The relation between the organizational information security climate and employees’ information security behavior

J. Timmermans
The relation between the organizational information security climate and employees’ information security behavior

Master thesis submitted to Delft University of Technology in partial fulfillment of the requirements for the degree of

Master of Science

in Complex Systems Engineering and Management
Faculty of Technology, Policy and Management

by

J. Timmermans

to be defended in public on

December 14th, 2018

Student number: 4245229
Thesis committee: Prof. dr. M.J.G. van Eeten, Dr. ir. W. Pieters, Dr. ir. M. Kroesen, MA C. Mattern, TU Delft, Chairperson, TU Delft, First supervisor, TU Delft, Second supervisor, Deloitte Risk Advisory, External supervisor
Preface

This report forms the final and concluding part of my Master of Science in Complex Systems Engineering and Management at Delft University of Technology. I experienced the journey to discover the various factors that contribute to the information security climate and their relation with the behavior of employees, as interesting, intriguing and challenging. Therefore, I enjoyed completing this graduation project.

Hereby, I would like to thank my graduation committee for their time and support to guide me through this project. I particular, I would like to thank Wolter Pieters for the discussions to shape the thesis, his constructive and motivating comments and critical view. I thank Maarten Kroesen, for the inspiring discussions and his expert knowledge in the field of statistics and behavioral modeling and Michel van Eeten for his inspiring feedback.

In addition, I would like to thank Deloitte cyber risk advisory for offering me the opportunity to work on my master thesis in a stimulating environment. Especially the support of Carl Mattern and his practical suggestions brought this thesis to a higher level. By introducing me to the network of Deloitte, I was enabled to interview information security experts. I would like to thank all these experts for their openness and valuable contribution.

Finally, I would like to express my gratitude towards my friends and family, supporting and encouraging me during my study at Delft University of Technology.

J. Timmermans
Delft, December 2018
Management summary

Organizations are frequently facing cyber security incidents, with data breaches increasing in number, complexity and severity. Technical measures to reduce security risks, are in themselves not always sufficient, and security issues due to human actions are causing a substantial percentage of data breaches in organizations (Ponemon Institute LLC, 2018).

Realizing the importance of human behavior to reduce security risks and to safeguard organizations information security, scholars investigated how this human behavior is influenced. This has resulted in a growing, but sometimes conflicting insight in what drives the behavior of employees. Additionally, research on the employees’ information security behavior has a limited dept and is often descriptive, philosophical or theoretical, and results cannot easily be translated to practice (Karlsson Fredrik, Åström Joachim, & Karlsson Martin, 2015). Review of the employees’ information security behavior literature reveals that empirical studies are not always representative nor generalizable for organizations, as the majority of the larger surveys are conducted under students and IT professionals.

The relation of organizational climate factors on employees’ information security behavior is not researched extensively, and often underlaying elements of the organizational climate, such as employee involvement and openness on information security issues, are not further specified in quantitative research. This should provide an answer to the main research question “What is the influence of the organizational information security climate on the information security behavior of employees?” As current research is scarce, often limited in focus, or only qualitative, the focus of this research is to unravel how organizational information security climate factors are related to employees’ information security behavior. For this research, organizational climate is defined as "the [by employees] shared perceptions of organizational policies, practices, and procedures, both formal and informal" (Reichers & Schneider, 1990, p. 22)

To gain insight in factors and mechanisms related to employee security behavior, a combination of qualitative and quantitative methods is used. First a review of organizational climate, safety climate and information security literature is performed, identifying possible factors and underlying mechanisms that influence employees’ information security behavior.

Additionally, different theories and methods to measure employees behavior were explored. The KAB-model, which originates from the social psychology, is suitable to investigate how environmental factors can influence the knowledge, attitude and behavior of employees. This model incorporates the idea that the accumulation of knowledge results in changes in the attitude of individuals. Triggered by the changes in attitude this eventually influence the behavior of individuals (Baranowski, Cullen, Nicklas, Thompson, & Baranowski, 2003; Chaffee & Roser, 1986; Fabrigar, Petty, Smith, & Crites Jr., 2006; Fishbein & Ajzen, 1975). Based on the KAB-model, Parsons et al. (2017) developed the human aspects of information security questionnaire (HAIS-Q) to measure security behavior on a detailed level, with questions on 7 specific focus areas: password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting. Both the KAB model and the HAIS questionnaire are used for the quantitative analysis.

Expert interviews

Semi-structured interviews with 8 information security experts are conducted to identify which organizational IS climate factors are observed to be important in practice. This enables a better alignment of this thesis with practice. The results from these interviews are used to prioritize which factors to include in further research.

The experts for the interviews were recruited via the network of Deloitte in the Netherlands. In total 8 security consultants and company experts are interviewed to get a broad picture based on an inside and outside view. The face-to-face interviews, with an average length of 50 minutes, provide valuable information and insights from practice. Although most of the findings from literature are confirmed, also factors are identified in which literature is not linked with the experiences from the experts.
Additionally, nuance is added to the literature review findings and important complementary insights, some of them scarcely touched in literature, are noted. Experts emphasize that employees are not just a big risk. They are also the human sensors and line of defense of the organization and their input is very valuable to secure the companies’ information.

**Hypotheses**

The insights derived from the reviewed literature, combined with the practical insights from information security experts, form the basis of the conceptual research model. This conceptual model and its underlying hypotheses are used as input for the statistical analysis. A challenge for the development of the conceptual model is to capture enough detail to explain the employee IS behavior, while keeping the model as parsimonious as possible. From the broad spectrum of factors identified, only a selected number of variables is included for further quantitative analyses, due to restrictions in resources and parsimony. This selection of these factors is determined on the expected importance and influence on employees IS behavior. Additionally, factors which require more research because of limited or contradicting findings are included. This results in the following factors and hypotheses:

- **H1**: Information security education and communication is, via improved knowledge, positively related to employees’ behavior
- **H2**: Openness on information security is, via improved knowledge and attitude, positively related to employees’ behavior
- **H3**: Employee involvement is, via improved knowledge and attitude, positively related to employees’ behavior
- **H4**: Work impediment is negatively related to employees’ attitude and behavior
- **H5**: Perceived management commitment is positively related to employees’ attitude and behavior
- **H6**: Task orientation is positively related to employees’ attitude and behavior

The security behavior of employees can be analyzed in several ways. The most objective way is to measure the actual behavior via observation of employees. However, it is very difficult to capture all aspects of information security (e.g., password strength) and underlying motivations via observations (Lebek, Uffen, Neumann, Hohler, & Breitner, 2014). Additionally, many companies are reluctant to share IS related information, due to its sensitive nature (Kotulic & Clark, 2004). A strong relation between behavioral intention and the actual behavior is reported in the literature (Lebek, Uffen, et al., 2014). Therefore, the self-reported behavioral intention via a questionnaire is used.

