting intellectual property and customer data. In addition, a member of the supporting staff, a lead developer and a member of the management team express that it is important to include an information classification scheme in the company policy, as to prevent misunderstandings about handling (confidential) information. Employees need to be aware of this, and adhere to the policy, as pointed out by a lead developer.

Security can also be about physical objects and everything that is tangible. For example, access to the office, confidential documents that are laying on desks, hardware, or the physical safety of your colleagues, according to a member of the management team and a member of the supporting staff, and two developers.

Training and education can contribute to the level of security amongst employees, pointed out by a lead developer and a developer. During such sessions, employees are instructed how applications can be kept secure, as well as how they can recognize and deal with social engineering.

3.3 Security Perception

In Cofano, there are many people with relatively good knowledge with regard to security, as pointed out by two lead developers (ML). All of the interviewees think the security within Cofano is at a (fairly) good level and they agree that a lot of time has already been invested in security. Two interviewees, a developer, and a member of the supporting staff, indicate they are not involved in security that much, and do not know where the restrictions lay. Furthermore, three interviewees - two developers and a security officer (SL) - do not name any points for improvement. However, 77% of the interviewees indicate some pain points exist. The interviewees point out the following:

- Documentation is good, but implementation and execution could be improved (three developers, supporting staff member, security officer (MSL), lead developer)
- Level of security is fairly good, but we can always do better, there is a continuous threat (management team member)
- Some pain points exist with regard to security, but people are (actively) working on improving those (infrastructure member)
- Workload before the audit is high, instead of spread throughout the year (security officer (MSL) and lead developer (ML))

In the past, internal audits, PC checks, pentests and a social engineering test have been done (security officer (SL), management team, a lead developer, two developers). Furthermore, it is difficult to bypass the digital security from the outside: Cofano has a good configuration which is set up and limited well, according to the infrastructure team and a developer. Additionally, a developer states that two-factor authentication is used in many applications, and a VPN exists that you can connect to if you work from home. The security officer (MSL) points out that, although Cofano has a good configuration, people should still be aware of the possibility of an attack. He indicates that with the acquisition of larger customers, Cofano might become more interesting to hack, so they should be wary of that and have to stay alert. In addition, according to a lead developer, social engineering is one of the most underestimated attack vectors which might pose as a risk for Cofano, even though all employees think it is unlikely to happen to them.

Cofano uses the ISO 27001 standard as input for the minimum requirements for their Information Security Management System, according to a member of the management team. A security officer (SL) describes how a few years ago, they

decided to obtain the ISO 27001 certification to help them properly organize and manage information security. A developer indicates that for the purpose of the certification, a security team has been created that actively deals with incidents, makes policy, and performs security checks and tests (for example phishing email tests). Annually, Cofano is audited in order to maintain the ISO 27001 certification. A security officer (SL) points out how the yearly audit forced Cofano to explicitly take a closer look at all matters that involved security. As a result, issues are identified and tackled that would have been overlooked otherwise. Currently, time is invested in security to maintain the ISO 27001 certification. These investments are made especially around the time of the annual audit, as mentioned by a lead developer (ML) and a security officer (MSL). However, it could be taken more seriously: time should be invested in security because it is important and fits the goals of the company, instead of it only being invested to maintain certified, as these two interviewees point out.

Although security on paper and in policy is good, the implementation is less well organized, as listed before in the pain points. A few people think it should be arranged better, especially with regard to handling customer data. For example, a new employee has access to a backup of a customer database immediately after being hired, as pointed out by two developers. In addition, dealing with assets like work laptops could be improved, according to a lead developer. A developer points out how Cofano would rather deliver new features for their software than follow extensive procedures which require a lot of extra work. In other words, the implementation part is rushed, and little time is taken to follow the procedure. For example, reporting and following-up issues could be improved, as mentioned by the security officer (MSL) and lead developer (ML). Currently, security seems like a trade-off for new functionality, whereas this should not be the case. Security is an important aspect of new functionality as well, a security officer (MSL) points out. Furthermore, a member of the management team describes how Cofano tries to comply with the policy, but also tries to improve continuously.

3.4 Perceived Goals of the Company

For Cofano, two important goals exist. The first goal is protecting source code, as indicated by a member of the supporting staff and a member of the management team. The second goal is protecting customer data, according to more than half of the interviewees. Customer data should be handled carefully. To achieve that, the software that is offered to customers should be secure and data breaches should be avoided. Cofano should be able to deliver service to their customers as complete, safe, and secure as possible, as pointed out by a lead developer (ML).

Next to that, a goal of Cofano is to improve the security awareness and knowledge amongst the employees, according to the security officer (MSL) and two lead developers (ML). The lead developers indicate that employees should be aware of standard exploits and should have sufficient knowledge to carry out their assigned tasks. One lead developer says that the security team should inform employees about why security is important and what the effects could be if nothing is done about security. That way, the security team can achieve that people are willing to do it voluntarily instead of seeing security as an obstruction for their daily jobs, according to that lead developer and the security officer (MSL). Currently, the security team still has to correct or steer issues, as told by the security officer (MSL). The security officer (MSL) and a lead developer (ML) thinks that another goal of the company is to relieve the security team from some of their duties. They think it should be possible to spread the security load should more evenly amongst all employees if the employees are willing to engage in security activities voluntarily.

3.5 The Concept of Security Awareness

The term already suggests it, as many participants noted during the interview: security awareness means that you are aware of security. According to a developer, being aware indicates that you have general knowledge about attack vectors: you know how to recognize an attack and you are aware what you can do to prevent such an attack. In addition, you have an idea of what good security is and what should be secured, are aware of vulnerabilities and restrictions of software and know where possible leaks or breaches can occur, according to more than half of the interviewees. Furthermore, you know and can apply methods to guarantee the security of applications and processes, as pointed out by the member of the infrastructure team. Moreover, you are aware of the policy, standards, and procedures with regard to security. In addition, you also understand why the company has these and know how to apply them, as mentioned by the security officer (MSL). This security officer (MSL) and a lead developer state that, when you understand why certain rules and procedures exist, and take into account the possible consequences voluntarily during your daily job, then you have achieved security awareness.

3.6 Security Awareness Perception

Employees of Cofano perceive security awareness in various ways. In figure 3.2, it is depicted what concepts interviewees mention when they talk about their perception

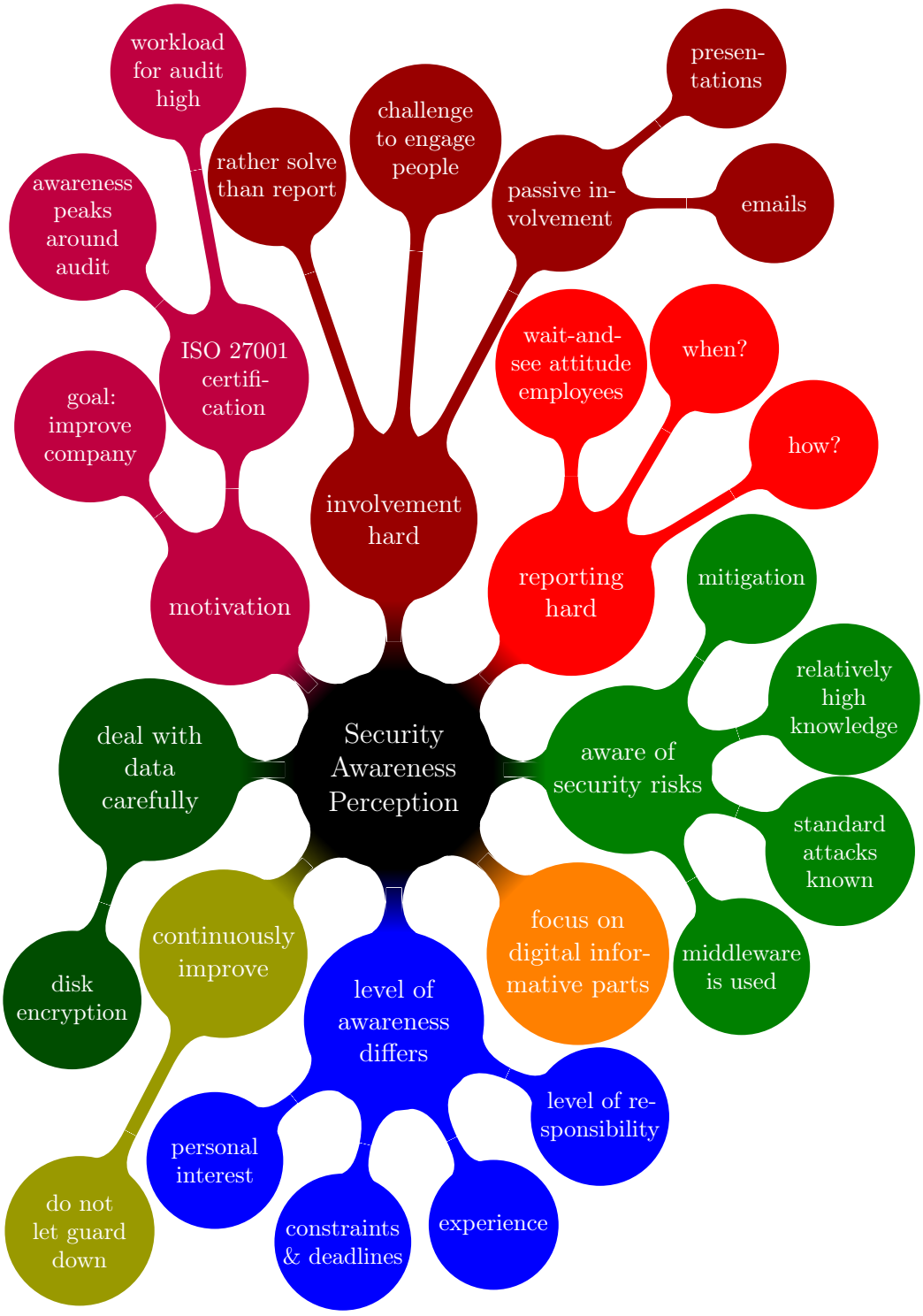

Figure 3.2: Security awareness perception: a mind map

of the security awareness within Cofano. The colors in the mind map stand for the various concepts the interviewees mention during the interviews. The connection of the concepts represents the flow of one concept to the other. For example, you have the top-level concept *security awareness perception*, then you have the first level concept *deal with data carefully*, and the second level concept *disk encryption*. The second level concept is an aid for the first level concept: *disk encryption* helps employees to *deal with data carefully*.

Within Cofano, employees are aware of security risks and how to mitigate those, despite not knowing everything, according to a lead developer and a security officer (SL). They point out that the level of knowledge of developers of vulnerabilities is relatively high, and the standard attacks are considered. Additionally, a developer points out that middleware is used to mitigate such risks. Moreover, employees know data should be carefully dealt with and have to encrypt their hard drives to protect their own data, according to this developer and a member of the supporting staff.

Two lead developers (ML) explain how the employees of Cofano do not always know when Cofano wants them to report a security incident and have a wait-and-see attitude. For example, does every downtime need to be reported, or only if it is serious? But when is downtime serious? What is expected with regard to the follow-up of incidents? If the priority lies elsewhere at that time, is that a good argument or not? What do I do when someone just walks into the office? People are unsure when to report an incident, or when to act on something, as pointed out by the lead developer (ML). In addition, it is hard to make a report as many uncertainties exist about how to report it, making the threshold for reporting an incident too high. As a result, an incident is not always reported. For example, the possibility of a stranger being into the office for some time without anyone acting on it, is high, as indicated by a member of the supporting staff and three developers. One developer points out how, currently, the focus is on the security of the digital informative parts such as code, and not the physical parts such as office access control. All of these employees work at the location in Enschede. None of the employees that work at the location in Sliedrecht have mentioned any access control difficulties. For Enschede, this problem will be mitigated soon by moving to a new office and introducing a form of access control, so visitors can no longer walk inside the Cofano office, unannounced.

Although security awareness is present and every employee has read and is aware of the company policy, security involvement is a lot harder, as indicated by a security officer (SL) and a developer. This security officer (SL) mentions how people rather solve a problem than reporting it according to the company policy. He emphasizes

how one of the greatest challenges is to make people feel compelled to engage in the entire process. Currently, the way employees are involved in security is passive. For example, they receive presentations or read emails about changes regarding security, but they are not actively involved in the entire process, according to one of the developers. In addition, not everyone is at the same level of security awareness, as pointed out by two members of the management team (MSL), a member of the supporting staff and a developer. The member of the supporting staff thinks this level differs per person and depends on the level of responsibility and experience of the employee. It might even depend on time constraints and deadlines sometimes, according to a developer. Some people are very aware because the subject interests them and they think it is important, according to a security officer (MSL) and a lead developer. Other people have a wait-and-see attitude: they will only act if the security team instructs them to do so.

The management team describes how around the time of the ISO 27001 audit, security awareness peaks and the workload is high for the security team. This indicates a change is needed, as good results in the audit might provide a false sense of security if not enough attention is paid to it outside the audit the rest of the year. Originally, Cofano engaged in security because of the ISO 27001 certification. However, Cofano should also engage in security as to improve the company, and not purely do it for the certification, as pointed out by a lead developer (ML). A lot of attention has been paid to the subject of security awareness, and many employees think that the level of security awareness is at least reasonable. Nevertheless, Cofano should be continuously working on improving it and cannot let their guard down, according to a member of the management team.

Additionally, a member from the infrastructure team points out how Cofano is not immune to social engineering. This is a small, but significant enough attack vector.

3.7 Security Awareness Importance

All employees agree that security awareness is important, and the management team indicates that it should play a role in the core values of the company. A member of the supporting staff and two developers point out that business continuity is one of the reasons why it is so important. The consequences of not having security awareness are major. In the worst case, it might even result in the company having to shut down, according to a member of the supporting staff and a developer. In addition, a lead developer (ML), a developer, a security officer (MSL) and a member of the supporting staff point out that customers trust Cofano with

their data, process and company, meaning they should carefully deal with this information. Moreover, Cofano wants to deliver a high-quality product, for which security awareness is also important, according to a member of the supporting staff and two members of the management team (ML). Security awareness is important as it provides insight into how data can be leaked, according to a developer, allowing for the protection of sensitive information and delivering a high-quality product.

A member from the infrastructure team, a security officer (MSL) and a developer point out that security awareness ensures that people know what to take into account and how to prevent and deal with incidents. If an incident occurs, they know where to report it and how to correctly report it. Without awareness, there is a higher chance something will go wrong, according to a developer. A lead developer points out how an important part of security awareness is showing people why it is useful. One can do so by showing practical examples to these people. As a result, they will feel more engaged and will no longer do it with reluctance. Although security awareness is important, it should not obstruct the daily routine or work of the employee, as pointed out by the previous lead developer and another developer.

3.8 Obtaining Security Awareness

During the interviews, employees of Cofano described the ways in which Cofano tried to create security awareness within the organization. These thoughts are visualized in a mind map, which is depicted in figure 3.3. The colors in the mind map stand for the various concepts the interviewees mention during the interviews. The connection of the concepts represents the flow of one concept to the other. For example, you have the top-level concept *obtaining security awareness*, then you have the first level concept *goal*, and the second level concepts *involvement variety of employees* and *no extra preparation needed for audit*. The second level concepts are more concrete forms of the first level concept: the *goal* is the *involvement of a variety of employees* and that *no extra preparation is needed for the audit*.