**Measuring organizational climate**

Similar to the measurement of the security behavior, the by the employee reported state of the organizational climate factors is considered. Hereby, the actual experience of the employee is captured, rather than observed values or values reported in formal documents, like organizational charts. This approach allows for a broader selection of different companies, as not all company related information must be collected manually, but can be derived from the survey. Additionally, combined with the anonymous processing of the data, this can decrease the chance of social desirability bias (Bradburn et al., 1979; Nederhof, 1985; Paulhus, 1984). Each of the included organizational climate factors is measured with multiple questions to increase the measurement accuracy. Both the behavioral and the organizational climate statements contain the same 5-point Likert answering scale, which ranges from strongly disagree to strongly agree.
Data analysis
The respondents are recruited via the crowd-sourcing platform Amazon Mechanical Turk (AMT). First a qualification survey was sent out to 2000 workers selected of AMT which meet criteria such as an approval rate of previous work above 98% and an experience of at least 100 assignments. The qualification survey contained questions on current employment, company size, company IS requirements and computer use. From the 2000 workers a total number of 723 met the sample requirements. The latter group was targeted via their worker id to fill out the final survey, for which 325 spots were available. In addition to the qualifications needed to fill in the questionnaire, checks on the respondent attention and consistency were included in the questionnaires. This resulted in 289 usable responses.

The collected data is statistically analyzed with structural equation modeling (SEM). SEM is a family of statistical models which can be used to analyze the dependence relationships among multiple factors (Hair, Black, Babin, & Anderson, 2010; Kline, 2010). It consists of a combination of a measurement model and a structural model. The measurement model, which is based on factor analysis, is used to assess the representation of the unobserved factors (also known as latent constructs) by the observed indicator variable (statement used in the questionnaire). For the structural model a path analysis is used to analyze the significance and strength of the interrelationships between those latent constructs. For both the measurement and the structural model, assumptions and modeling choices are made.

A factor analysis is used to analyze the measurement model. This is done via an exploratory factor analysis (EFA) and a confirmatory factor analysis (CFA) (Kahn, 2006). To measure each specific factor, multiple statements per (intended) factor are made. Based on the analysis, the organizational climate factor “task” is excluded. This results in a model with 5 organizational climate factors, which is used for further analysis. To increase the model fit some of the relations of the original model are revised, based on the input of expert interviews or supported by theory. The most important changes in the revised model are the relations from education & communication and involvement to work impediment.

All relations as shown in the revised model are significant. From the organizational climate factors, education has by far the largest total effect. Surprisingly, the effect of management commitment and involvement is quite low.
Conclusion
The main research question “What is the influence of the organizational information security climate on the information security behavior of employees?” can be answered with this research. The organizational climate of a company can be characterized by many different factors. A qualitative analysis is performed with an extensive review of safety climate and information security literature, followed by semi-structured interviews with 8 security experts. This analysis resulted in a set of organizational climate factors which are suggested to influence employee information security behavior. Based on a quantitative analysis of these factors, using structural equation modeling, the following organizational climate factors are found to have a significant relation with the information security behavior of employees.

The strongest significant positive relation is found between IS education & communication and knowledge. The factor knowledge on its turn positively relates, via attitude, to the self-reported behavior of employees. Education and communication have also a significant negative relation to work impediment. These findings, which support the first hypothesis, are in line with findings reported in the IS literature and input from security experts. The latter emphasize the importance of frequent and relevant training and communication.

IS education and communication also have a significant negative relation to work impediment. This relation is addressed by some security experts, stating that education can contribute to more insight in the vulnerabilities of the organizations, which result in improved understanding and acceptance of the required measures. Additionally, IS education can improve the skills of employees, thereby decreasing the effort needed to perform certain security handling, which explains the reduction of work impediment. These findings are confirmed in safety climate literature, and indirectly in IS literature.

Openness on information security risks and (near) incidents is significantly and positively related to employees’ behavior, albeit not directly via increased attitude, but only via knowledge, resulting in a partly supported hypothesis. Experts mention the importance of openness to increase employees' knowledge, attitude and IS behavior. Additionally, an atmosphere which allows for openness on information security risk and issues can improve the attitude and behavior of employees. Though, despite the presumed benefit, it remains difficult to obtain wide acceptance for openness in practice. The openness on security errors and risks as operationalized in this study is barely touched in the IS literature.

However, it is identified as an important driver of safety in the safety climate literature. More research within the field of information security on the effect of openness on IS risks and error could be interesting as the total effect is quite large and the IS literature on this factor is scarce.

Another interesting finding is the significant, but relatively weak, negative relation between the work impediment on the behavior of employees. IS experts mention that work impediment is one of the most important triggers for non-complaint behavior. Therefore, reducing work impediment by increasing the ease of use of the security measures is suggested to be important. Though the relation of work impediment with employee behavior is not strong, it still provides evidence for the fourth hypothesis. Concluding, the significance of the relation between work impediment and behavior is in line with the findings from literature and practice.

As expected from the analysis of the literature and expert interviews, the model shows a significant relation between management commitment and employees’ attitude. In comparison with the direct effect of education & communication, the direct effect of management commitment is rather low. However, management commitment is also crucial for education, communication and openness. Although not extensively researched, this positive relation of management commitment is confirmed by scholars. During the interviews the experts indicated that management commitment is critical. When this commitment lacks, this will
directly negatively influence the IS behavior of employees. The commitment of management can also make a positive difference, for example by emphasizing the importance of IS for the business and leading by example. Despite the limited strength of the relation, the hypothesis 5 is still supported via the significant relation in the estimated model.

Unfortunately, hypothesis 6, regarding the relation between task orientation and employees' behavior could not be analyzed, due to reliability issues, combined with discriminant and convergent validity problems.

Overall it can be concluded that the organizational climate, in this research represented by education and communication, managerial commitment, employee involvement, openness on IS and (reduction of) work impediment, is positively related to, and thereby likely to influence, the information security behavior of employees.

**Limitations**

Like all research, this research has its assumptions and limitations. Although countermeasures for methodological limitations have been used, some limitations remain.

The first limitation is related to the expert interviews. To integrate insights from practice, expert interviews were conducted with 8 information security experts from different companies in the Netherlands. The number of interviewed experts is too small to be representative for the whole population. Additionally, all interviewed experts work at companies which have attention for information security, which is clearly visible from the levels of IS maturity. The latter also has its advantages, as the experts of those companies have a high level of expertise. Due to the sensitive nature of the topic, experts can be reluctant to fully disclose the limitations with regard to managing the IS behavior of their employees. To reduce this possible bias, all interviewed experts were promised anonymous processing of their statements.

Most information security experts fulfill a role of ensuring IS of the company. Thereby, they are likely to have a different perspective on IS than the employees themselves. To incorporate other perspectives, information security consultants were also interviewed, as these consultants can provide an outside view. The view of employees is captured via the questionnaire among employees. Because of time and budget constraints, this questionnaire was targeted to US employees. This difference between nationalities of experts and employees could have influenced the research results, though the international focused role of some experts can partly compensate this difference.

Another limitation can be found in the quantitative analysis, where data collected via an online questionnaire was used. The measurement of IS behavior is based on self-reported behavior of employees. To limit different interpretations on “secure” or compliant IS behavior, a more granular measurement based on the HAIS questionnaire, was used. Although a link between behavioral intention and actual behavior is mentioned in the literature (Lebek, Uffen, et al., 2014), this cannot be guaranteed and verified for the sample. To increase the likelihood of fair responses, anonymous processing of the responses was promised to the respondents.

The HAIS questionnaire also has some shortcomings. The formulation of some HAIS statements seems to be outdated (e.g. focus on paper based information in the information handling focus area and not including a password manager or two factor authentication in the password management focus area). Additionally, the correlation between the knowledge and attitude items is very high. A possible explanation is the use of normative language in the knowledge items, which results in overlap with the attitude statements.

The respondents for the questionnaire were recruited via Amazon mechanical turk (AMT). Using AMT for academic research, and especially the representation of AMT workers for the population, can be challenging. To improve the sample quality, a qualification survey was used to determine which respondents are part of the targeted population. An important design choice is to only include respondents which reported that their employer has some form of information security requirements. Thereby, employees of companies which do not do anything on IS are excluded. This is done based on the argumentation that a certain level of IS maturity is required before working on the organizational climate. However, one could argue that this may result in a certain bias on the selection of respondents. Additionally, in comparison with the data of the US bureau of labor statistics, the sample contains relatively many respondents in the age category of 30-39 years old. Although it can partly be caused by the sample requirements, it is important to keep this in mind for the generalization of the results.
The final limitation can be appointed to the development of the research model, in which a trade-off had to be made between capturing enough detail and being as parsimonious as possible to increase generalizable. It is simply not feasible and desirable to include every possible factor and relation which could influence employees behavior in the model. Therefore, a selection was made based on the findings from the literature review and expert interviews. With the current research setup it is not possible to statically determine the causality of the relations. The expert interviews and literature do give insights in the likely directions of the causalities. However, more research is required to statistically prove these causalities.

**Recommendations**

Finally, based on the findings from both the qualitative and quantitative analyses, recommendations for organizations and scholars in the field of information security are formulated. Organizations can use these recommendations to improve and strengthen their information security climate and thereby the employees’ information security behavior in the organization. It is important to realize that, although some of recommendations seem to focus on the perception of individual employees, the combination of all employees’ experiences en perceptions are forming the information security climate within an organization.

Summarized, the following recommendations for organizations are derived:

- Facilitate training about security rules and measures on a regular base, offering practical information in small chunks and related to the daily practice
- Communicate frequently about actual and appealing information security topics
- Provide openness about (near) incidents and the current information security threats of the company
- Involve employees to improve information security measures and to find practical and user-friendly solutions
- Demonstrate that management is committed and leading by example
- Ensure that information security gets enough priority and is considered as an integral part of all business decisions and projects

It requires investments in time, money and trust of the management to create an organizational climate in which the employees are not seen as the biggest risk. Employees are the human sensors of the organization, and the first line of defense. Therefore, with the support and commitment of management, employees can positively contribute to the information security of the organization.

By providing education and information, involving employees where possible, creating openness, and embedding information security in all business activities, the combined effort from the whole organization can help to build a strong information security climate and to reach a higher level of information security.
Contents

1 Organizational climate and employee information security behavior 1
  1.1 Research problem. ............................................................... 1
    1.1.1 Problem exploration .................................................. 1
    1.1.2 Knowledge gaps ....................................................... 4
    1.1.3 Research scope ....................................................... 4
    1.1.4 Problem statement .................................................... 4
    1.1.5 Objective and deliverable ........................................... 4
  1.2 Research questions ......................................................... 4
  1.3 Relevance .......................................................................... 5
    1.3.1 Scientific relevance .................................................... 5
    1.3.2 Societal relevance ...................................................... 5
    1.3.3 Fit with master program .............................................. 5
  1.4 Research approach .......................................................... 6
  1.5 Thesis outline ................................................................. 6
    1.5.1 Organizational factors and employee information security behavior .................................. 7
    1.5.2 Employee information security behavior in practice ....................................................... 7
    1.5.3 Conceptualizing employee security behavior ............................................................... 7
    1.5.4 Modeling and analyzing employee behavior ............................................................... 7
    1.5.5 Bringing all elements together ....................................... 7

2 Organizational climate and employee behavior 8
  2.1 Methodology ................................................................. 8
  2.2 Organizational climate ..................................................... 8
  2.3 Safety climate .............................................................. 9
  2.4 Conclusion ................................................................. 11

3 Employees' information security behavior 13
  3.1 Methodology ................................................................. 13
  3.2 Security awareness and behavior .................................... 13
    3.2.1 Security awareness and knowing-doing ......................................................... 14
    3.2.2 Security awareness and employees' attitude ................................................. 14
  3.3 Theories and models on employees' information security behavior. .................................. 14
    3.3.1 Theory of reasoned action and planned behavior ............................................. 15
    3.3.2 Protection motivation theory .............................................. 15
    3.3.3 General deterrence theory .............................................. 16
    3.3.4 Technology acceptance model ........................................... 16
    3.3.5 Knowledge, attitude and behavior model ............................................... 16
    3.3.6 Measuring behavior ..................................................... 16
  3.4 Conclusion ................................................................. 17