Within Cofano, security awareness was obtained through several information mediums. After it was announced that Cofano would get audited in order to get ISO 27001 certification, presentations were held about ISO 27001 and what it entailed, according to a security officer (MSL) and three developers. An Information Security Management System was set-up according to the requirements from ISO 27001. Respectively, policy was created with regard to information security and information security awareness, as pointed out by the management team, a lead developer

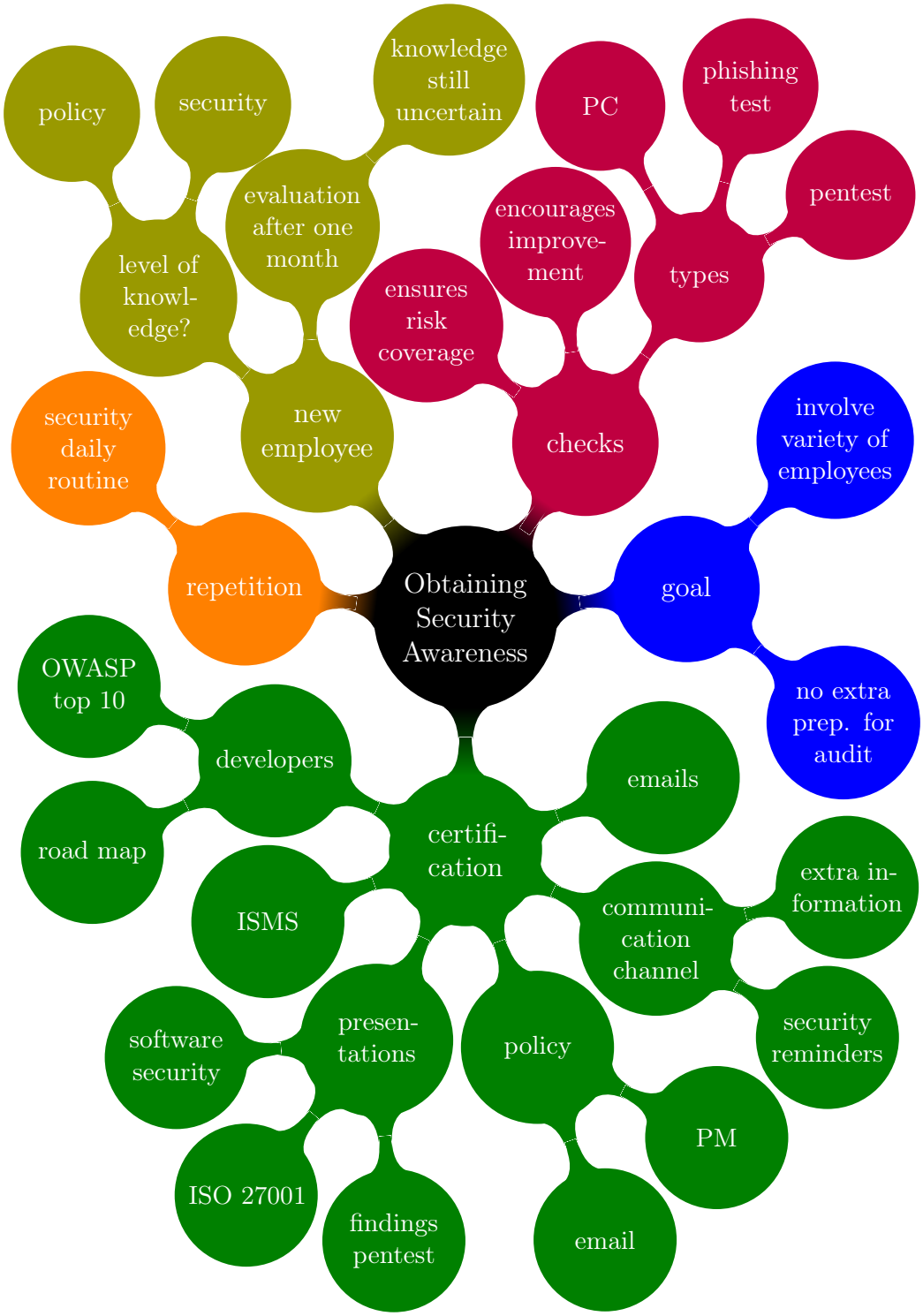

Figure 3.3: Obtaining security awareness: a mind map

and a developer. In the policy, some house rules were stated, such as the need to lock a PC whenever leaving a desk. A developer mentions that the policy also includes having a clean desk and having to anonymize customer databases.

The security officer (MSL) describes how the policy documents were registered in Cofano's Process Manager (PM), and were emailed to every employee. All employees pointed out that additional presentations were held about software security, which pointed out known problems and solutions. In addition, presentations were given that indicated the findings of the pentests done at Cofano. A lead developer and three developers point out how each developer received a list with the OWASP top 10 web application security risks and a road map on the procedure of developing software. Additionally, emails were sent out informing the employees about the changes with regard to security, which is mentioned by all employees. Moreover, the communication channel of the company was used to provide extra information about security awareness within the company, as indicated by a member of the supporting staff. In addition, this employee mentions how the communication channel also showed reminders when the PCs would need to be updated.

Although every new employee receives and reads all documents with regard to the company security and policy, a supporting staff member and two lead developers (ML) wonder how quickly this knowledge fades after. After reading all documentation, it is still questionable if the new employee immediately has the same level of knowledge about the policy and security within Cofano in comparison to other employees. Currently, after one month, new employees get an evaluation in which they are asked if they read the documents and if they remember anything, according to the lead developer (ML). They can say they did read the documents and that they remember the contents, but their knowledge about it is still uncertain.

The supporting staff, a lead developer, and a security officer (MSL) indicate that repetition is an important part of not only obtaining, but also maintaining security awareness. A supporting staff member thinks that every few months, a repetition session with regard to security awareness should take place so that people stay focused. Currently, some things are repeated, but repetition is not done regularly. A member of the management team points out that some employees are pro-active on the area of security and share information and articles whenever they can. Nevertheless, the security awareness cannot be high enough and should be part of the daily routine. Additionally, the last opinion is shared by a lead developer and a security officer (MSL), as they think including security awareness in the daily routine is a good idea.

Not only the security team, but also a member of the supporting staff, a lead

developer and three developers state that is also important to do checks every now and then. These checks are carried out by the security team. A security officer (SL) describes how a check ensures that all risks are covered, and if not, it encourages improvement. Within Cofano, checks have been done on PCs, for example to check if the disk is still encrypted, if security updates are done regularly and if there is no unlicensed software installed on the PC, as indicated by several interviewees. Additionally, a phishing test has been carried out to find out how vulnerable employees were to social engineering. Moreover, developers mention that pentesting is done to see if any vulnerabilities can be identified in the applications of Cofano. Accordingly, presentations were given, or emails were written to show the results of these tests, and how it can be improved. A security officer (MSL) describes how it is always easier to make people aware of something if you can support it with practical examples in which people themselves had a share in.

Currently, only the security team and management team are involved in the audit for the ISO 27001 certification. The security team is trying to get more variety in the people that are involved in the audit. Each year, the audit forces Cofano to take a good look at the security of their company again, which several employees think is useful. However, the management team thinks that is not the most ideal situation. They indicate that an audit should be possible every day of the year, and Cofano should be able to pass it without extra preparation. Additionally, a lead developer thinks that the security team could give more internal presentations about how security is currently dealt with. In this presentation, the security team could describe the findings and action points from the ISO 27001 audit.

3.9 Security Awareness Involvement

Most employees of Cofano indicate that they are involved in security awareness purely on individual level. In other words, they are not actively involved in creating security awareness for Cofano, but they try to keep an eye on security and keep themselves informed. In addition, the developers perform code reviews. Moreover, some developers perform pentests. Supporting staff deals with sharing login details while trying to keep security in mind and informing new employees about policy and procedures with regard to security. In general, all employees participate in everything Cofano does to improve security awareness.

The employees that are part of the security team are the most involved in security awareness. These employees motivate security awareness within the company, organize awareness sessions and presentations and roll out improvements. In general, they try to be a figurehead with regard to security. Next, part of the

management team is responsible for the security awareness of the employees of the location Enschede. In addition, the management team has to be able to answer questions from customers about Cofano's security and holds quarterly meetings about the security within Cofano. Furthermore, some of the lead developers are responsible for internal IT. These lead developers check if new employees have encrypted their hard drive, and provide security advice to employees, for example about strong passwords. In the field of developing, if they notice mistakes, they try to explain why it is wrong so the employee can do better next time.

3.10 Personal Goals Security Awareness

The employees of Cofano have not given goals on the area of security awareness much thought, because the employees do not have security related goals as part of their job description and duties. Two employees do not have any goals on the area of security awareness at all. About 40% of the interviewees want to keep their knowledge up-to-date with the latest security issues and potential attack techniques. In addition, they think it is important to be aware of what you are doing and if security can be guaranteed, especially when they are working on something security related. For example, a developer mentions that during software development libraries are used, which can have exploits if they are not used in the right way. Furthermore, a member of the supporting staff points out that continuing to stress that information needs to be handled carefully and shared in the right way matters. A lead developer mentions that if improvements are possible, they are shared with the security team. Most developers think it is sufficient that only the security team deals with security issues. Some employees are pro-active and indicate that they are interested in learning more about security with regard to developing. A few employees want to help spread and explain information about security awareness.

One of the goals of the management team is that Cofano does not only do security for the ISO 27001 certification, but that every employee has a high personal responsibility, and is always aware what they are doing. In addition, they should try to do it as secure as possible and work on continuous improvement, as security is an important theme in software development. The management team indicates how security should be seen as part of the quality of the software, instead of as an obstruction.

One of the goals of the security team is that people understand why security is so important, why Cofano has a policy and certain regulations. In an ideal situation, the employees are able to combine this with their daily job and notice possible

improvements. The security team thinks it would be great if other employees are a step ahead of them.

3.11 Security Awareness Problems

Opinions about the problems of security awareness are divided. Currently, most interviewees, about 62 %, think that there is nothing that is really problematic on the area of security awareness as everyone adheres to the rules. This opinion is mainly shared by employees that are involved in security awareness on an individual level only. However, they think Cofano can do better. Continuous attention needs to be paid to the subject of security, and tests such as phishing emails need to be done to see if everyone is alert. Usually, people overestimate themselves and think they will not get phished or are not vulnerable to social engineering. Therefore, social engineering is one of the highest risks, according to a lead developer and a member from the infrastructure team. A member of the supporting staff points out that the more Cofano grows, the more vulnerable they will be to attacks. Therefore, the aforementioned employees think that social engineering will need more attention within Cofano.

A developer and a member of the infrastructure team think that the introduction that new employees get, is not sufficient. Over time, they receive enough information to get in line with the security practices at Cofano. However, the intake that new employees get could be improved in such a way that they are fully aware of Cofano's security practices from the start. A new employee manual has already been created that contributes to the improvement of this process.

Another problem, according to a developer, is the exchange of customer information. Currently, this data is not always shared over the right channels which are included in the information security policy. The developer indicates how this problem can easily be fixed by sending all employees an email explaining the right way of sharing data.

Additionally, the interviewees mention that the security awareness of employees subsides at some point, whereas this should not be the case. Several steps could be taken to prevent this. Employees have suggested the following in order to pay constant attention to the subject:

- Monthly reminder like newsletter
- Email with most frequent and latest attacks
- Education/repetition every few months, especially for new people
- Testing knowledge and awareness of employees every few months through

various methods
- Making security awareness an interactive challenge

Furthermore, the security officer (MSL) mentions how the level of security is different for each member of the management team. All members think it is important, but not all members are actively involved in its implementation. For some members, the business, selling the software and delivering new functionality has a higher priority than security.

Moreover, what is problematic is that people see security as a lot of work and hassle, according to a lead developer (ML). For example, security incidents are followed-up accordingly, but the administration of these incidents is neglected, whereas this is an important requirement for improvement. Additionally, it aids in the prevention of such an incident, so that it will not happen again. Employees of Cofano like the practical side, whereas the administrative side is often ignored. In addition, this lead developer (ML) and a member of the infrastructure team describes how the current processes for reporting and solving problems are hard to find in the Process Manager (PM) of Cofano, making the threshold for people to report an incident high if they have never done so before.

Furthermore, a security officer (MSL) and lead developer (ML) indicate a peak of security awareness exists around the audit, reflected in the number of issues that are reported during this time. The number of reported issues is considerably higher compared to the number of reported issues in the rest of the year. A member of the management team mentions that, as Cofano continues to grow, there will be room for a dedicated cyber security function.

With regard to the highest priority, interviewees think it is important that employees are continuously engaged in security. Additionally, they think people should be aware of the latest developments and that education on security should be repeated. The security team thinks it is a priority that security is not only the responsibility of the security team, but a responsibility of all employees. They do no longer want to chase people to do it. In addition, attention has to be paid to all fronts with regard to security, not only the technical ones, but also the social ones.

3.12 Security Awareness Challenges

The security officer (SL) indicates that social engineering could be a challenge. Next to that, large changes within the company could also be a challenge. Cofano split up six months ago, which they were not as prepared for as they had thought with regard to security. In the annual audit, the split came up, and the auditor

wanted to know if Cofano had checked whether any data or hardware was taken by the other company. Consequently, Cofano has taken appropriate action to mitigate this challenge. Another challenge is the administration process which revolves around the move of the Cofano location Enschede. Usually, moving is a matter of packing things and relocating them from A to B, but in terms of security, the consequences of relocating have to be identified. You have to think about the consequences for the current location and the consequences for the new location. Additionally, you have to consider things like:

- Safely move hardware
- Secure the new location
- Arranging a new secure internet connection
- Arranging an internet backup line

The security team has to invest some time into that, otherwise they could get into trouble during the next audit. The auditor will want Cofano to show they carefully handled the relocation, since the situation has changed. There is a new building, new access roads, new companies next to Cofano, so they have to check whether their information security is in order.

According to a developer, another challenge is the readability of the documentation of Cofano. From a technical point of view, Cofano documented everything well, only it is hard to find and difficult to read. The developer points out the processes could be improved by making the documentation easier to find and understand. With one glance, you should be able to comprehend what it is about, instead of having to read a few pages documentation. The information is present, and it is clear and concrete, but the transfer rate is a challenge.

Two developers are not aware of any challenges within Cofano. This might not only be the case because of their low level of involvement in security awareness, but also because they feel the security team solves any challenges with regard to security.

Moreover, making time for security awareness will always be a challenge, according to a lead developer. Furthermore, he questions if it is possible to make everyone completely aware of security. He thinks you have to find at point at which you are satisfied with the level of awareness, because the costs are exponential compared to the amount of security awareness.

Continuously keeping security in the back of your mind proves to be difficult, according to a member of the management team, a member of the supporting staff and a lead developer. This lead developer mentions that the workload of the

tasks of the employees is already sufficient enough to fill all working hours. In addition, according to the security officer (MSL) and two lead developers (ML), security should not be seen as an obstruction and extra workload, but as something which contributes to the quality of the software. However, a lead developer (ML) indicates that Cofano is not the right company for many formal processes and obligations, so it is a challenge to motivate people to engage in security awareness. The security officer (MSL) mentions that although a company policy exists, people do not always adhere to it. He adds that it is a challenge to educate smart people about security topics they might already have sufficient knowledge of. In addition, security knowledge fades after a while, therefore repetition is important, as a member of the supporting staff points out.

An ongoing challenge is to keep developing software in a secure way. A developer suggests that as the company grows and acquires reputation, it might be more interesting to hack. Therefore, it is increasingly challenging to keep web applications safe and secure. Accordingly, checks and tests should be done regularly, so Cofano does not let their guard down, as pointed out by a member of the management team. Currently, with the Coronavirus disease, more and more people work from home. As a result, working from home needs to be integrated in the policy, which could be challenging, according to a developer.

According to the management team, security awareness is an increasingly important subject, especially with the increasing digitization and Cofano's acquisition of larger customers. Cofano needs to pay constant attention to security awareness, in order for it to stay at the same level, particularly when working with new customers. A member of the supporting staff that is concerned with sales indicates how the difference between Cofano's various customers is large. One customer might be constantly engaged in security, whereas the other customer shows no interest in the subject at all. Despite these differences, Cofano has to treat both customers the same with regard to security, as they think it is important. However, the way it is handled entirely depends on the kind of customer and kind of data, according to a member of the supporting staff.

Many challenges Cofano encounters on the area of security and security awareness are reported, according to the management team and two developers. Consequently, measures are taken to mitigate or resolve these challenges. Additionally, changes will be implemented in the policy whenever needed, as pointed out by the security officer (MSL). Moreover, challenges are resolved by investing time and paying constant attention to the subject, as well as encouraging people to discuss and implement improvements, according to two lead developers (ML) and the security team. Furthermore, a security officer (SL) mentions that the way presentations

were given on the subject of security awareness, was improved.

A security officer (MSL) thinks a shortcoming in the way Cofano deals with challenges is that it is reactive: something has to go wrong before anything is done about it. In addition, the findings from the security team are not always exposed Cofano-wide, so employees do not learn from them, as pointed out by a lead developer. In addition, challenges with the security level of customers are not always easy to handle according to policy, as described by a member of the supporting staff. Consequently, they are resolved according to feeling. Finally, there is always the shortcoming of capacity, time, and money, which is mentioned by the management team as well as a lead developer.

3.13 Not Addressing Security Awareness

All employees of Cofano agree with each other that not addressing security awareness could be troublesome for the future of the company. If security awareness is not addressed, the consequences might be disastrous for the business continuity, as indicated by almost 40% of the interviewees.

As a result of not addressing security awareness, people will have less knowledge (two developers) on the subject of security, become lax (infrastructure member) and the level of security will deteriorate (about 40% of interviewees). A lead developer (ML) mentions that prior to the annual audit a high workload will continue to exist. In addition, the all security-related matters will still be the responsibility of the security team, instead that everyone feels responsible and the workload is spread more evenly. Eventually, not addressing security awareness could cause problems with the audit. Moreover, Cofano could lose its certification, as pointed out by part of the management team (MSL) and a member of the supporting staff. In addition, people with malicious intent could gain (unauthorized) access to the applications of Cofano (security officer (SL)), and data leaks will arise (developer, member of supporting staff, member of infrastructure). Hence, Cofano will have loss of face, which could lead to great financial losses, according to a member of the supporting staff and a member of the infrastructure team.

3.14 General Remarks of Participants

Throughout the interview, participants made some remarks. The points that were identified are categorized based on the interview question during which it was mentioned and can be found in table 3.1.