4 Organizational climate and employee information security behavior 18
  4.1 Methodology ................................................................. 18
  4.2 Management ............................................................... 18
    4.2.1 Management support .................................................. 19
    4.2.2 Management commitment ............................................. 19
    4.2.3 Management participation .......................................... 19
    4.2.4 Transformational leadership .......................................... 19
    4.2.5 Key findings ........................................................... 20
4.3 Knowledge and awareness improvement measures ........................................... 20
  4.3.1 ISP provisioning and quality ................................................................. 20
  4.3.2 Training and internal communication ................................................... 20
  4.3.3 Key findings ......................................................................................... 21
4.4 Employees' capabilities and risk perception ....................................................... 21
  4.4.1 Risk perception ..................................................................................... 21
  4.4.2 Employees' capabilities and impact of risk mitigation measures ............... 22
  4.4.3 Key findings ......................................................................................... 24
4.5 Social environment .......................................................................................... 24
  4.5.1 Organizational environment .................................................................... 25
  4.5.2 Influence of colleagues ........................................................................... 26
  4.5.3 Bond with the organization .................................................................... 27
  4.5.4 External influences ................................................................................ 28
  4.5.5 Key findings ......................................................................................... 28
4.6 Other factors .................................................................................................... 29
  4.6.1 Age & gender ......................................................................................... 29
  4.6.2 Personality ............................................................................................. 29
  4.6.3 Education, knowledge and experience ................................................... 29
  4.6.4 Job ........................................................................................................ 29
  4.6.5 Company characteristics ........................................................................ 29
  4.6.6 Key findings ......................................................................................... 29
4.7 Conclusion ........................................................................................................ 29
5 Expert interviews ................................................................................................ 31
  5.1 Interview approach ...................................................................................... 31
  5.2 Coding process ............................................................................................ 31
  5.3 Results ......................................................................................................... 32
    5.3.1 Management ........................................................................................ 33
    5.3.2 Knowledge and awareness improvement measures ............................. 33
    5.3.3 Employee capabilities and risk perception ........................................... 34
    5.3.4 Organizational characteristics ............................................................ 35
    5.3.5 Organizational & social environment ................................................ 35
    5.3.6 Cause of incidents ............................................................................. 36
  5.4 Conclusion .................................................................................................... 37
  5.5 Relation between literature and practice ....................................................... 38
6 Research model .................................................................................................. 39
  6.1 Level of detail .............................................................................................. 39
  6.2 Types of behavior (dependent variables) ........................................................ 39
  6.3 Theoretical basis ......................................................................................... 39
  6.4 Organizational climate (independent variables) ............................................. 40
    6.4.1 Variables included in the model ............................................................ 40
    6.4.2 Variables not included in the model .................................................... 41
  6.5 Conclusion .................................................................................................... 42
7 Methodology of quantitative analysis ................................................................ 43
  7.1 Methodology: measuring employee behavior & organizational climate ............. 43
    7.1.1 Measuring employee behavior ............................................................. 43
    7.1.2 Measuring organizational climate ....................................................... 43
    7.1.3 Collecting responses .......................................................................... 43
    7.1.4 Questionnaire outline ....................................................................... 44
    7.1.5 Test questionnaire .............................................................................. 44
  7.2 Data collection .............................................................................................. 44
    7.2.1 Population .......................................................................................... 44
    7.2.2 Sample ............................................................................................... 45
Organizational climate and employee information security behavior

Organizations are frequently facing cyber security breaches, which are increasing in number, complexity and severity. These breaches not only cause substantial economic damage, but also lead, via public scrutiny, to customer retention and business opportunity losses (Cisco, 2018). Dealing with these (potential) data breaches is quite challenging for organizations, especially due to the complex and fast changing environment with a big variety of both internal and external stakeholders and complex political dynamics (Tisdale, 2015).

Until recently, the primary focus within the information security field, was to reduce these risks via technological measures. However, those measures are in themselves not sufficient without effort of employees to reduce security risks (Bulgurcu, Cavusoglu, & Benbasat, 2010; Spears & Barki, 2010). Not all security risks can be avoided by technical measures. For example, a phishing attack is sometimes not detected by a spam filter. These employees are often considered as a high security risk factor for the security of information systems (Sasse, Brostoff, & Weirich, 2001; Siponen, 2000b; Spears & Barki, 2010; Warkentin & Willison, 2009).

An analysis from Verizon (2017) revealed that social engineering attacks are used in 43% of the breaches. Another study, on a select number of countries, showed that human errors are the cause of 18 to 35% of the data breaches in 2018 (Ponemon Institute LLC, 2018). Therefore, the consideration of the human aspects of information security is important to reduce cyber risks.

To deal with the human related risk, many companies have adapted information security policies and invested in training programs and campaigns to educate employees and raise their knowledge level on the security of information (Bulgurcu et al., 2010). However, an increased knowledge level is not always resulting in compliant information security behavior of employees (Lee et al. 2004).

As stated by Cram, Proudfoot, and D’Arcy (2017, p. 605) "security issues originating from employee actions remain a persistent problem for today’s organizations". Therefore, more research on how organizations can close the gap between their employees’ information security knowledge and the actual employee information security behavior is needed.

In this chapter the problem is further explored to define knowledge gaps which form the basis for the formulation of a problem statement. Based on this problem statement the research objective and research questions are formulated. After a discussion on the relevance, the research approach is described. Finally, the outline of this thesis is provided.

1.1. Research problem

1.1.1. Problem exploration

Realizing that human behavior is really important to reduce security risks and to safeguard organizations’ information security, several scholars have investigated how this human behavior is influenced. These analyses are based on a variety of social psychology theories and behavioral principles. This results in a growing, but sometimes conflicting insight in what drives the behavior of employees. The importance of human behavior for information security did not only gain attention of academics but also from organizations. Therefore,
organizations try to improve employee behavior by implementing information security policies, in which they define the standards, rules, boundaries and responsibilities of employees (Bulgurcu et al., 2010; Lowry & Moody, 2015). Additionally, employees receive training to increase their information security knowledge and understanding of these policies. In the context of this thesis, knowledge is defined as "the theoretical or practical understanding of a subject, fact, information, value or skills achieved through education or experience" (Safa, Von Solms, & Furnell, 2016, p. 72).