Category	Remarks
Company Goals	• Cofano reduces risks based on trust in employees: they thoroughly look at risks from the outside, but they trust everyone on the inside • It is good to ensure everyone has sufficient knowledge about security
Security Awareness	• It is a challenge to make people feel involved in security awareness • Many employees have a wait-and-see attitude • We need to be alert constantly - the consequences can be severe, especially for customers • In practice, policy is ignored when it is inconvenient
Obtaining	• Security team could present findings more often: communication is key in the entire process • Knowing where to find policy is not enough; you need to know the applicability of it • Put a list of security tips in a convenient place - like on the fridge, so you get confronted with it often • Documents are hard to find through the Process Manager, distribute them elsewhere too
Personal Goals	• No work from home policy yet

Problems	• Monthly reminder like newsletter or email with security hacks / points / improvements • Security team deals with security - not much is asked of employees • Education on security and security awareness should be done more often: the more you know, the easier it is to prevent and report • Information exchange is sometimes done through the wrong mediums - can easily be improved • Theoretical knowledge of security awareness should be tested in practice • Every once in a while, there should be a security talk with the team • Keeping knowledge up-to-date is important - people should be aware of the latest developments with regard to security
Challenges	• Security knowledge fades, therefore, repetition is important • Documentation is good, but could be improved to make it more comprehensible

Table 3.1: General remarks of participants during the interviews

3.15 Extracted Improvement Possibilities

From the conducted interviews, improvement possibilities can be extracted. The points of improvements are listed in the tables below and are also visualized. The category in which they are listed is based on the previous sections. Some sections are left out as categories, since no improvements could be extracted from these sections, simply because none were mentioned during the interview. The mapping of the previous sections to the improvement categories, figures, and tables can be found in table 3.2. As can be seen from the table, section 3.6 and section 3.7, and section 3.8 and section 3.9 are merged into Security Awareness and Obtaining, respectively. The sections were merged into those categories because on their own, they were small, and they were similar enough to merge into the other category.

The improvements possibilities will be used to propose a solution for treating Cofano's problem.

Section	**Category**	**Fig**	**Table**
3.2 The Concept of Security	-	-	-
3.3 Security Perception	Security	3.4	3.3
3.4 Perceived Goals Company	Company Goals	3.5	3.4
3.5 The Concept of Security Awareness	-	-	-
3.6 Security Awareness Perception	Security Awareness	3.6	3.5
3.7 Security Awareness Importance	Security Awareness	3.6	3.5
3.8 Obtaining Security Awareness	Obtaining	3.7	3.6
3.9 Security Awareness Involvement	Obtaining	3.7	3.6
3.10 Personal Goals Security Awareness	Personal Goals	3.8	3.7
3.11 Security Awareness Problems	Problems	3.9	3.8
3.12 Security Awareness Challenges	Challenges	3.10	3.9
3.13 Not Addressing Security Awareness	-	-	-

Table 3.2: Sections and their improvement categories, figures, and tables

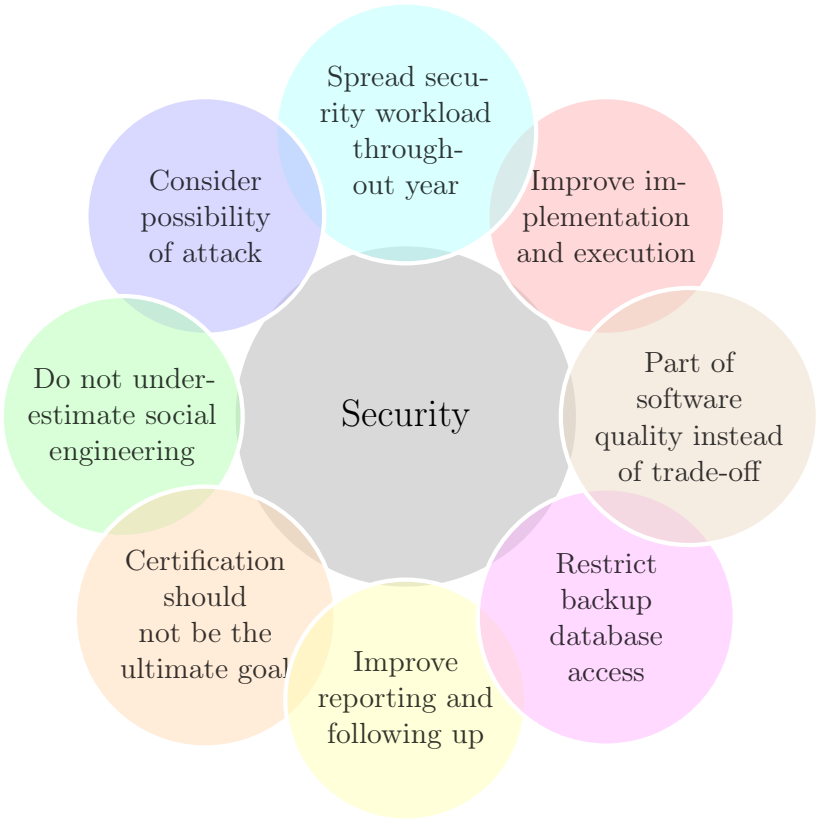

Figure 3.4: Improvement points security

Category	Improvement points
Security	• Documentation is good, but implementation and execution could be improved • Workload before the ISO 27001 audit is high, instead of spread throughout the year • Possibility of attack should be considered more with acquisition of larger customers • Social engineering is underestimated; could pose as a risk • Security should be the ultimate goal instead of ISO 27001 certification • Access of new employees to backup customer databases should be restricted • Reporting and following up security issues should be improved • Security should not be a trade-off for new functionality, it should be seen as part of the quality of the software

Table 3.3: Improvement points security

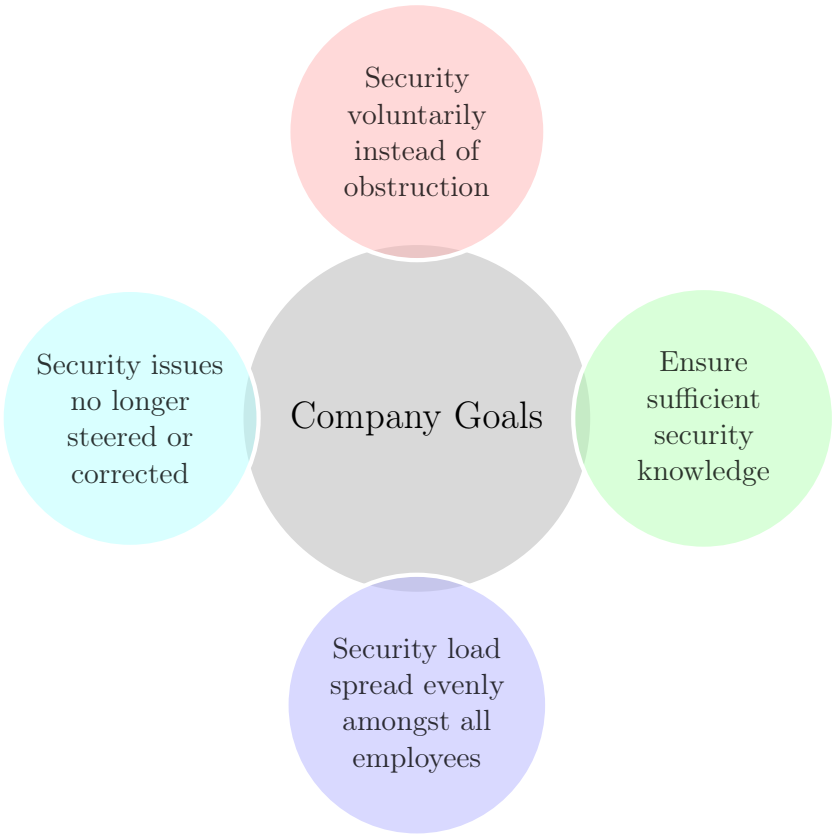

Figure 3.5: Improvement points company goals

Category	**Improvement points**
Company Goals	• It should be achieved that people are willing to do it voluntarily instead of seeing security as an obstruction for their daily jobs • Security issues should no longer have to be steered or corrected • Security load should be spread more evenly amongst all employees • It is good to ensure everyone has sufficient knowledge about security

Table 3.4: Improvement points company goals

Figure 3.6: Improvement points security awareness

Category	Improvement points
Security Awareness	• It should be clearer when to report a security incident • It should be easier to report a security incident • The wait-and-see attitude of employees should be turned around: people should feel compelled to engage in the entire security process • Employees should not only have security awareness; security involvement is the next step • Security awareness should not only peak around the audit, but should always be present • The high workload indicates a change is needed • Cofano should engage in security to improve the company and not only for the ISO 2001 certification • The level of security awareness should be continuously improved • Cofano should be more resistant against social engineering

Table 3.5: Improvement points security awareness

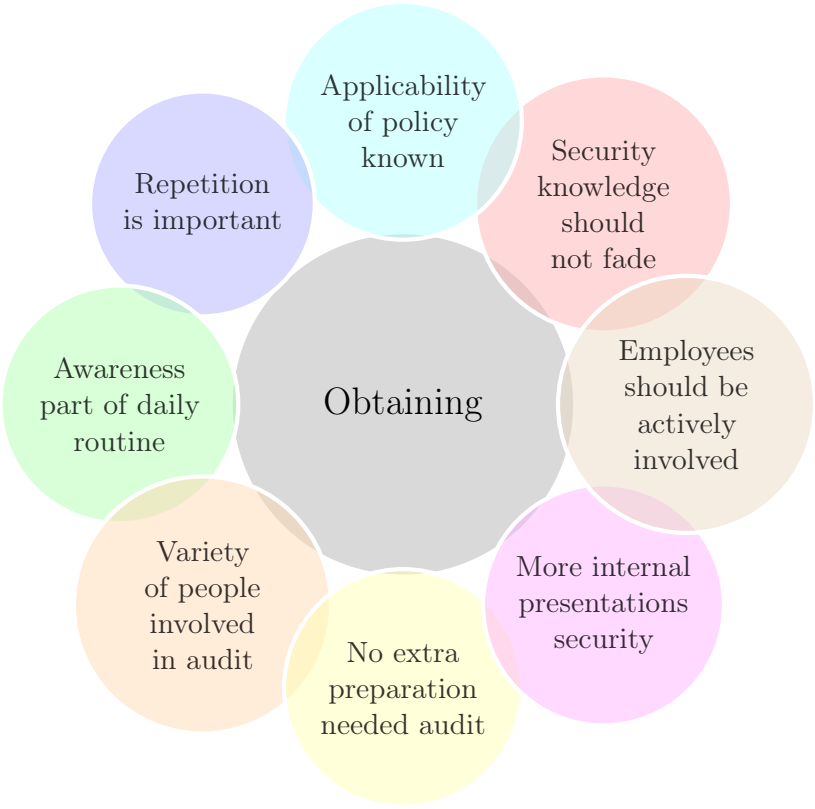

Figure 3.7: Improvement points obtaining

Category	Improvement points
Obtaining	• It should be ensured that security knowledge of (new) employees does not fade quickly after reading documents • Knowing where to find policy is not enough; you need to know the applicability of it • Repetition is important, information with regard to security should be repeated more often / regularly • Security awareness should be part of the daily routine • There should be more variety in the people involved in the audit • An audit should always have the same results (be passed without extra preparation), no matter when it is conducted • More internal presentation could be given about current security status / findings / actions points audit • Employees should be actively involved

Table 3.6: Improvement points obtaining

Figure 3.8: Improvement points personal goals

Category	Improvement points
Personal Goals	• Security awareness should not only be done for ISO 27001 certification • Every employee should have a high personal responsibility • Every employee should be aware of what they are doing with regard to security • Security should be part of the quality of the software instead of an obstruction • Employees should understand why security awareness is so important and should be able to combine this with their daily job

Table 3.7: Improvement points personal goals

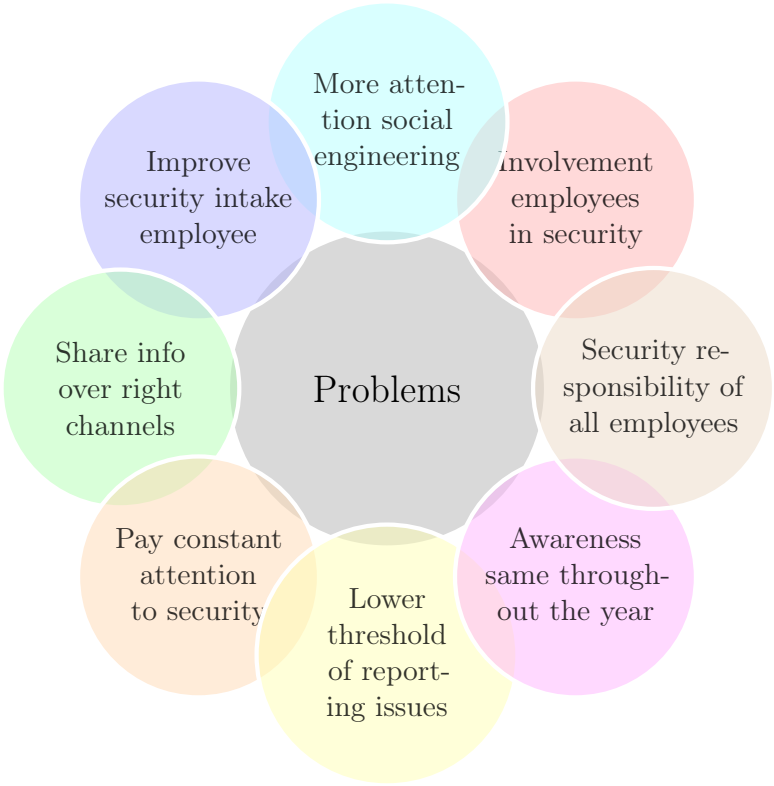

Figure 3.9: Improvement points problems

Category	Improvement points
Problems	• Employees should be involved in security company-wide instead of only on an individual level • Social engineering will need more attention; Cofano needs to keep doing tests and checks • Security intake new employees should be improved further • Information should be shared over the right channels • Security awareness subsides, constant attention should be paid to the subject, for example through monthly reminders, emails, repeated education, and tests • Threshold of reporting security issues should be lowered • Security awareness should not only peak around the annual audit; it should be the same throughout the year • Employees should be constantly engaged in security: security should be the responsibility of all employees, not only that of the security team

Table 3.8: Improvement points problems

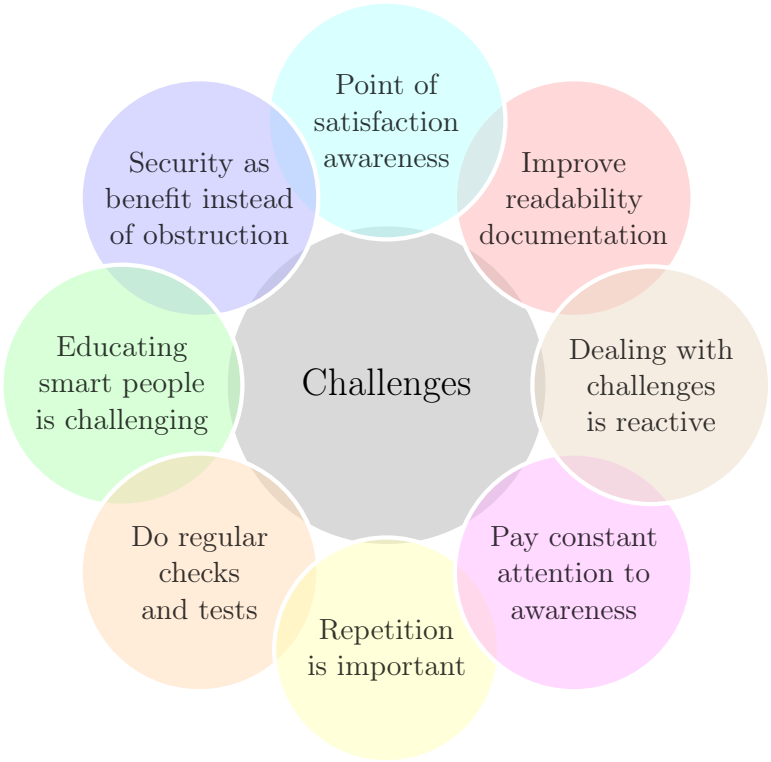

Figure 3.10: Improvement points challenges

Category	Improvement points
Challenges	• Readability of (security) documentation could be improved: you should be able to comprehend what it is about with one glance • Making time for security awareness is a challenge, there should be a point at which you are satisfied with the amount of awareness • Security should be seen as a benefit and contribution to the quality of the software, it should not be seen as an obstruction or extra workload • Educating smart people proves to be a challenge • Repetition is important, since security knowledge fades after a while • Checks and tests should be done regularly to check for vulnerabilities • Constant attention needs to be paid to security awareness for it to stay at the same level • Dealing with challenges is reactive: something has to go wrong first

Table 3.9: Improvement points challenges

3.16 Discussion on Validity

Before discussing validity threats, it is worthwhile noting that our qualitative research related to the problem investigation, in fact achieved theoretical saturation of the qualitative data. The concept of "saturation" is defined by qualitative research methodologists [25, 9, 27, 15] as the state of the research process in which the action of sampling more data (i.e. interviewing more people) would not lead to more information related to their research questions and to the answers that were found already. The researchers recognize that they arrived at this point when interviewing more practitioners did not bring any new aspects of the already defined categories in the qualitative data analysis. In other words, the researchers see very similar pieces of information or instances of the already known categories in their interview data over and over again. At this point, one could say that the categories resulting from the analysis are "saturated", and researchers are allowed to stop sampling data and can round off their analysis. However, in this thesis we acknowledge that there are no explicitly stated guidelines for determining the point at which saturation is reached. Therefore, researchers have to support their claims of saturation by an explanation of how they achieved saturation, including clear evidence. After the eleventh interview, we started hearing things repetitively, like accessibility to backup customer databases, keeping customer data safe, disk encryption, presentations to improve security awareness, the importance of repetition, the low involvement of employees in security awareness and how constant attention should be paid to the subject of security awareness. After hearing these concepts in the interviews repetitively, the researchers recognized that they arrived at a point when interviewing more employees of Cofano would not bring any new aspects of the already defined categories in the qualitative data analysis.