As illustrated in figure 1.1, a higher level of information security knowledge is related to an increased level of information security awareness. On its turn, awareness is mentioned to be an important factor which affects the attitude of employees to perform compliant behavior (Flores, Holm, Nohlberg, & Ekstedt, 2015; Parsons et al., 2017; Safa & Von Solms, 2016). Besides the beforementioned factors, research also suggests that in practice many other variables, under which the organizational culture and climate, might influence employee behavior. Before discussing these factors, first the definition of information security awareness and attitude, as used in this thesis is given.

**Attitude:** The degree to which the performance of the by the company required information security behavior is positively valued (Ajzen, 1991; Bulgurcu et al., 2010; Fishbein & Ajzen, 1975).

**Awareness:** Employees’ cognitive ability to recognize and understand information security threats and risks in the context of their organization’s information security requirements (Bauer & Bernroider, 2017; Bulgurcu et al., 2010).

---

The knowing-doing gap

The relationship between knowledge and behavior, is not as straight as suggested by some scholars. Research on the gap between knowing and doing reveal that also many other variables, such as social and personal norms are influencing the intended and actual behavior of employees (Bauer & Bernroider, 2017); (Cox, 2012).

In their latest report ENISA (2017) also refers to this discrepancy between employees’ knowing and doing. They state that human factors should not be ignored in order to successfully deploy cybersecurity policies. Sometimes the rules are not followed due to a lack of understanding of prioritization, simply because employees want to "do their job". An example is that in a hospital emergency department the computers are left "logged-in" in order help patients immediately and potentially save lives, despite this is against the security policy. Thus, only focusing on measures to improve knowledge is not enough to ensure compliant employee behavior. Therefore, more insight in the mechanisms and variables driving employee behavior is needed.
1.1. Research problem

Drivers of employee behavior
Organizational factors, such as managerial commitment and peer behavior are suggested to play an very important role on the behavior of employees in general (Porter & McLaughlin, 2006; Schneider, Ehrhart, & Macey, 2013). Therefore, this research will focus on the influence of organizational factors on the information security behavior of employees.

The relation of organizational factors on employees’ information security behavior has been studied by several scholars, a few of them focusing on organizational climate, and some other on the relation of organizational culture. Both factors are not researched extensively, and often underlaying elements of climate or culture are not further specified in quantitative research. Research has a limited dept and is often descriptive, philosophical or theoretical, therefore results cannot easily be translated to practice (Karlsson Fredrik et al., 2015).

The terminology culture and climate is often interchanged by scholars, due to their close relationship and various viewpoints among scholars. However, there are also clear differences. The organizational culture is related to the intangible elements, such as values, beliefs and norms that an organization develops over a long time. The organizational climate however, is more dynamic and determined by more tangible factors such as management support, procedures and recognition, which relates to the actual atmosphere and work practice in the organization. Changing and influencing the organizational climate is relatively easy. This in contrary to changing the organizational culture, which can take many years (Schneider et al., 2013).

For this thesis the following definitions for organizational culture and climate are used:

**Organizational climate**: “The [by employees] shared perceptions of organizational policies, practices, and procedures, both formal and informal” (Reichers & Schneider, 1990, p. 22).

**Organizational culture**: "A pattern of shared basic assumptions that was learned by a group [i.e. an organization] as it solved its problems of external adaptation and internal integration, that has worked well enough to be considered valid and, therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.” (Schein, 2004, p. 17).

Literature reviews reveal that some organizational factors, e.g. organizational values, norms and security training are generally showing a positive relationship with employee behavior. The findings on managerial support are however conflicting. Although, mostly a positive association with compliance is reported, also neutral or even negative relationships are found (Cram et al., 2017; D’Arcy & Greene, 2014; Q. Hu, Dinev, Hart, & Cooke, 2012).

Unfortunately, an extensive literature review, to identify and understand which organizational factors are influencing the information security awareness of employees in organizations, did not provide insight in the relation of these factors with employee behavior (Haeussinger & Kranz, 2017). The empirical evidence for the influence of managerial information security support, awareness and commitment on the awareness of employees was not provided in any study. This in contrary to the behavior of peers and colleagues, which was identified as an important factor of influence on the awareness of employees.

Another remarkable finding in reviews of employees’ information security behavior literature is that empirical studies are not always representative for organizations. This because the majority of the larger surveys were conducted under students and IT professionals. Therefore, scholars state that more research in an organizational context is needed (Lebek, Uffen, et al., 2014).

Such a more in depth research on organizational factors was performed by Connolly, Lang, Gathegi, and Tygar (2017) with a qualitative study under employees in the US and Ireland. The organizational factors insights, solidarity, task orientation and a flat structure are suggested to have a positive relation with employee information security behavior (Connolly et al., 2017). Despite the fact that Vroom and von Solms (2004) already predicted in 2004 a strong relationship between organizational factors and employees’ information security behavior, Connolly et al. (2017) conclude that research on the influence of organizational factors is scarce. Therefore, they call for more research, under which a quantitative analysis of their results of their qualitative research.
Summarized, more research to understand the relation of organizational IS climate factors on employee information security behavior is required. Current research is scarce, often limited in focus, or only qualitative. Therefore, the focus of this research will be to unravel how organizational information security climate factors influence employees’ information security behavior.

1.1.2. Knowledge gaps
From the previous section it becomes clear that, although quite some research is performed to understand what triggers employee information security behavior, there is a broad variety in approaches, definitions, constructs and findings. From the reviewed literature the following knowledge gaps are derived:

- The relation between the organizational information security climate and employee information security behavior is not fully understood and study results on what encourages and motivates employees to comply (or not) with the information security requirements are conflicting or inconclusive. Next to this, research on the influence of specific organizational climate characteristics, such as security training, management commitment, job attitude and peer behavior is scarce or only qualitative.

- Research is often performed with students or IS professionals, but they are not representative for the behavior of employees in a business environment.

1.1.3. Research scope
Based on the identified knowledge gaps, this research will focus on the relation of the organizational climate on the information security behavior of employees. Research also indicates that individual factors and national culture could influence employees’ security behavior (Connolly et al., 2017; Dinev, Goo, Hu, & Nam, 2009; Hovav & D’Arcy, 2012). Unfortunately, due to time constraints it is not possible to cover all of these factors in this thesis. Therefore, the influence of the national culture is eliminated by focusing on a single country.