The most important question in qualitative research is the one about the generalizability of the findings. One might wonder: would the problematic aspects resulting from the problem analysis at Cofano be observable in other companies? Following Seddon and Scheepers, we think that it might well be possible to observe our findings in companies that share the same contextual settings as those of Cofano [32]. Examples of companies that share the contextual settings of Cofano, are those operating in the same business sector, having similar business processes and supporting applications. Additionally, they have an unstructured and operational planning orientation, high flexibility, informal managerial process, limited budget for training and their competitive advantage is centered around human capital. Although universal generalizability cannot be claimed, the results are descriptive and insightful enough to come up with an artifact, which is presented in chapter 4.

Finally, a validity threat in qualitative research is the possible bias on the side of the researcher. In our case, we think that this threat is minimal, because the analysis of the researcher was constantly checked by a senior colleague working in the same organization. Moreover, the researcher had already been working at Cofano for some time, making the researcher aware of and experienced with the context of the organization. In addition, the interviewees were familiar with the researcher, meaning they felt comfortable sharing their honest opinions and thoughts with her. Furthermore, the researcher herself has a background in security, as this is her master track specialization. Her knowledge of the topic of security helped her develop theoretical sensitivity and consciousness for possibly passing bias into the analysis. Whenever she doubted the meaning of the collected pieces of data, she consulted her senior colleague on an ongoing basis. This measure assured the data analysis was de-biased as much as possible.

3.17 Summary

To summarize, in this chapter the results of the qualitative text analysis of the stakeholder interviews were presented. In addition, saturation was achieved during the interview process. Furthermore, improvement possibilities were extracted from the conducted interviews, which serve as an inspiration and foundation for the artifact in chapter 4. Finally, the mitigation of threats to the validity of the research was discussed.

Chapter 4

Proposed Solution

This chapter proposes a solution to the problem Cofano is currently experiencing. First, the available treatments that could be extracted from literature are discussed in section 4.1, as well as their application to Cofano. The available treatments aid us in identifying the current state of security awareness at Cofano. In addition, from these treatments concepts and components can be extracted regarding how to achieve a higher level of security awareness. This will be discussed in section 4.2. Section 4.3 discusses how these concepts and components contribute to the stakeholder goals. Finally, in section 4.4 the artifact that was designed based on existing literature and interviews (chapter 3) is presented.

4.1 Available Treatments

This section presents the available treatments identified in our earlier research, that could serve as candidates in the development of a framework for SMEs such as Cofano. The identification of the available treatments was done based on the systematic review of 17 selected papers for a research topics paper prior to this research. The available treatments are described in section 4.1.1 and section 4.1.3.

4.1.1 Organizational Culture and Information Security Culture Framework

From the research topics paper, a framework created by Lim et al. could be identified which could aid organizations to reach their desired level of information security culture [23]. The original framework by Lim et al. can be found in appendix

G.

According to Lim et al., three types of relationships between organizational culture (OC) and information security culture (ISC) exist:

- Type 1: ISC is separated from OC
- Type 2: ISC is a subculture of OC
- Type 3: ISC is embedded into OC

In type 1 relationship, when ISC is separated from OC, information security is not an integral part of the OC. The involvement of employees of the organization in security implementation is non-existent or low: they have little knowledge with regard to security and do not feel responsible for any issues that are security related. Security is seen as an expense and organizations struggle to obtain funding for security related activities. In addition, the security awareness amongst the employees is low and security-related activities are only initiated by the IT department instead of organization-wide.

In type 2 relationship, where ISC is a subculture of OC, the ISC of an organization consists of a mix of security subcultures. Each of these subcultures corresponds to the responsibilities and tasks of the various subgroups. Moreover, management is paying more attention to the implementation of information security practices, as well as requiring the employees to follow security training. Additionally, employees have a higher level of security awareness, but the involvement is still low: only a small amount of people is involved in the implementation of security measures. Furthermore, little coordination exists between departments with regard to handling information security within the organization.

In type 3 relationship, where ISC is embedded into OC, ISC unconsciously has become part of the daily routine of the employees. The security of the organization is the responsibility of all employees. Employees are inclined to adhere to the security policy of the organization, which is regularly updated. The level of employee involvement is relatively high, and a holistic approach is taken for the implementation of security measures.

Lim et al. point out how these three types of relationships correspond to cultural views of an organization as defined by Fitzgerald [14]. Fitzgerald define criteria to rate which cultural view (high, moderate, or low) an organization belongs to. According to Fitzgerald, the criteria are as follows:

- High
  - Information security is brought up by senior management during discussions about new projects
  - Within the organization, an information security officer is appointed at a high level
  - Information security is incorporated in all major projects
  - Individuals that are experienced in information security are involved in the design of an application
  - The board of directors of the organization receives periodic updates on information security
  - The level of security awareness is high amongst employees and they know how to report incidents
  - No major audit findings exist, and findings highlight known issues which will be addressed
  - Budget exists for an ongoing security program
  - Security is perceived as a reducer of business risk and security efforts are actively supported by the management team
- Moderate
  - Some information security training has been given to employees of the organization
  - The information security role has been assigned to an employee as suggested by the auditor
  - Security policies are primarily created within the IT department and may not have organization-wide support - employees do not know where to find the policies
  - The employees that develop the applications have security knowledge, but not all applications are always verified in each phase of development
  - The understanding of information security is delegated to the chief information officer (CIO) by senior management - they trust the CIO to handle all security-related matters correctly
  - An employee has been assigned for information security which handles the operational activities with regard to security, such as setting up accounts, resetting passwords, and arranging access to files
  - The response to the findings of an audit is reactive and motivates change and support for future security initiatives

- Low
  - Security policies do not exist, or are reactive: they are only introduced when a security incident has occurred and are usually issued by memo
  - Employees think information security is about passwords, viruses, and firewalls
  - Password sets and resets are not strong enough
  - The management team acknowledges security is important - however, it is not assigned the level of importance that it should be assigned
  - No funding exists that is specifically for information security

Since these cultural views map to the relationship types, they can be seen as a continuum ranging from ISC not being a part of OC to ISC being completely embedded into the OC. The continuum is depicted in figure 4.1. At the left of the continuum, an organization has a low cultural view, where the information security culture is not part of the organizational culture. At the middle of the continuum, an organization has a medium cultural view, where the information security culture is a subculture of the organizational culture. At the right of the continuum, an organization has a high cultural view, where the information security culture is embedded completely into the organizational culture.

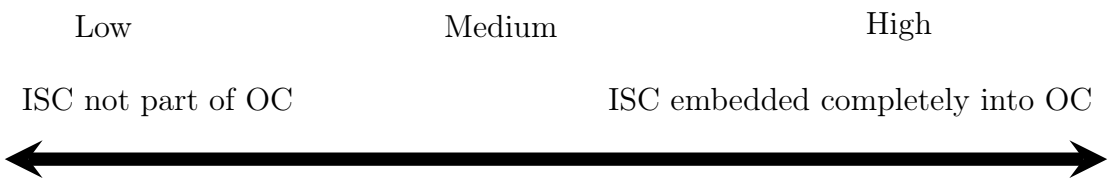

Figure 4.1: The continuum of embedding ISC in organizations [23]

4.1.2 Application to Cofano

Lim et al. have derived a framework from literature in which they list the types of relationships, the organizational culture, the actions and behaviour of the employees, and the probable consequences with regard to security. With the framework, we can determine what the type of relationship is that the information security culture has with the organizational culture within Cofano. To achieve this, we first evaluate the organization culture of Cofano. This evaluation can be found in table 4.1. Next, we compare the beliefs, actions and behaviours of employees, as can be found in table 4.2. Finally, we compare the probable consequences from the framework to those of Cofano, which can be found in table 4.3. In these tables, the first column indicates the constructs of the framework by Lim et al. under which the characteristics of

Cofano can be categorized. These characteristics are observed by the researcher and verified by a security expert of Cofano. The second column shows how Cofano deals with the categories of this construct. The third column tells the type of relationship the information security culture has with the organizational culture within of Cofano.

Construct of Organizational Culture	**Cofano**	**Type**
Management Involvement	Security matters are handled by the security team	2
Locus of Responsibility	Lead developer responsible for code team	2
Information Security Policy	Organization-wide, regularly updated	3
Education/Training	Some security awareness training is given, employees participate, but it is not compulsory	2
Budget Practice	Budget is allocated for the annual audit, there is some room for security activities within the infrastructure budget, if any more budget is needed, management can act promptly towards that	2
Result	With regard to organizational culture, Cofano falls under the type 2 relationship, where the information security culture is a subculture of the organizational culture	2

Table 4.1: Organizational culture within Cofano

Construct of Information Security Culture	**Cofano**	**Type**
Responsibility	Some employees feel responsible for security, other employees have a wait-and-see attitude and let the security team handle security matters	2
Participation	Employees are usually only involved in security on an individual level instead of organization-wide, they receive some security training, they are not always motivated to report security incidents, but do handle them	2

Commitment	Most employees leave security to the security team, they do not always feel responsible for security matters	2
Motivation	Some employees are motivated to deal with security matters	2
Awareness/Know how	Most employees know how to deal with security issues, not all employees are experienced in reporting security issues	2
Result	With regard to organizational culture, Cofano falls under the type 2 relationship, where the information security culture is a subculture of the organizational culture	2

Table 4.2: Information security culture within Cofano

Construct of Probable Consequences	**Cofano**	**Type**
Risk Vulnerability	The risk vulnerability of Cofano is low	3
Awareness	Employees are aware, but the level of awareness is not the same throughout the year, not all employees are always concerned about security matters	2
Responsibility	The security team is mainly responsible for security matters	1
Security Practices	Security is not a routine activity of all employees	1
Investment for Security Practices	There is medium cost in implementing security activities, such as the audit	2
Result	With regard to organizational culture, Cofano falls under the type 2 relationship, where the information security culture is a subculture of the organizational culture	2

Table 4.3: Probable consequences for Cofano

Based on the evaluation in table 4.1, 4.2 and 4.3, we can conclude that the information security culture of Cofano is a subculture of the organizational culture, or, as Lim et al. indicates, a type 2 relationship. According to Lim et al., organizational

culture has a significant impact on employees. Research shows that an information security culture needs to be created within an organization to improve employee behaviour with regard to organizational information security. Therefore, the ultimate goal is to have a type 3 relationship, where the information security culture of Cofano is embedded completely into their organizational culture, as to influence employee behaviour positively with regard to information security practices.

4.1.3 Information Security Competence Maturity Model

From literature, a model by Thomson and von Solms on information security competence maturity could be identified, as depicted in figure 4.2 [38]. This model is a method for evaluating the extent that information security is embedded in the corporate culture of an organization. Additionally, it indicates what steps are needed to reach a level where security controls are embedded completely into the employee behaviour and daily routine.

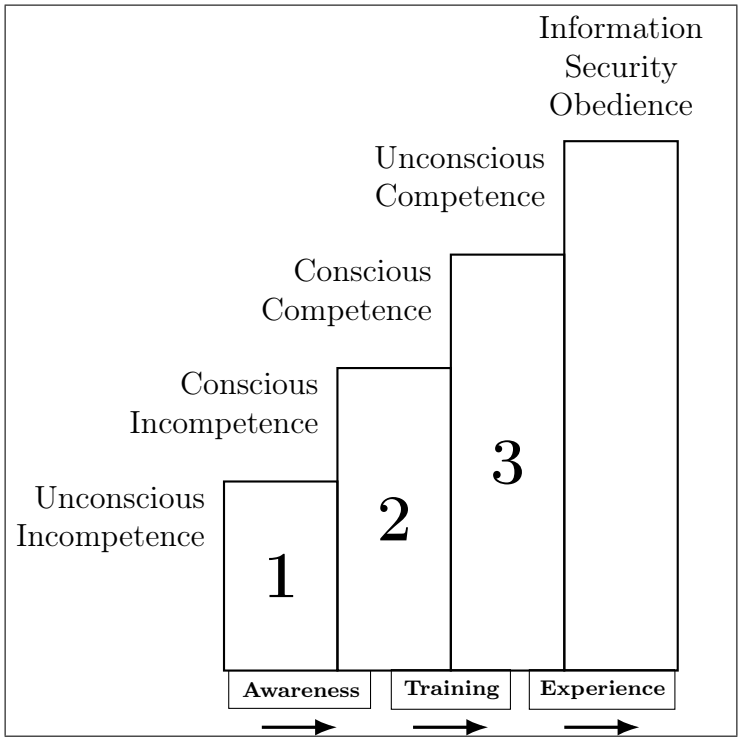

Figure 4.2: Information Security Competence Maturity Model [38]

Information security is based on people, since they have to understand the technology to be able to understand the information security problems [36]. The success of

information security practices within the company is dependent on the behaviour of employees, which is affected by the organization's corporate culture [5]. So, the corporate culture of an organization should be considered when implementing information security controls, or employee behaviour will be an obstacle in ensuring information security [24, 33].

With regard to information security, employees can become the strongest link, provided that they are well-trained. Therefore, it is important to comprehend how employees can get dedicated to and knowledgeable about their roles and responsibilities with regard to information security. Additionally, it is critical that employees follow an information security program and adjust their behaviour to the information security policy. Senior management within the organization should see to the creation, enforcement, and encouragement of the information security program through policy [16].

According to Thomson and von Solms, employees often are unconsciously incompetent with regard to information security practices. If the employee is unaware of their lack of skills with regard to information security, the employee is located at Stage 1 of the Information Security Competence Maturity Model, *Unconscious Incompetence*, as depicted in figure 4.2. The behaviour of the employees cannot be changed unless they recognize the benefits of a change in behaviour, so they can make it part of the corporate culture [29].

Employees can progress from Stage 1 to Stage 2 through following an Information Security Awareness Program. The employees merely receive instructions about information security, but do not have an active role in the program [43]. During this training, employees are made aware of possible threats to information security.

At Stage 2 of the Information Security Competence Maturity Model, *Conscious Incompetence*, employees are aware of their responsibilities and roles with regard to information security. Additionally, they understand the benefits of information security. Employees can go from Stage 2 to Stage 3 through following Information Security Training. During this training, employees apply what they learned during the Information Security Awareness Program in practice. Essentially, they learn how to protect information assets and become familiar with good information security practices. During the training, personal responsibility of the employees for information security is promoted. Additionally, the training tries to achieve a change in employee behaviour with regard to information security [43].

Stage 3 of the Information Security Competence Maturity Model is *Conscious Competence*. At this stage, it is needed that employees consciously focus on

performing information security practices. The employees know how to correctly perform these, but the practices are neither part of the corporate culture nor like a second nature to them. Employees can progress from Stage 3 to Stage 4 through following Information Security Education, which will result in a deeper understanding of information security practices. Next to the program, the employees have to gain experience with information security practices. Consequently, the practices will become like a second nature to them.

Through awareness, training, and experience, employees can become *Unconsciously Competent* and reach Stage 4 of the Information Security Competence Maturity Model. Information security will then be part of the corporate culture and incorporated in the behaviour of employees. Information Security Obedience is then reached.

4.1.4 Application to Cofano

From the Information Security Competence Maturity Model, we can derive at what stage Cofano is with regard to information security obedience of employees. To achieve this, we first compare the employee behaviour of Cofano to that of the stages in the model. The evaluation can be found in table 4.4. In the table, the first column indicates the stage of the Information Security Competence Maturity Model. The second column shows the characteristics of Cofano at that particular stage. The evaluation is based on the interview results from chapter 3. The characteristics listed in the table are observed by the researcher and verified by a security expert of Cofano.

Model Stage	**Cofano**
Unconscious Incompetence	The employees of Cofano are all aware of their skills with regard to information security.
Conscious Incompetence	Employees have been given presentations about information security and have been made aware of possible threats to information security. Not all employees fully understand the benefits of information security.
Conscious Competence	Some employees consciously focus on information security, but not all.
Unconscious Competence	Information security practices are not a second nature to employees and are not part of the corporate culture.

Table 4.4: The status of Cofano per stage of the maturity model

Based on the evaluation in table 4.4, Cofano is somewhere between Stage 2 and Stage 3, or, Stage 2.5, of the Information Security Competence Maturity Model.

According to Thomson and von Solms, the corporate culture of an organization has a significant impact on employee behaviour and contributes to the effectiveness of information security within the organization. Therefore, it is important that information security practices are like a second nature to employees. Hence, the ultimate goal is to get to Stage 4, where Information Security Obedience is reached.

4.2 Concepts and Components for the Problem Treatment

The findings from the previous sections can be used as a starting point for the solution to Cofano's problem of creating security awareness.