1.1.4. Problem statement
To reduce security incidents caused by human behavior, organizations developed information security training programs and policies. However, human errors still account for a large portion of the security incidents. Several scholars have researched which factors and mechanisms influence the security behavior and compliance of employees. However, research on organizational climate factors and their relation with employees’ information security behavior is still limited and inconclusive. Therefore, additional research is needed to investigate these elements and underlying mechanisms.

1.1.5. Objective and deliverable
The objective is to provide insight in which organizational climate characteristics are influencing employees’ security behavior in an organizational setting. The identified characteristics could be used to increase the effectiveness of security interventions and employees’ security behavior.

1.2. Research questions
Based on the problem statement the following research question is formulated:

**Research question:** What is the influence of the organizational information security climate on the information security behavior of employees?
The following sub questions are used to answer the main research question. In the next chapter the methodological approach for each sub question is discussed.

**Sub-questions:**

1. Which factors and mechanisms that influence employees’ behavior are described in the organizational climate and safety climate literature?
2. Which theories are used to explain employees’ information security behavior?
3. Which factors and processes that influence employees’ information security behavior are described in the literature?
4. Which of the identified (and additional) factors and processes are observed in practice by information security experts?
5. What is the relation, effect and magnitude of the factors and processes identified in literature and practice with employee behavior?

### 1.3. Relevance

In this section the scientific and social relevance of the research are discussed. Additionally, the embedding of the study with the CoSEM is curriculum is addressed.

#### 1.3.1. Scientific relevance

This research will contribute to the academic literature by providing insight in the relation between the organizational climate and employee security behavior. The combination of qualitative research via a review of the literature and expert interviews, to identify possible influencing factors, with quantitative empirical research, via a survey, contributes to a better understanding of what triggers employees’ information security behavior. The identification, formulating and statistically testing of influencing organizational climate characteristics will add to the currently scarce amount of quantitative scientific research on the influence of the organizations’ climate on employee information security behavior in a business environment.

#### 1.3.2. Societal relevance

The societal relevance of this research is that it will add some pieces to the puzzle of what drives employee security behavior. Improved insights from this study can be helpful to identify influential organizational climate factors which organizations can use to increase their employees’ information security behavior. Organizations could use these insights as input for their information security approach and activities to improve employee security behavior. More compliant employee information security behavior can contribute to a higher information security in organizations. Companies could for example put more emphasis on management commitment rather than just knowledge improvement or involve employees rather than enforcing ISPs via sanctions. Via these improved information security measures, this study can ultimately contribute to a reduction of cyber security incidents due to human behavior.

#### 1.3.3. Fit with master program

A graduation project for a master thesis on Complex Engineering and Management should focus on a socio-technical problem, addressing both technical, ethical and managerial choices. This study fits in these criteria, as it focus on information security and employee behavior in an organizational context. The socio-technical problem central in this thesis is the human aspect in information security, as the behavior of employees in organizations is crucial to protect the information security of companies. Insight on the relation of the underlaying factors of the organizational climate on employee behavior can provide solutions for this socio-technical problem.

The fit with the IA track is made via the data analytics course by constructing and the statistically testing of the research model. The outcomes can be used in organizations to adjust their information security approach and activities in organizations to increase employee information security compliant behavior. Finally, both the social and technical aspects of cyber security as provided in the cyber security specialization, are prominent in this study.
1.4. Research approach

To gain insight in factors and mechanisms related to employee security behavior, a combination of qualitative and quantitative methods is used. Qualitative methods can enable a rich understanding of the factors that contribute to employee IS behavior. Additionally, qualitative research methods can facilitate in the establishment of the research model. A quantitative method, structural equation modeling, is used to empirically test the model. This combination results in a context rich and testable study (Kaplan & Duchon, 1988).

The qualitative analysis starts with a review of the literature, in which possible factors and underlying mechanisms that influence employee information security behavior are identified. The focus of this review is on factors related to the organizational climate.

Thereafter, information security experts are interviewed to increase the alignment of the research with insights from practice. Therefore, factors identified in the literature and other factors which could influence employee information security behavior are discussed. These combined with the findings from the literature form the basis of the conceptual model of this research and its underlying hypotheses. Finally, the conceptual model is quantitatively analyzed with data collected via a survey among employees. The output of the survey is used to determine the significance, effect and magnitude of the hypothesized relation between the identified factors and employee behavior. More specific details on the research methods used per sub-question are shown in table 1.1.

1.5. Thesis outline

In the subsections below a detailed overview of this thesis and the relation of the various chapters to each other is provided. A schematic overview of the research steps and chapters of the thesis is presented in figure 1.2.
1.5. Thesis outline

1.5.1. Organizational factors and employee information security behavior
The organizational climate has proven to have a close relation to employee behavior in general. Therefore, in chapter 2, a review of organizational climate literature, with a focus on what drives employee behavior, is performed. Due to the many similarities of safety climate and information security climate, a special deep dive is made into the organizational safety climate literature. This results in a set of factors and mechanisms influencing employee behavior.

In chapter 3, the theories as used to explain employees’ information security behavior are explored. Additionally, methods to measure this behavior are reviewed. Based on these insights a choice is made on which theoretical basis and measurement are most suitable for further analysis.

The results of an extensive literature review of the research on organizational factors and employee information security behavior is presented in chapter 4. Due to the comprehensive amount of literature reviewed, this chapter is divided in several sub-chapters, each ending with the key findings of the reviewed topic. All pieces are brought together in a final conclusion and an overview of the organizational processes and factors, including their expected influencing effects.

All elements of these three chapters are combined to acquire a total picture of what influences the behavior of employees in an organizational context. These outcomes are used in the next chapter, in which the findings from literature are compared with the experiences in practice.

1.5.2. Employee information security behavior in practice
The before mentioned findings are analyzed via semi-structured interviews with information security experts in chapter 5. First the interview approach and coding process are explained. This is followed by the description of the outcome of the interviews in section 5.3. The insights from the expert interview forms an essential contribution to the choices made for the construction of a conceptual model. This model is used to statistically analyze the relations and underlying hypotheses of organizational factors and employee information security behavior.

1.5.3. Conceptualizing employee security behavior
Based on the output from literature reviews and the practical insights acquired from the interviews with information security experts, a conceptual research model is developed and presented in chapter 6. The considerations, possibilities, limitations and restrictions of the model are discussed. Finally, the model and its hypotheses are presented.