According to the evaluation in section 4.1.2, the information security culture of Cofano is a subculture of the organizational culture, or, a type 2 relationship. The ultimate goal is to have a type 3 relationship, where the information security culture is embedded into the organizational culture completely. Information security culture can be completely embedded into the organizational culture when the following characteristics can be found within the organization:

- *Organizational culture*
  - Management involvement: security matters and strategy are brought into board meetings
  - Locus of responsibility: every member of the organization is involved in security
  - Information security policy: created in a holistic way, as well as regularly updated
  - Education/training: the security awareness program is made compulsory for all employees
  - Budget practice: budget is allocated for security activities annually by management
- *Employee beliefs, actions and behaviour*
  - Responsibility: employees always adhere to security procedures and guides
  - Participation: employees undergo security training periodically, and an awareness programme exists
  - Commitment: employees feel responsible for security, as well as the ownership of information
  - Motivation: employees are motivated and committed towards matters of security

  - Awareness / Know how: employees know how to deal with security and who to go to when facing problems
- *Probable consequences*
  - Risk vulnerability: should be low, as employees are highly aware of security
  - Awareness: employees are highly aware, and they are concerned about the security in their organization
  - Responsibility: every employee is responsible for security
  - Security practices: security unconsciously becomes part of the daily routine
  - Investment for security practices: a large amount of money is spent on implementing security activities

According to the evaluation in section 4.1.2, the information security culture of Cofano is a subculture of the organizational culture, or, a type 2 relationship. The ultimate goal is to have a type 3 relationship, where the information security culture is integrated completely into the organizational culture.

According to the evaluation in section 4.1.4, Cofano is at Stage 2.5 of the Information Security Competence Maturity Model. To go from Stage 2.5, *Conscious Incompetence*, to Stage 4, *Unconscious Competence*, or *Information Security Obedience*, the following must be achieved:

- *Stage 3*
  - Employees need to understand the benefits of information security
  - Employees need to follow Information Security Training, in which they:
    * Apply knowledge from the Information Security Awareness Program (Stage 2) in practice
    * Learn how to protect information assets
    * Become familiar with good information security practices
    * Are made aware of the importance of personal responsibility
  - A change in employee behaviour with regard to information security is trying to be achieved

- *Stage 4*
  - Employees consciously focus on performing information security practices
  - Employees need to follow Information Security Education, in which they:
    * Gain a deeper understanding of information security practices
  - Employees will have to gain experience with information security practices, so they will become like a second nature to them

4.3 Contribution to Stakeholder Goals

The concepts and components of available treatments contribute to the stakeholder goals from section 3.10 in the following way (concept/component: stakeholder goal):

- Employees have to undergo security training periodically: employees keep their knowledge up-to-date and stay aware of what they are doing with regard to security
- Security unconsciously becomes part of the daily routine: employees are able to combine security with their daily job and security during development can be guaranteed
- Employees are motivated and committed toward security matters: employees recognize possible improvements and share these with the security team and understand why Cofano has a policy and certain regulations
- Employees gain a deeper understanding of information security practices: security is not only done for the ISO 27001 certification
- Employees feel responsible for security, as well as ownership of information: employees have a high responsibility
- Employees are highly aware, and they are concerned about the security in their organization: employees are always aware of what they are doing and security is seen as part of the software quality instead of an obstruction
- Employees know how to deal with security and who to go to when facing problems: employees understand why security is so important

4.4 Artifact

This section introduces our proposed artifact. From the framework by Lim et al., we can extract 15 concepts, or categories, on which an organization can improve. These categories are classified under three main concepts: organizational culture, employee beliefs, actions, and behaviour, and probable consequences. We can merge the concepts into our own categories to later map the results from the interviews from chapter 3 to them. For merging the concepts, we looked at the similarity of the concept description. The results can be found in figure 4.3.

Consequently, we can map the improvement points from the interviews in chapter 3 to our categories. We make the note that for the categories *Investment & Budget* and *Risk Vulnerability*, as depicted in figure 4.3, no improvement points could be found. As a result, these categories were left out. The mapping is shown in figure 4.4. The improvement points with the diagonal stripes in the background indicates that the improvement point for a category is duplicate.

Next, we can remove the duplicate improvement points in the striped boxes and organize our concepts and categories in such a way that we create a clear overview of what Cofano has to do per category to improve their organizational security awareness. The final product is visualized in figure 4.5. The implications of the created artifact are pointed out in the following sections.

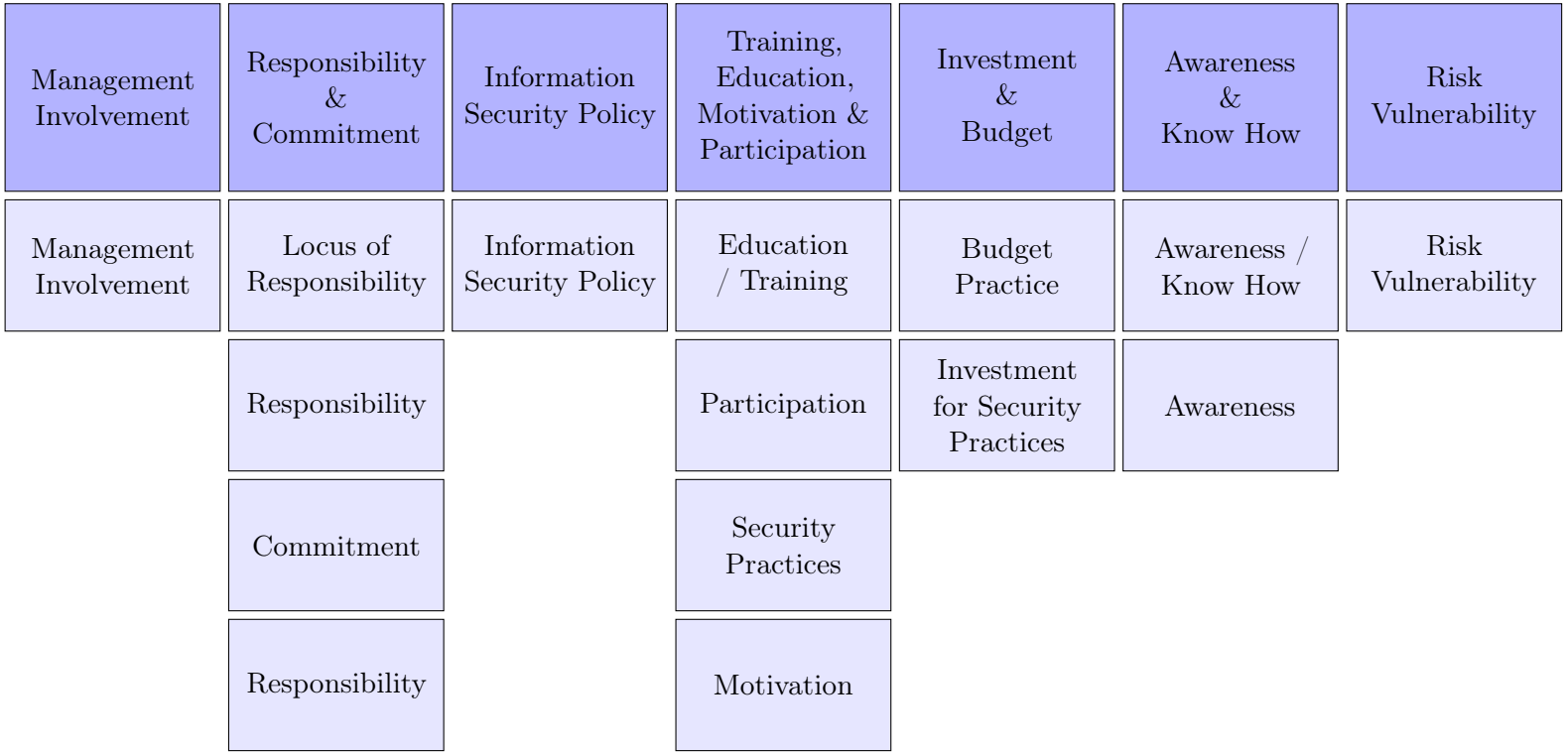

Figure 4.3: Merging categories from the Lim et al. framework

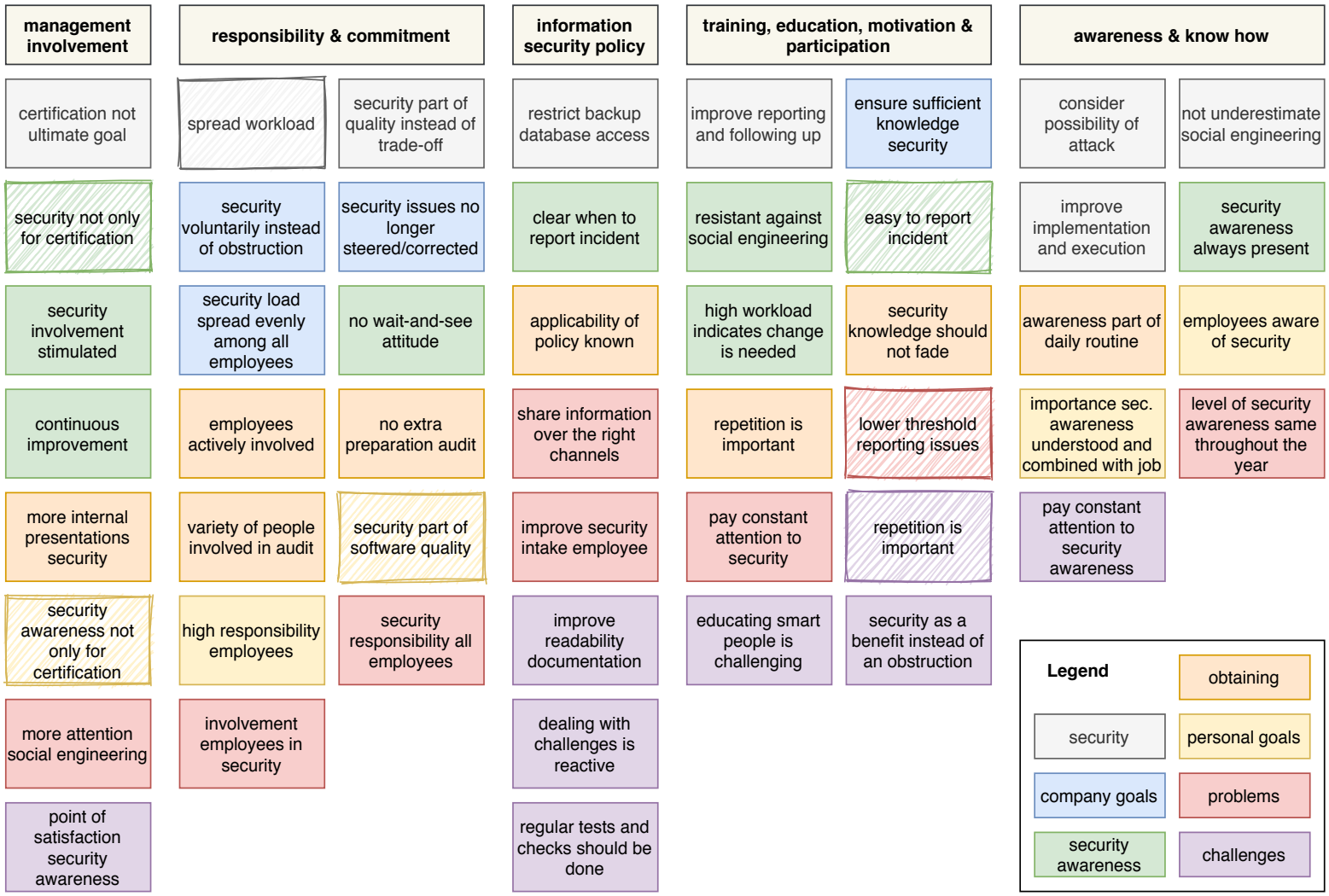

Figure 4.4: Mapping of the improvement points to the merged categories of the existing framework

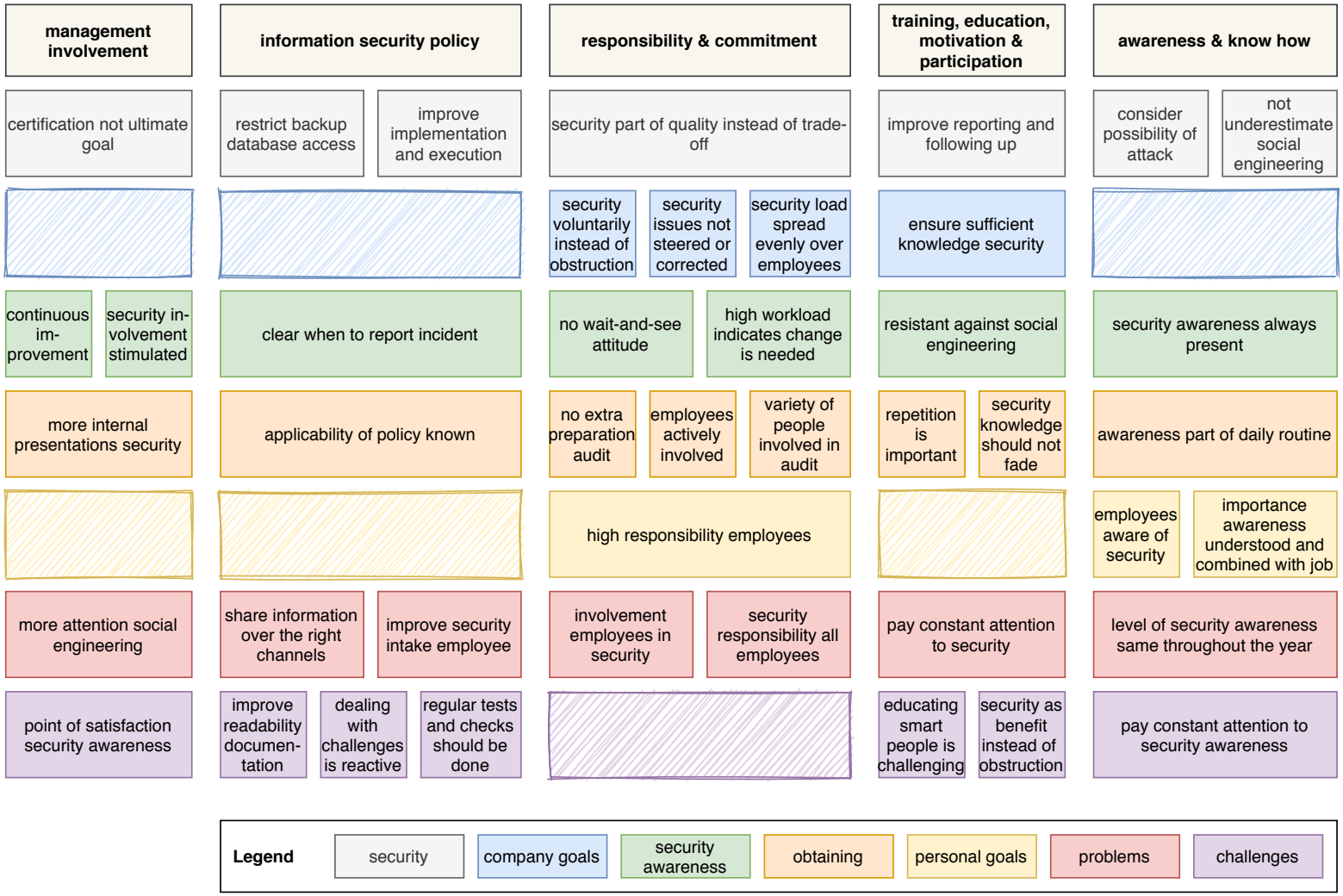

Figure 4.5: Our proposed artifact

In the following sections, it is described what Cofano has to do in order to achieve a higher level of security awareness within the organization. In these sections, possible actions for Cofano are described, following the order of the constructs at the first row of figure 4.5.

4.4.1 Management Involvement

Security matters and strategy are brought into board meetings.

With regard to the involvement of the management, Cofano needs to have the common goal to perform security activities for the benefit of the company, instead of only for the certification. Moreover, the management should inspire the organization to continuously improvement these security activities. In addition, the management needs to stimulate security involvement across the entire organization. Management should consider giving more internal presentations about the security of the organization to make employees feel more involved in this process. Furthermore, management could give more attention to social engineering and explain its implications. With regard to security awareness, management should find a point at which they are satisfied with the level of security awareness.

4.4.2 Information Security Policy

Information security policy needs to be created in a holistic way, as well as regularly updated.

With regard to the information security policy, the access to backup databases from customers should be restricted for new employees to ensure the confidentiality of the data. Policy should indicate that new employees receive this access after some time, and that before having access, new employees only receive already anonymized customer databases. The security intake for new employees needs to be improved in order for the new employees to be completely in line with Cofano's security practices.

Overall, everything with regard to security is well-documented, but implementation and execution should be improved. Additionally, the readability of the information security policy documentation should be improved, so employees can comprehend important information about security better and faster. In the information security policy, it should be clearly stated when an employee has to report an incident. Moreover, it should be ensured that the policy is not only read and understood, but that the applicability of the policy is also known amongst employees. Although the policy already states over which channels what information may be shared,

it should be ensured that only the right channels are used to share sensitive information. Additionally, regular tests and checks should be done to identify possible vulnerabilities.

Currently, dealing with challenges is reactive: something has to go wrong first before action is taken on the subject matter. However, prevention is better than cure, so challenges have to be considered in the policy so they can be responded to accordingly.

4.4.3 Responsibility & Commitment

Every member of the organization is involved in security. Employees always adhere to security procedures and guides. In addition, they feel responsible for security, as well as the ownership of information. Moreover, every employee is responsible for security.

With regard to the responsibility and commitment of the employees, it is important that they do not see security as an obstruction. Employees need to be moved to do it voluntarily. Additionally, they need to recognize that security is a part of the quality of the software, instead of it being a trade-off for the ability to deliver new features in the software. The high workload for the security team before an audit indicates a change is needed in the entire process. Currently, employees have a wait-and-see attitude, but employees should be actively involved in security in a way that the security load can be spread evenly over all employees. Additionally, a variety of employees needs to be involved in the audit. Since the security load is spread evenly over the employees, no extra preparation will be needed for the audit. As a result, security will be the responsibility of all employees. Moreover, a high responsibility for security needs to be created amongst employees, in such a way that security issues no longer need to be steered or corrected by the security team.

4.4.4 Training, Education, Motivation & Participation

Employees undergo security training periodically, and a security awareness programme exists that is compulsory for all employees. Furthermore, employees are motivated and committed towards matters of security, and security unconsciously becomes part of their daily routine.

With regard to training, education, motivation, and participation, it should be ensured that every employee has sufficient knowledge of security, which should not fade. Therefore, repetition is important. Although educating smart people might

be challenging, it should be shown to these people how security is beneficial, and not an obstruction. Constant attention should be paid to security, so Cofano is resistant against security vulnerabilities such as social engineering. Additionally, the reporting and following up of security issues should be improved.

4.4.5 Awareness & Know How

Employees know how to deal with security and who to go when they are facing problems. In addition, they are highly aware and concerned about the security in their organization.

With regard to awareness and know how, the importance of security awareness should be understood by the employees and should be combined with their job. Actually, the awareness should always be present and should be part of the daily routine of the employees. All employees should be aware of security. Constant attention needs to be paid to security awareness, so the level of security awareness can be maintained throughout the year. Additionally, employees should be taught not to underestimate social engineering, and the possibility of an attack should always be considered.

4.5 Application of Model

The categories *responsibility & commitment*, *training, education, motivation & participation*, and *awareness & know how* all focus on the behaviour of the employees with regard to security. This coincides with the Information Security Competence Maturity Model of Thomson and von Solms, where Cofano is at stage 2.5. To get to the third stage, Cofano needs to provide employees with Information Security Training. During this training, the knowledge that employees already obtained during their Information Security Awareness presentations will be applied in practice and employees will learn how they can actually protect information assets. In addition, they will become familiar with good information security practices, and are made aware how important their personal responsibility is with regard to security. When a change in employee behaviour with regard to information security is achieved, the objectives of stage 3 are achieved, and employees are ready to move on to this stage.

To get to the fourth and final Information Security Obedience stage, Cofano needs to provide employees with Information Security Education. In this stage, employees consciously focus on performing information security practices, which they will have to gain experience with in such a way that it will become like a second nature to them. During their education, they gain a deeper understanding of information security practices and security will become part of their daily routine.

Chapter 5

Expert Evaluation

In this chapter, it is described how the artifact is validated. The validation is done by interviewing experts about the proposed artifact. The experts are asked how familiar they are with the concept of security awareness. In addition, they received questions about the perceived ease of use, the perceived usefulness and intention to use of the artifact.

5.1 Expert Background

The first expert is familiar with the concept of security awareness, as he is the security officer at the Cofano location in Sliedrecht. This security officer was closely involved in the process of making Cofano ISO 27001 compliant and is experienced on the area of security. Next to that, he is a lead developer. The second expert has familiarized himself with the concept of security awareness through interviews and reading. He thinks security awareness is an indication of how concerned people are with security during their daily work. The second expert is a lead developer at the Cofano location in Enschede.

5.2 Perceived Ease of Use

Both experts think the artifact, together with the explanatory notes, provides a clear overview of all steps Cofano can undertake to reach a higher level of security awareness.

The first expert mentions that, although all points of attention are identified, not

all of those points are transformed into action points. For example, the point "Management should inspire continuous improvement". He thinks it is a good point, but he would then also like to see an approach for such an attention point. Currently, Cofano is missing capacity to undertake the steps described in the artifact. The expert wonders how much time it would take to undertake all steps.

The second expert mentions that, although the artifact is clear, the two categories that were left out, should not be forgotten. He thinks the categories *Investment & Budget* and *Risk Vulnerability* should be paid attention to too. In other words, budget should be allocated for security activities annually by the management team. In addition, a large amount of money is spent on implementing security activities. With regard to the risk vulnerability, this should be low, as employees are highly aware of security. Next, he thinks the focus of the artifact is on improving the security awareness, but not improving the current status. Finally, he thinks that there should be an explanation about figure 4.3 and 4.4 underneath the figure, in addition to the explanation in section 4.4.

5.3 Perceived Usefulness

Both experts think that the proposed artifact contains all the steps needed for Cofano to obtain a higher level of security awareness amongst employees.

The first expert thinks that the artifact, together with the explanatory notes, could perhaps have been formulated more concretely. In addition, he thinks it could be useful to add definitions. Consequently, the artifact can be used and interpreted separately from the research.

The second expert wonders, although the artifact contains all the steps needed to improve security awareness, if the artifact can also be used to maintain the current level of security awareness. In addition, he thinks that the artifact contains very concrete points. He wonders, if all points are considered, the company will be at the maximum level of security awareness. Or, if the artifact could then be re-used to keep improving.

5.4 Intention to Use

Both experts think, with their feedback considered, the artifact could be used to improve the security awareness at Cofano. The first expert thinks that, in order to be able to make use of the artifact, all points of attention have to be converted into action points. Consequently, the artifact could be a good tool to improve the

security awareness within Cofano.

The second export mentions that it is valuable to see the points on which Cofano can improve with regard to security and security awareness. However, he thinks an abstract step in between is missing, like, the artifact, and then the artifact applied to Cofano in the current situation. He wonders about the usability of the artifact in a few years, and the applicability to other comparable organizations.

5.5 Improvements Proposed Artifact

From the expert interviews, the following improvement points could be identified:

- Points of attention need to be transformed into action points
- An estimate should be provided of the time needed for implementation
- The categories *Investment & Budget* and *Risk Vulnerability* should be paid attention to
- It should be clear how the artifact improves the current situation, in addition to improving the security awareness overall
- An explanation is needed underneath figure 4.3 and 4.4
- The artifact and explanatory notes could be formulated more concretely
- Definitions need to be added to the artifact, as to be able to use it separate from this research
- The level of security awareness after the implementation should be indicated
- The re-usability of the artifact should be indicated
- An abstract step needs to be added to not only show what improvements the artifact will bring, but also the artifact itself and application of artifact to current situation
- The applicability to other comparable organizations needs to be researched

After incorporating these points, the artifact will be at a level that indicates it is ready to be implemented and tested.

Part IV

Reflection on the Research

Chapter 6

Discussion

In this chapter, the results presented in chapter 3, chapter 4 and chapter 5 are discussed. First, we discuss what the results of this research mean. Next, we discuss why these results matter. Finally, we discuss the limitations of this research.

6.1 Interpretations

The interviews with the employees of Cofano indicate that many improvement possibilities exist on the area of security awareness within Cofano. These improvement possibilities, together with existing literature, are used to create an artifact which aids Cofano in reaching and maintaining a higher level of security awareness. To validate this artifact, two experts in the field were interviewed. From the validation, we gather that the artifact is useful in the field of security awareness.

6.2 Implications

The results from the interviews, as described in chapter 3, provide insight into the thoughts of employees on the security awareness of Cofano. The artifact that was created next, builds on both these interviews and literature which includes a framework from Lim et al. [23] and a model by Thomson and von Solms [38]. The artifact was then validated by experts from the field. These results indicate that the artifact is usable at Cofano. The artifact contributes to reaching a higher level of security awareness amongst the employees of Cofano.

For the management team of Cofano, the artifact provides an overview of all steps

that can be taken to obtain a higher level of security awareness amongst employees. Before, the management team did not have such an overview. As a result, the management team was unaware of the steps that could be taken to improve the security awareness within the organization. The artifact will be used by the security team to initiate and monitor the identified improvement possibilities.

The author of this thesis thinks that the artifact might be a good candidate for the use in any SME operating in the same business sector as Cofano. If such an SME is interested in achieving security goals similar to those of Cofano, then the artifact could be a valuable first step for the company's journey.

In chapter 5, one of the experts wonders about the maturity level of security awareness in the organization after the use of the proposed artifact. He wonders, if all steps are considered, the company will be at the maximum level of security awareness. Or, if the artifact could then be re-used to keep improving. The researcher thinks that some steps in the artifact can only be performed once, but other steps can be repeated. For example, from the artifact, depicted in figure 4.5, if we take the point *restrict backup database access*, that is an improvement point that can only be executed once. The backup database access needs to be restricted for certain users, and once that is done, the point can be discarded. If we then take another point, *ensure sufficient knowledge security*, that is a recurring improvement point. Ensuring sufficient security knowledge is something that needs constant and consistent monitoring, because it is a moving target. Knowledge needs to be updated constantly, and if new employees arrive, it needs to be ensured that they have sufficient knowledge of security.

6.3 Limitations

The scope of the problem investigation of this research was limited to the security awareness of the employees of Cofano. However, even though their security awareness may be on an appropriate level after implementing the treatment, that of their customers might not be. The questions that remains is then: How secure can you be if your customers are not?

In addition, the interviews from chapter 3 and 5 are conducted in Dutch, which is the native language of the interviewees. The analysis was done in English, which is the language of this thesis. It could be the case that some of the context got lost during translation. With a supervisor and an expert overseeing this process, the risk for this bias could be mitigated.

A common limitation in qualitative interview studies is traceable to the number of participants. It is the doubt that if the researcher includes more interviewees, he or she could get different findings. We note that in this research, our data collection and analysis actually achieved saturation (see chapter 3). This means that adding more interviewees would not necessarily bring new insights and, in turn, change our results. Therefore, we think that the validity threat due to the number of participants is very low.

Moreover, the artifact validation was done by two experts from Cofano. Although these experts indicate that the artifact is useful, we acknowledge that it is not tested in practice with the end users. However, in this respect, Cofano has very specific future plans: the author of the thesis will remain part of the company in the future, and she is willing and available to carry out a broader evaluation by using the artifact in a project and learn from these experiences. Only then, Cofano will know for sure what effects the artifact would have in their organizational context and what possible refinements of the artifact might be considered.

Chapter 7

Conclusion

In this chapter, the conclusion of this research is presented. First, the research questions will be answered. Consequently, future work will be discussed.

7.1 Answering the Research Questions

The goal of this research was to design and validate an artifact for Cofano that treats the problem of creating and maintaining security awareness in SMEs with regard to ISO 27001 and with preservation of corporate culture. In order to achieve this goal, the Design Science Methodology by Wieringa was used. In the following sections, the answers to the research questions will be discussed.

7.1.1 Challenges

The first research question about the challenges Cofano is currently experiencing, was split up in three sub-questions. The answers to the sub-questions will be discussed. Consequently, the answer to the first research question will be presented.

RQ1.1: Who are the stakeholders and what are their goals?

The stakeholders of this research are Cofano, Cofano employees and SMEs, as described in section 2.2.1. However, the focus of this research is on the second group of stakeholders, the employees. Their goals, as discussed in section 3.10, are mainly: (1) keeping their knowledge up-to-date with the latest security issues and potential attack techniques, (2) staying aware of what you are doing, (3) guarantee

security during development, and (4) share improvements with security team if possible. The goals of the management team include: (1) not only doing security for the ISO 27001 certification, (2) high responsibility of employees, (3) employees are always aware of what they are doing, (4) continuous improvement, and (5) security should be seen as part of the software quality, instead of an obstruction. The goals of the security team are that: (1) employees understand why security is so important, (2) employees understand why Cofano has a policy and certain regulations, (3) employees are able to combine security with their daily job, and (4) employees recognize possible improvements.

> **RQ1.2:** What is Cofano currently doing to resolve the challenges? If applicable and known, what are the shortcomings of the approaches that were tried out?

From the interview results in section 3.12, continuously keeping security in the back of your mind proves to be difficult. The workload of the tasks of the employees is already sufficient enough to fill all working hours. Since Cofano is not the right company for many formal processes and obligations, it is a challenge to motivate people to engage in security awareness. The question remains if it is possible to make everyone completely aware of security. A point needs to be found at which the level of security awareness is satisfactory, because the costs to increase the awareness even more will be exponential.

It is a challenge to educate smart people about security topics they might already have sufficient knowledge of. In addition, security knowledge fades after a while, therefore, repetition is important.

An ongoing challenge is to keep developing software in a secure way. As the company grows and acquires reputation, it might be more interesting to hack. Therefore, it is increasingly challenging top keep web applications safe and secure. Accordingly, checks and tests should be done regularly, so Cofano does not let their guard down. Security awareness is an increasingly important subject, especially with the increasing digitization and Cofano's acquisition of larger customers. Constant attention needs to be paid to security, in order for it to stay at the same level.

Many challenges Cofano encounters on the area of security and security awareness are reported. Consequently, measures are taken to mitigate or resolve these challenges. Additionally, changes will be implemented in the policy whenever needed. Moreover, challenges are resolved by investing time and paying constant attention to the subject, as well as encouraging people to discuss and implement improvements. Furthermore, the way presentations were given on the subject of

security awareness, was improved.

A shortcoming in the way Cofano deals with challenges is that it is reactive: something has to go wrong before anything is done about it. In addition, the findings from the security team are not always exposed Cofano-wide, so employees do not learn from them. Moreover, challenges with the security level of customers are not always easy to handle according to policy. Consequently, they are resolved according to feeling. Finally, there is always the shortcoming of capacity, time, and money.

> **RQ1.3:** What are the effects if the challenges are not treated and how do these detract from stakeholder goals?

According to the interview results in section 3.13, the employees of Cofano agree that not addressing security awareness could be troublesome for the future of the company. The consequences might be disastrous for the business continuity. As a result of not addressing security awareness, (1) people will have less knowledge on the subject of security, (2) employees become lax, (3) the level of security will deteriorate, (4) the annual audit will still have a high workload prior to it, (5) the responsibility of security will still be at the security team, (6) Cofano could get in trouble with the audit and certification, (7) unauthorized access could be gained to Cofano applications, and (8) data leaks will arise. Hence, Cofano will have loss of face, which could lead to great financial losses.

> **RQ1:** What are the challenges Cofano currently experiences from the perspective of security awareness and Cofano's organizational culture?

The combination of the sub-questions resulted in an overview of the challenges that Cofano currently experiences from the perspective of security awareness and Cofano's organizational culture. First, the stakeholders and stakeholder goals are identified. Next, challenges and their approaches are identified, and if applicable the shortcomings of these approaches. Finally, the effects of not treating the challenges are discussed, and how these detract from the identified stakeholder goals.

7.1.2 Proposed Artifact

RQ2.1: What are the available treatments?

From a research topics paper, two available treatments were identified. The first is a framework by Lim et al. that could aid organizations in reaching their desired level of information security culture [23]. In this framework, the types of relationships, the organizational culture, the actions and behaviour of the employees and the probable consequences with regard to security are listed. With the help of the framework, we were able to determine what the type of relationship is that the information security culture has with the organizational culture within Cofano: a type 2 relationship, where the information security culture of Cofano is a subculture of the organizational culture.

The second available treatment is a model by Thomson and von Solms on information security competence maturity [38]. This model is a method for evaluating the extent that information security is embedded in the corporate culture of an organization. Additionally, it indicates what steps are needed to reach a level where security controls are embedded completely into the employee behaviour and daily routine. With the help of this model, we were able to determine to what extent the information security of Cofano is embedded in their corporate culture: Cofano is somewhere between stage 2 and stage 3, or, at stage 2.5, of the Information Security Competence Model.

RQ2.2: What are the concepts and components of available treatments that treat the problem?

According to Lim et al., organizational culture has a significant impact on employees. Research shows that an information security culture needs to be created within an organization to improve employee behaviour with regard to organizational information security [23]. Therefore, the ultimate goal is to have a type 3 relationship, where the information security culture of Cofano is embedded entirely into their organizational culture, as to influence employee behaviour positively with regard to information security practices. Hence, we can make use of the characteristics of a type 3 relationship to ensure that the information security culture of Cofano can be completely embedded into their organizational culture. The characteristics can be found in section 4.2.

According to Thomson and von Solms, the corporate culture of an organization has a significant impact on employee behaviour and contributes to the effectiveness of information security within the organization [38]. Therefore, it is important that information security practices are like a second nature to employees. Hence,

the ultimate goal is to get to stage 4 of the model, where Information Security Obedience is reached. We can make use of the characteristics of stage 3 and 4, in order to ensure that information security practices become like a second nature to the employees of Cofano. The characteristics can be found in section 4.2.

RQ2.3: How do these contribute to the stakeholder goals?

The concepts and components of available treatments contribute to the stakeholder goals from RQ1.1 in the following way (concept/component: stakeholder goal):

- Employees have to undergo security training periodically: employees keep their knowledge up-to-date and stay aware of what they are doing with regard to security
- Security unconsciously becomes part of the daily routine: employees are able to combine security with their daily job and security during development can be guaranteed
- Employees are motivated and committed toward security matters: employees recognize possible improvements and share these with the security team and understand why Cofano has a policy and certain regulations
- Employees gain a deeper understanding of information security practices: security is not only done for the ISO 27001 certification
- Employees feel responsible for security, as well as ownership of information: employees have a high responsibility
- Employees are highly aware, and they are concerned about the security in their organization: employees are always aware of what they are doing and security is seen as part of the software quality instead of an obstruction
- Employees know how to deal with security and who to go to when facing problems: employees understand why security is so important

RQ2: What artifact can be designed that treats the problem Cofano is experiencing?