1.5.4. Modeling and analyzing employee behavior
In chapter 7 the methodology to collect and analyze the data that will be used to test the model and its hypotheses are discussed. First the methodology for measuring employee behavior and organizational climate is described, followed by the explanation of the data collection approach. Next, the methodology for analyzing the collected data is discussed.

The results of this quantitative analyses are presented and discussed in chapter 8. After the description of the characteristics of the collected sample, the analysis of the measured model factors is presented. Finally, the results of the SEM-based analysis of the relations between the organizational climate factors and employees’ behavior are presented.

1.5.5. Bringing all elements together
The conclusions of this research, and the relation of the selected organizational climate factors to the behavior of employees are provided in chapter 9. The results of the quantitative analyses are discussed in relation to the reviewed literature and experiences from the information security experts. Based on the SEM-based analysis of the final model, the hypotheses, as formulated in chapter 6, are discussed, together with the limitations of this research. Next the societal relevance and scientific contributions are addressed, followed by recommendations for organizations and suggestions for further research. In the last chapter of this theses report, a reflection on the project and process is provided.
Organizational climate and employee behavior

Before the discussion of the organizational information security specific literature, an analysis on the organizational (safety) climate literature is presented. The amount of information security specific literature on the organizational climate is limited, while there is a rich body of organizational safety climate literature. Organizational safety and information security both focus on the protection of the organizations’ assets. Due to these similarities, the literature of the organizational safety climate can be a valuable addition for this thesis.

Over several decades scholars have researched the organizational climate and the influence of this climate on the behavior of employees. Initially the organizational climate research covered the integrated concept of the majority of the organizational processes and elements. Now, the term culture is used for this concept, whilst climate is used for the manifestation of culture in the organization (Ehrhart, Schneider, & Macey, 2014). In the following paragraphs a comprehensive overview from this organizational climate research is presented. Insights in the mechanisms and models of this climate research can be valuable to identify which elements of the organizational climate are influencing employees’ behavior in general. Given the similarities of the organizational safety climate and the information security climate, specific attention is given to the safety climate literature in relation to employee behavior.

2.1. Methodology
For the review of organizational climate and safety climate literature, several sources are accessed. Searches on Scopus and Google Scholar, using the keywords organizational climate, safety climate in combination with employee behavior, resulted in several articles, white papers, dissertations and books. The search was limited to papers written in English. The publishing date was not an exclusion criterion. The literature achieved via these searches was roughly screened by reading abstracts and book summaries to verify their usefulness. In a second round, full reading was done to identify possible factors and mechanisms that influence employee information security behavior. Additionally, references from literature reviews and papers achieved via a forward and backward search were analyzed. Hereby, especially attention was payed on the well established, often cited, works and authors thereof.

2.2. Organizational climate
The research on how people describe and experience their work environment has followed two different streams; research on the organizational climate and research on the organizational culture.

Although research on organizational climate or organizational culture followed a separate and different track, with other researchers and methodologies and nearly no integration, the two constructs have many similarities. They both focus on the shared experiences of employees, the role of leadership and the how the organizational context relates to the effectiveness of the organization (Schneider et al., 2013). However, also big differences can be noted. Climate research is rooted in psychology, with a focus on surveys and quantitative analyses, while culture research is based on anthropology, and the use of qualitative methods. The focus of climate research is mainly related to the tangible elements, such as policies, practices and procedures and how employees experiences management initiatives in their daily work, bringing insights in how managers can influence behavior (Denison, 1996). Culture research is broader and relates to the more intangible norms, values and assumptions of an organization. Recent climate research is giving more attention to specific process climates, for example safety or service climates, where culture research is often more generic and less
focused. Another clear difference is the potential of change. Changing the culture with values and assumptions in an organization is, in comparison with changing an organizations’ climate, more difficult and can take many years. As stated earlier, this research will focus on the influence of tangible organizational climate factors on the behavior of employees. Additionally, specific safety climate research is reviewed.

The definition which is used in this research to describe organizational climate is: "the [by employees] shared perceptions of organizational policies, practices, and procedures, both formal and informal" (Reichers & Schneider, 1990, p. 22)

Empirical research on the organizational climate started late 1960s and addressed the generic environment in the organization. In 1975 Schneider introduced the focused climate research and stressed that the predictive value of climate measure could be much stronger if research was focused on specific aspects of the environment (Schneider, 1975). This view was supported by several researchers and the focused climate construct was broadly applied with studies on different organizational processes and strategic streams, such as safety and service climate.

This climate research has given good insight in how the organizational environment can play a role in employees’ behavior. In their extended climate literature research reviews Kuenzi and Schminke (2009) and Ehrhart et al. (2014) found strong relationships between a positive job attitude and employee behavior and the organizational climate. Specific climates, such as safety and ethical climates were statistically positively correlated with safety violation rates and unethical behavior. They also found evidence for the potential of managers to affect the organizational climate, due to their interpretation and filtering of the relevant processes and practices for their group members. This influence of leadership is one of the most important and frequently studied variables. Next to the above described factors, the climate strength plays a role, where factors as leadership, team diversity, social interaction and the size and cohesiveness of groups are identified as important influencers of this strength. A higher interaction, more communication in the team and with the leaders and a shared and clear strategic vision leads to a stronger climate (Schneider et al., 2013).

2.3. Safety climate

A specific organizational climate is the safety climate. Organizational safety and information security are both important to protect the organizations’ assets. Due to these similarities, also the literature from safety climate research is reviewed.

As mentioned before, many scholars have researched the field of organizational safety climate to unravel the mechanisms influencing safety behavior (Zohar, 2010). A review of safety climate research shows that initially the organizational climate research covered the integrated concept of the majority of the organizational processes and elements. Currently, scholars use the term culture for this concept, whilst climate is used for the manifestation of culture in the organization. Reviewing 30 years of safety climate research, Zohar (2010, p. 1517) concluded that “we have achieved an enormous task of validating safety climate as a robust leading indicator or predictor of safety outcomes across industries and countries”. Indeed, his research on organizational climate, safety climate and employee behavior reveals a range of factors as important elements of a safety climate. Zohar (1980) was one of the fist scholars to identify influencing safety climate factors. He reported that safety and training programs, safe conduct on promotion, the required work pace on safety, level of risk, social environment, management attitude, and the status of the safety officer and safety committee are all contributing to the safety climate and employee behavior.