The combination of the sub-questions resulted in the design of an artifact that possibly treats the problem that Cofano is experiencing. The artifact is depicted in figure 4.5 and described in section 4.4. The explanatory notes of the artifact revolve around five important topics: *management involvement*, *information security policy*, *responsibility & commitment*, *training, education, motivation & participation* and *awareness & know how*. For each of these topics, possible actions for Cofano are listed that could help them achieve a higher level of security awareness within the organization.

7.1.3 Applicability of Proposed Artifact

> **RQ3.1:** To what extent is the proposal useful for the practitioners in the field?

The artifact, together with the explanatory notes, can be used by practitioners in the field to increase the level of security awareness in an organization. The artifact provides a clear overview of all steps Cofano can undertake to reach a higher level of security awareness and the intention to use is present.

> **RQ3.2:** To what extent is the proposal usable at Cofano? Can the practitioners apply it in the context for which the artifact was envisioned?

In the context of this research, the artifact can be understood and used at Cofano without help. The practitioners can apply it in the context for which the artifact was envisioned, especially after the identified improvements points are carried out. Cofano intends to use it.

> **RQ3:** What is the applicability of the proposed artifact?

The proposed artifact, together with the explanatory notes, provides a clear overview of all steps that can be taken by Cofano to improve and maintain the level of security awareness amongst their employees. In addition, it can be used for the purpose of increasing the level of security awareness. It is worthwhile noting that Cofano has the intention to use it. Moreover, the practitioners can apply it in the context for which it was envisioned for, especially after the improvement points are implemented. The artifact can be understood and used at Cofano, in the context of this research, without help.

7.2 Future Work

In this research, the focus is on the first three steps from the engineering cycle, according to Wieringa [40]. These steps are the problem investigation, the treatment design, and the treatment validation. Future researchers could implement the improvement points for the proposed artifact. These were extracted from expert interviews during the treatment validation, as can be read in chapter 5. As a result, the researcher ends up with a treatment that is ready for the fourth and fifth step in the engineering cycle: the treatment implementation and the implementation evaluation.

In the fourth step, the problem is treated with our proposed artifact. In other words, the artifact is tested in practice with the end users to see if it can stimulate organizational change with regard to security awareness. Consequently, in the fifth step, it is evaluated if the treatment actually contributes to reaching a higher level of security awareness within the organization. In other words, it is evaluated if the treatment has been successful. As a result, the effects of the artifact in the organizational context of Cofano can be determined. After completing the fourth and fifth step, the steps from the engineering cycle can be repeated again to see if the problem still exists, or if the proposed treatment can be improved.

Moreover, the application of this research to other, similar companies can be investigated. Future researchers can determine the generalizability of the artifact to other organizations. As a result, it can be determined if the proposed artifact, possibly with some adaptions, is usable at other companies in a similar business sector as that of Cofano.

Appendix A

Pilot Interview

Stakeholders and goals

1. Wat is je naam?
2. Wat is je functie binnen Cofano?
3. Wat zijn je taken binnen Cofano?
4. Op welke manier ben je betrokken bij security awareness binnen Cofano?
5. Wat zijn je doelen op gebied van security awareness binnen Cofano?
6. Is er, volgens jou, iets wat problematisch is op het gebied van security awareness? En is er, met betrekking tot security awareness, iets wat je graag verbeterd zou willen zien worden? Welke verbetering heeft, volgens jou, de hoogste prioriteit?

Resolving challenges

7. Kom je uitdagingen tegen op het gebied van security awareness? Welke uitdagingen merk je dat je tegenkomt op dit gebied? Is er geprobeerd deze uitdagingen te verslaan? Zo ja, op welke manier? Ben je nog tekortkomingen tegengekomen in deze aanpak?
8. Wat denk je dat de effecten zullen zijn van het niet aanpakken van security awareness binnen Cofano?

Appendix B

Interview

Algemene Informatie

1. Wat is je naam?
2. Op welke locatie van Cofano werk je?
3. Wat is je functie binnen Cofano?
4. Wat zijn je taken binnen Cofano?
5. Heb je contact met klanten? Zo ja, op welke manier?

Security Kennis

6. Wat is, volgens jou, security?
7. In jouw ogen, hoe is de security binnen Cofano?
8. Wat zijn de doelen van Cofano op gebied van security?
9. Wat is, volgens jou, security awareness?

Na het verkrijgen van algemene informatie en de kennis op het gebied van security volgt de definitie van security awareness. De definitie luidt als volgt: **Security awareness is de kennis en het gedrag dat leden van een organisatie hebben met betrekking tot bescherming van de fysieke en vooral informatieve activa van een organisatie.**

Je kan hierbij denken aan:

- het herkennen en melden van phishing mails
- veilig omgaan met bedrijfsinformatie - hoe en waar mag ik bepaalde informatie opslaan?
- het beschermen van de data op je harde schijf door middel van encryptie
- (beveiligings)updates regelmatig uitvoeren
- voor developers: code moet bestand zijn tegen SQL injectie en mag niet gevoelig zijn voor XSS (Cross-Site Scripting)
- het melden van een incident omtrent security in IRIS
- fysiek: wat doe ik als een onbekend iemand het kantoor binnenloopt?

Security Awareness

10. In jouw ogen, hoe is de security awareness binnen Cofano?

11. Vind je security awareness belangrijk? Waarom?

12. Hoe is er geprobeerd security awareness te krijgen binnen Cofano?

Betrokkenheid Security

13. Op welke manier ben je betrokken bij security awareness binnen Cofano?

14. Heb je doelen op het gebied van security awareness? Zo ja, welke?

15. Is er, volgens jou, iets wat problematisch is op het gebied van security awareness? En is er, met betrekking tot security awareness, iets wat je graag verbeterd zou willen zien worden? Welke verbetering heeft, volgens jou, de hoogste prioriteit?

Resolving challenges

16. Kom je uitdagingen tegen op het gebied van security awareness? Welke uitdagingen merk je dat je tegenkomt op dit gebied? Is er geprobeerd deze uitdagingen te verslaan? Zo ja, op welke manier? Ben je nog tekortkomingen tegengekomen in deze aanpak?

17. Wat denk je dat de effecten zullen zijn van het niet aanpakken van security awareness binnen Cofano?

Appendix C

Word Cloud

Figure C.1: Word cloud constructed by MAXQDA from interview data

Appendix D

Coding with Subcategories

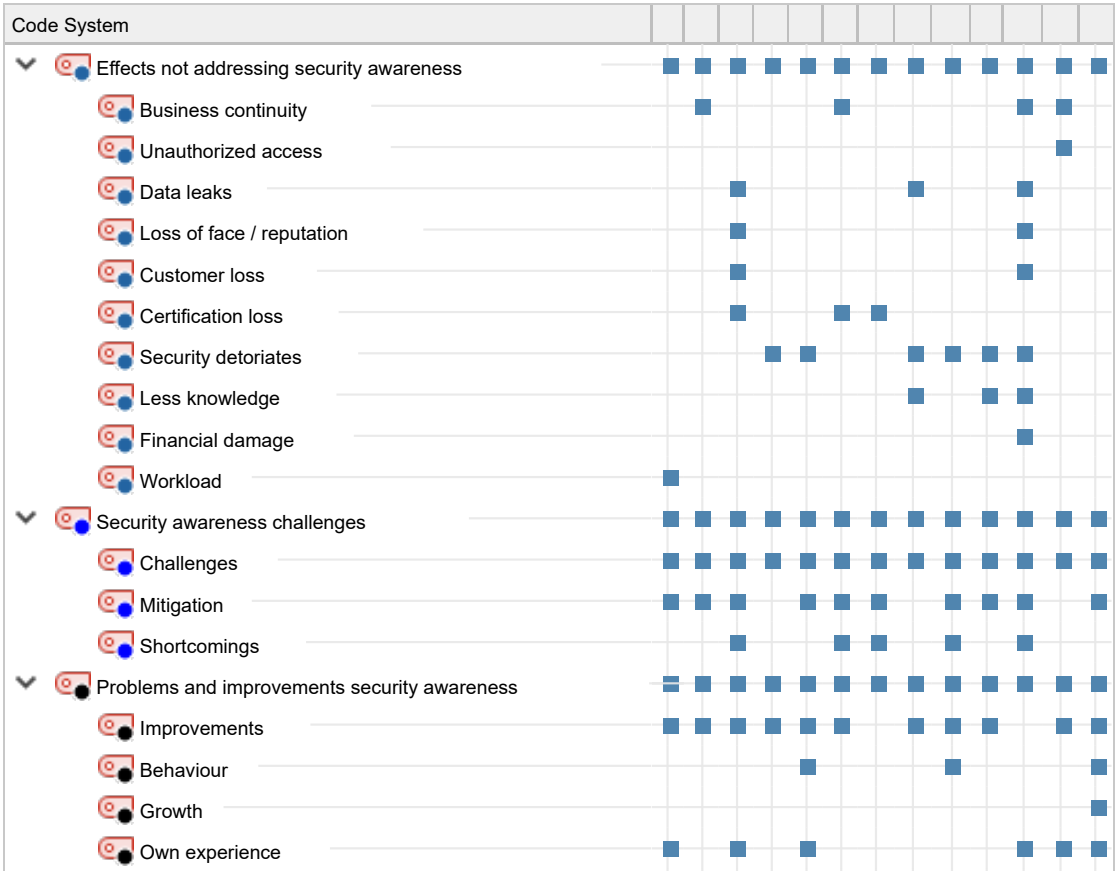

Figure D.1: Categories and subcategories from coding with MAXQDA

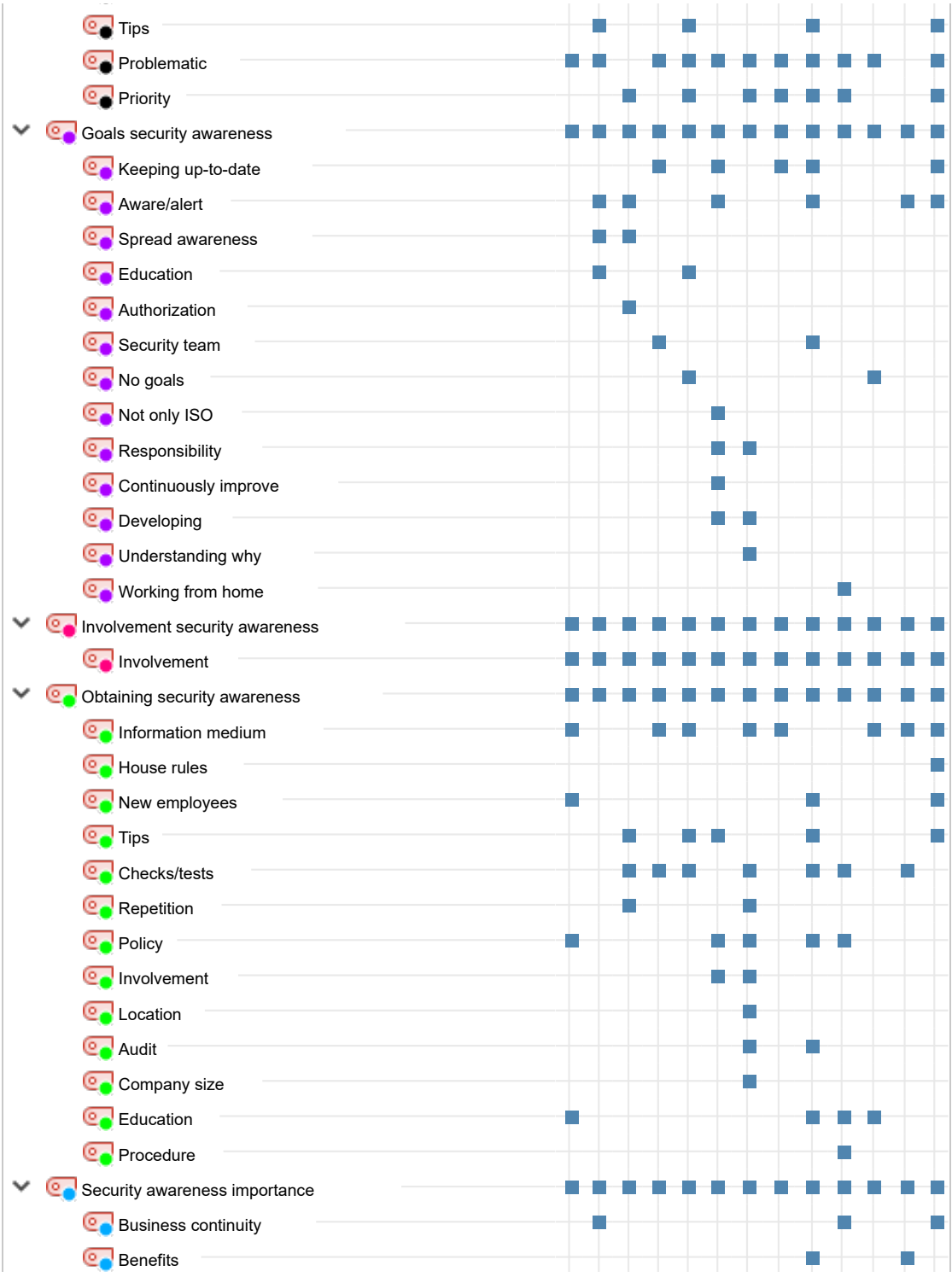

Figure D.2: Categories and subcategories from coding with MAXQDA - continued

Figure D.3: Categories and subcategories from coding with MAXQDA - continued

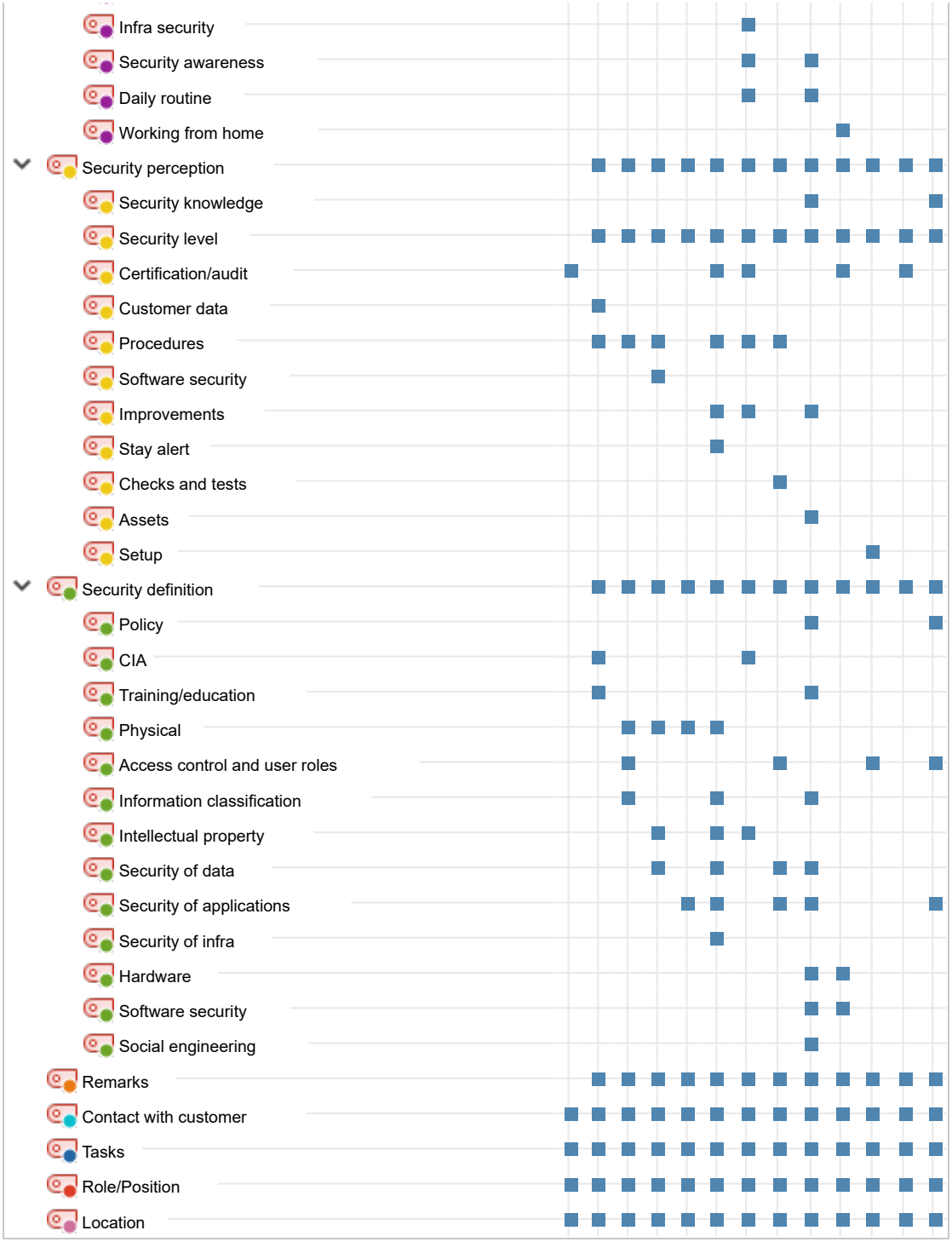

Figure D.4: Categories and subcategories from coding with MAXQDA - continued

Appendix E

Creative Coding

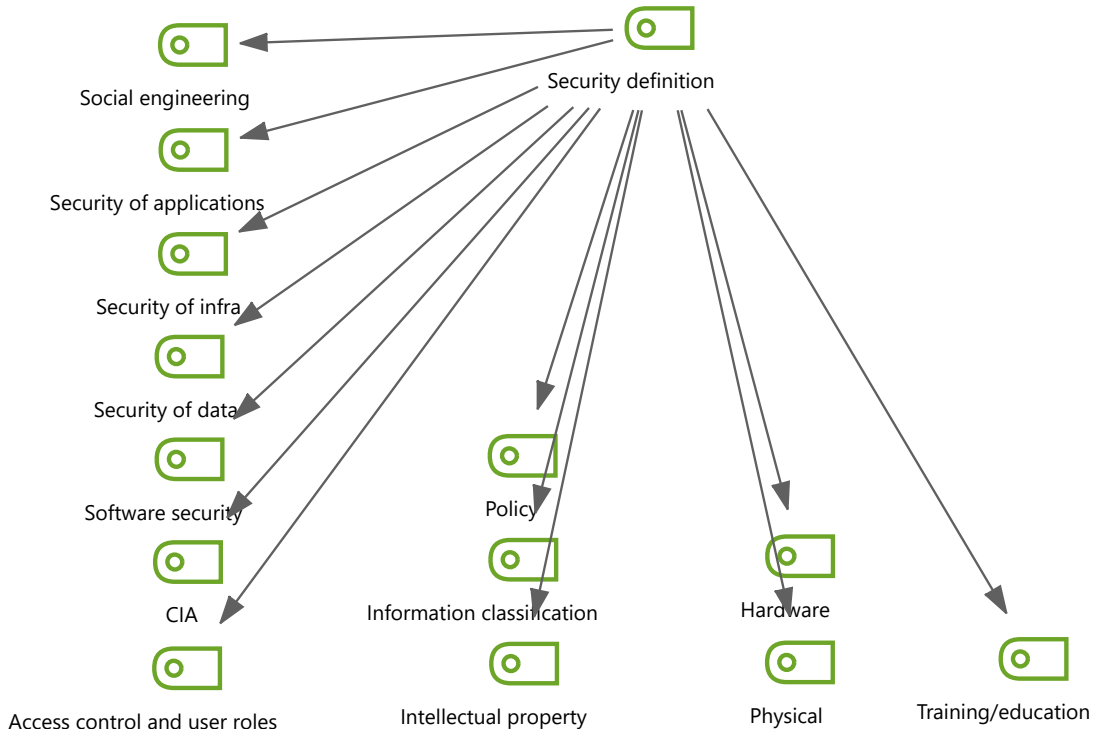

Figure E.1: Creative coding for the category security definition

Appendix F

Expert Interview

Algemene Informatie

1. Wat is je functie binnen Cofano?
2. Wat zijn je taken binnen Cofano?
3. Hoe bekend ben je met het concept security awareness?

Perceived Ease of Use

4. Vind je dat het voorgestelde artefact, tezamen met de begeleidende tekst, een duidelijk overzicht geeft van alle stappen die Cofano nog kan ondernemen om een hoger niveau van security awareness te bereiken en te behouden? Zo niet, wat zou er veranderd moeten worden?

Perceived Usefulness

5. Denk je dat het voorgestelde artefact alle stappen bevat die Cofano nodig heeft om een hoger niveau van security awareness te bereiken en te behouden? Zo niet, welke stappen mis je?

Intention to Use

6. Zijn er voornemens om het artefact te gebruiken binnen Cofano ter bevordering van de security awareness?

Appendix G

Framework

Nature of Relationship	**Organizational Culture**	**Employee Beliefs, Actions and Behaviours**	**Probable Consequences**
Type 3 relationship: the information security culture is embedded into the organizational culture [31, 39, 38] High [14]	**Management Involvement:** Management brings security matters and strategy into board meeting. Updates are made on a periodic basis to the company board of directors **Locus of Responsibility:** Management involves every member of organizations. **Information Security Policy:** Created in holistic manners. In addition, there are regular updates on security policy. **Education/Training:** Management make the awareness program compulsory for all the employees. **Budget Practice:** Management allocates budget for security activities annually	**Responsibility:** Always adhere to the security procedures and guides **Participation:** Employees undergo periodic security training, awareness programme **Commitment:** Employees feel responsible and ownership of information. **Motivation:** Motivated and committed towards security matters **Awareness/Know how:** Know how and who to deal with when facing security problems	**Risk Vulnerability:** Low **Awareness:** Employees are highly aware and concern about security matters in organization. **Responsibility:** Security is every employee's business **Security Practices:** Holistic manners. Unconsciously become daily routine activities **Investment for security practices:** High cost in implementing security activities

Type 2 relationship: the information security culture is a subculture of the organizational culture [12, 28] Moderate [14]	**Management Involvement:** Management typically delegates understanding of information security matters to CIO. **Locus of Responsibility:** Management starts to empower security matters to head of dept. **Information Security Policy:** Created within IT department and may not have widespread support or knowledge of where they are located **Education/Training:** Management starts to pay attention to awareness. People receive some training of information security **Budget Practice:** Management acts promptly towards expenses pertaining security activities	**Responsibility:** Adhere to security matters as a requirement of management **Participation:** Employees are involved in security matters in own dept. Less interdepartmental coordination. **Commitment:** Responsible and committed in security matters for own dept. **Motivation:** Employees are motivated in security matters in own dept. **Awareness/Know how:** Know how and who to deal with when facing security problems within dept.	**Risk Vulnerability:** Medium **Awareness:** Employees are aware of security matters within their own dept **Responsibility:** Employees are responsible for security matters within own dept. **Security Practices:** Security is employees' routine activities within own dept. **Investment for security activities:** Medium cost in implementing security activities
Type 1 relationship: the information security culture is separated from the organizational culture [7, 20, 34] Low [14]	**Management Involvement:** Management intuitively knows that information security is important, but it assigns the same level of importance as ensuring that computer is up **Locus of Responsibility:** Management assigns all the security responsibility to IT department. **Information Security Policy:** Created by copying without the means to enforce them. Usually issued by a memo. **Education/training:** Low awareness. Management does not emphasize on security training. **Budget Practice:** Usually part of a budget for IT support	**Responsibility:** Do not care and not responsible towards security matters **Participation:** Employees are not involved in security matters **Commitment:** Employees leave it to IT dept. Always bypass security procedures. **Motivation:** Employees are not motivated in dealing with security matters **Awareness/Know how:** Do not know what to do when facing with security problems	**Risk Vulnerability:** High **Awareness:** No awareness in security matters **Responsibility:** Only IT dept is responsible for security matters **Security Practices:** Not a routine activity of employees **Investment for security activities:** Low cost in implementing security activities

Table G.1: Framework of the relationship between organizational culture and information security culture [23]

Appendix H

List of Figures

Appendix I

List of Tables

Appendix J

Acronyms

CIA confidentiality, integrity, and availability. 22, 23

CIO chief information officer. 54

ISA information security awareness. 3, 4, 98

ISC information security culture. 53, 55, 98

ISMS Information Security Management System. 3, 24, 30, 31

OC organizational culture. 4, 53, 55, 98

OWASP Open Web Application Security Project. 32

PM Process Manager. 31, 32, 36, 40

QCA qualitative content analysis. 15

SaaS Software as a Service. 5

SC security culture. 4, 98

TAM Technology Acceptance Model. 17

Bibliography

[1] *All-In-One Qualitative & Mixed Methods Data Analysis Tool*. URL: https://www.maxqda.com/.

[2] Eric Amankwa, Marianne Loock, and Elmarie Kritzinger. "A Conceptual Analysis of Information Security Education, Information Security Training and Information Security Awareness Definitions". In: *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*. IEEE, Dec. 2014. DOI: 10.1109/icitst.2014.7038814.

[3] Mandy Andress and Brian Fonseca. "Manage People to Protect Data". In: *InfoWorld* 22.46 (2000), p. 48. ISSN: 0199-6649.

[4] Taimur Bakhshi. "Social Engineering: Revisiting End-User Awareness and Susceptibility to Classic Attack Vectors". In: *2017 13th International Conference on Emerging Technologies (ICET)*. IEEE, Dec. 2017. DOI: 10.1109/icet.2017.8281653.

[5] Lee Roy Beach. *Making the Right Decision: Organizational Culture, Vision, and Planning*. Englewood Cliffs, N.J.: Prentice Hall, 1993.

[6] Susan Breidenbach. "How Secure Are You?" In: *Information Week* 800 (Aug. 2000), pp. 71–78.

[7] Pauline A. Chia, Sean B. Maynard, and Anthonie Bastiaan Ruighaver. "Understanding Organizational Security Culture". In: *Sixth Pacific Asia Conference on Information Systems*. Sept. 2002, pp. 731–740.

[8] Isabella Corradini. *Security: Human Nature and Behaviour*. English. Vol. 284. Studies in Systems, Decision and Control. Springer International Publishing, 2020, pp. 23–47. ISBN: 978-3-030-43999-6. DOI: 10.1007/978-3-030-43999-6_2.

[9] John W. Creswell and Cheryl N. Poth. *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. SAGE Publications, 2018. ISBN: 978-1-5063-3020-4.

[10] Fred D. Davis. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology". In: *MIS Quarterly* 13.3 (Sept. 1989), p. 319. DOI: 10.2307/249008.

[11] Gurpreet Dhillon. *Managing Information System Security*. Macmillan Education UK, 1997. DOI: 10.1007/978-1-349-14454-9.

[12] Amitava Dutta and Kevin McCrohan. "Management's Role in Information Security in a Cyber Economy". In: *California Management Review* 45.1 (Oct. 2002), pp. 67–87. DOI: 10.2307/41166154.

[13] Ramon Eijkemans. *Stopwoordenlijst voor 21e eeuws Nederlands*. Feb. 2019. URL: https://eikhart.com/nl/blog/moderne-stopwoorden-lijst.

[14] Todd Fitzgerald. "Building Management Commitment through Security Councils, or Security Council Critical Success Factors". In: *Information Security Management Handbook, Sixth Edition*. CRC Press, May 2007, pp. 105–122. DOI: 10.1201/9781439833032.

[15] Greg Guest, Arwen Bunce, and Laura Johnson. "How Many Interviews Are Enough? An Experiment with Data Saturation and Variability". In: *Field Methods* 18.1 (Feb. 2006), pp. 59–82. DOI: 10.1177/1525822x05279903.

[16] K. Henry. "The Human Side of Information Security". In: *Information Security Management Handbook*. Boca Raton, London, New York, Washington D.C.: Auerbach Publications, 2004.

[17] H.L. James. "Managing Information Systems Security: a Soft Approach". In: *Proceedings of 1996 Information Systems Conference of New Zealand*. IEEE Comput. Soc. Press. DOI: 10.1109/iscnz.1996.554947.

[18] Cynthia M Jones et al. "Utilizing the technology acceptance model to assess the employee adoption of information systems security measures". In: *Issues in Information Systems* 11.1 (2010), p. 9.

[19] Aamir Hussain Khan et al. "SartCyber Security Awareness Measurement Model (APAT)". In: *2020 International Conference on Power Electronics & IoT Applications in Renewable Energy and its Control (PARC)*. IEEE, Feb. 2020, pp. 298–302. ISBN: 978-1-7281-6575-2. DOI: 10.1109/parc49193.2020.236614.

[20] Kenneth J. Knapp et al. "The Top Information Security Issues Facing Organizations: What Can Government do to Help?" In: *EDPACS* 34.4 (Oct. 2006), pp. 1–10. DOI: 10.1201/1079.07366981/46351.34.4.20061001/95104.1.

[21] Udo Kuckartz. "Qualitative Text Analysis: A Systematic Approach". In: *Compendium for Early Career Researchers in Mathematics Education*. Ed. by Gabriele Kaiser and Norma Presmeg. Cham: Springer International Publishing, 2019, pp. 181–197. ISBN: 978-3-030-15636-7. DOI: 10.1007/978-3-030-15636-7_8.

[22] Udo Kuckartz and Stefan Rädiker. *Analyzing Qualitative Data with MAXQDA*. Springer International Publishing, 2019. DOI: 10.1007/978-3-030-15671-8.

[23] Joo S. Lim et al. "Exploring the Relationship between Organizational Culture and Information Security Culture". In: *Proceedings of the 7th Australian Information Security Management Conference* (2009), pp. 88–97. DOI: 10.4225/75/57B4065130DEF.

[24] Adéle Martins and Jan Elofe. "Information Security Culture". In: *Security in the Information Society: Visions and Perspectives*. Boston, MA: Springer US, 2002, pp. 203–214. ISBN: 978-0-387-35586-3. DOI: 10.1007/978-0-387-35586-3_16.

[25] Mark Mason. "Sample Size and Saturation in PhD Studies Using Qualitative Interviews". In: *Forum: Qualitative Social Research*. Vol. 11. 3. Sept. 2010. DOI: 10.17169/fqs-11.3.1428.

[26] Philip L. Morgan et al. *A New Hope: Human-Centric Cybersecurity Research Embedded Within Organizations*. Springer International Publishing, 2020, pp. 206–216. ISBN: 978-3-030-50309-3. DOI: 10.1007/978-3-030-50309-3_14.

[27] Donald Polkinghorne. "Phenomenological Research Methods". In: *Existential-Phenomenological Perspectives in Psychology*. Springer US, 1989, pp. 41–60. DOI: 10.1007/978-1-4615-6989-3_3.

[28] Sriraman Ramachandran, Srinivasan V. Rao, and Tim Goles. "Information Security Cultures of Four Professions: A Comparative Study". In: *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*. IEEE, Jan. 2008. DOI: 10.1109/hicss.2008.201.

[29] Edgar Schein. *The Corporate Culture Survival Guide*. San Francisco, Calif: Jossey-Bass, 1999. ISBN: 978-0-7879-4699-9.

[30] Edgar Schein. *Organizational Culture and Leadership*. San Francisco: Jossey-Bass, 2010. ISBN: 978-0-470-18586-5.

[31] Thomas Schlienger and Stephanie Teufel. "Information Security Culture: The Socio-Cultural Dimension in Information Security Management". In: *Proceedings of the IFIP TC11 17th International Conference on Information Security: Visions and Perspectives*. 2002, pp. 191–202.

[32] Peter B Seddon and Rens Scheepers. "Towards the improved treatment of generalization of knowledge claims in IS research: drawing general conclusions from samples". In: *European Journal of Information Systems* 21.1 (Jan. 2012), pp. 6–21. DOI: 10.1057/ejis.2011.9.

[33] Ken M. Shaurette. "The Building Blocks of Information Security". In: *Information Security Management Handbook*. Boca Raton, London, New York, Washington D.C.: Auerbach Publications, 2004.

[34] P. Shedden, Anthonie B. Ruighaver, and Atif Ahmad. "Risk Management Standards - The Perception of Ease of Use". In: *Proceedings of the Fifth Annual Security Conference* (2006).

[35] Bahareh Shojaie, Hannes Federrath, and Iman Saberi. "The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001". In: *2015 10th International Conference on Availability, Reliability and Security*. IEEE, 2015, pp. 159–167. DOI: 10.1109/ares.2015.25.

[36] Bryan Shorten. "Information Security Policies from the Ground Up". In: *Information Security Management Handbook*. Boca Raton, London, New York, Washington D.C.: Auerbach Publications, 2004, pp. 1269–1280.

[37] Anselm L. Strauss and Juliet M. Corbin. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage Publications, 1990. ISBN: 978-0-803-93251-7.

[38] Kerry-Lynn Thomson and Rossouw von Solms. "Towards an Information Security Competence Maturity Model". In: *Computer Fraud & Security* 2006.5 (May 2006), pp. 11–15. DOI: 10.1016/s1361-3723(06)70356-6.

[39] Basie von Solms. "Information Security — The Third Wave?" In: *Computers & Security* 19.7 (Nov. 2000), pp. 615–620. DOI: 10.1016/s0167-4048(00)07021-8.

[40] Roel J. Wieringa. *Design Science Methodology for Information Systems and Software Engineering*. Springer Berlin Heidelberg, 2014. DOI: 10.1007/978-3-662-43839-8.

[41] Ashleigh Wiley, Agata McCormac, and Dragana Calic. "More Than the Individual: Examining the Relationship Between Culture and Information Security Awareness". In: *Computers & Security* 88 (Jan. 2020), p. 101640. DOI: 10.1016/j.cose.2019.101640.

[42] Mark Wilson and Joan Hash. *Building an Information Technology Security Awareness and Training Program*. Tech. rep. NIST SP 800-50. 2003. DOI: 10.6028/nist.sp.800-50.

[43] Mark Wilson et al. *Information Technology Security Training Requirements: a Role-and Performance-Based Model*. Tech. rep. NIST SP 800-16. 1998. DOI: 10.6028/nist.sp.800-16.

[44] Steven Woodhouse. "Information Security: End User Behavior and Corporate Culture". In: *7th IEEE International Conference on Computer and Information Technology (CIT 2007)*. IEEE, Oct. 2007. DOI: 10.1109/cit.2007.186.