Griffin and Neal (2000) demonstrated a positive relation of the organizational climate on the safety climate, and from the safety climate on employees’ knowledge and motivation. This increased knowledge and motivation did on its turn lead to higher safety compliance. In their research they identified the following influencing factors: management values and practices (e.g. training, safety provision, quality of systems and attention for personal well-being), communication and employee involvement (Neal, Griffin, & Hart, 2000). Results of a longitudinal study during 5 years on safety climate, motivation and behavior in relation to accidents, showed that self-reported safety behavior had a predictive validity (Neal & Griffin, 2006).

This growing evidence of safety climate as a predictor for safety behavior is also mentioned by Kines et al. (2011). Based on the research of many scholars, Kines et al. (2011) developed and validated an safety climate questionnaire. They defined safety climate as “workgroup members shared perceptions of management and
workgroup related safety policies, procedures and practices” (Kines et al., 2011, p. 634). In this 50 elements counting questionnaire, 7 safety climate dimensions are defined: 1) management safety priority, commitment and competence; 2) management safety empowerment; 3) management safety justice; and the shared perceptions of 4) workers’ safety commitment; 5) workers’ safety priority and risk non-acceptance; 6) safety communication, learning, and trust in co-workers’ safety competence; and 7) workers’ trust in the efficacy of safety systems (Kines et al., 2011). This questionnaire will be used as valuable input for a survey of the information security climate.

A visualization of the aspects of safety in an organizational environment was proposed with the safety climate/culture model from Cooper (2000). This model has proven to be of practical support for organizations to improve their safety environment and optimize accident prevention (Cooper, 2000, 2016; Ehrhart et al., 2014; Flin, Burns, Mearns, Yule, & Robertson, 2006).

![Figure 2.1: Reciprocal Safety Culture Model adopted from (Cooper, 2000, p. 120)](image)

This model reflects the dynamic interaction of the behavioral, situational and psychological or personal aspects. These three elements are all influencing each other, but the strength of the aspects may be different, depending the context or situation. The personal, or psychological aspects are elements such as personal values, attitudes, subjective norms and perceptions. The situational aspects encompass the characteristics of the safety climate and culture. Cooper (2016) states that although psychological aspects should not be ignored, focusing on the behavioral and situational aspects can really contribute to reduce safety issues. Therefore he suggest to focus on the six organizational culture/climate characteristics which he identified in his review of the safety culture and climate literature: management and supervision, safety systems, risk, work pressure, competence and procedures and rules.

An overview of these characteristics, including underlying elements is presented in table 2.1. In the third column, the results of a public inquiries on industrial safety disasters are presented, showing clear relations with many of the identified characteristics.
<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Academic Summary</th>
<th>Results of Public Inquires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management / Supervision</td>
<td>i. Management attitudes, commitment, and actions regarding safety, (Senior, Middle, and Front-line management) ii. Management concern for employee well-being</td>
<td>i. 'Ineffective leadership', where leadership and the prevailing corporate culture prevented the recognition of risks and opportunities, leading to wrong safety decisions being made at the wrong time, for the wrong reasons ii. Blame Culture', so that problems remained hidden as they were driven underground by those trying to avoid sanctions or reprimands</td>
</tr>
<tr>
<td>Safety Systems</td>
<td>i. Effectiveness of safety communication within the organization ii. Availability of safety instructions iii. Availability of personal protective equipment iv. Status of safety people and safety committees within an organization</td>
<td>i. 'Miscommunicating', where critical safety information was not relayed to decisionmakers and/or the message had been diluted ii. 'Ignoring 'lessons learned', where critical safety information was not extracted, shared, or enforced</td>
</tr>
<tr>
<td>Risk</td>
<td>i. Employees risk perception ii. Satisfaction with safety measures iii. Control over one's own safety on the job iv. Beliefs about accident causation</td>
<td>i. 'Inattention to Risk' - Not recognizing down-playing or dismissing the significance of particular hazards and risks</td>
</tr>
<tr>
<td>Work Pressure</td>
<td>i. Perceived status of safety targets relative to production pressures ii. Effects of the required work pace iii. Effects of job induced stress iv. Conflict among co-workers</td>
<td>i. 'Profit coming before safety', where productivity always came before safety, as safety was viewed as a cost, not an investment</td>
</tr>
<tr>
<td>Competence</td>
<td>i. Importance and effectiveness of safety training</td>
<td>i. 'Competency failures', where there were false expectations that direct hires and contractors were highly trained and competent</td>
</tr>
<tr>
<td>Procedures / Rules</td>
<td>i. Existence and effectiveness of safety rules and procedures</td>
<td>i. 'Non-compliance' to standards, rules and procedures by managers and the workforce</td>
</tr>
</tbody>
</table>

### 2.4. Conclusion

A review of the literature of organizational climate research provide valuable insights in the role of leadership and the organizational context on the behavior and shared experiences of employees. Climate research is mainly related to the tangible elements, such as policies, practices. A strong relationship between the organizational climate and employees’ job attitude and behavior is confirmed in many studies (Ehrhart et al., 2014; Kuenzi & Schminke, 2009).

Specific research on the influence of the safety climate on employees’ behavior reveals more detailed information. Based on this research, several characteristics of the climate of organizations are identified to influence security behavior. Although scholars sometimes use slightly different words to describe a specific climate factor, these factors can be classified in the following general categories:

- Management related factors
- Training and communication
- Risk and work pressure related factors
- Social environment and employee related factors
An overview of the safety climate factors as identified in literature is presented in Table 2.2.

Table 2.2: Summary identified safety climate factors

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supervision</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attitude</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Priority and commitment</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Values &amp; practices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Empowerment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Justice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training &amp; communication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training programs</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Communication &amp; trust</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedures &amp; rules</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td></td>
</tr>
<tr>
<td>Safety systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk &amp; work pressure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk level</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work pressure</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rewarding safe conduct</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee safety priority &amp; risk non-acceptance</td>
<td></td>
<td></td>
<td></td>
<td>*</td>
</tr>
<tr>
<td>Social environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employees well-being</td>
<td>*</td>
<td>*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee involvement</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These identified factors from safety climate literature provide the answer on the first sub-question and contribute to the understanding of the relation between employees’ behavior and the organizational (safety) climate. These factors are used in chapter 6 for the development of a conceptual model of the relation between the organizational information security climate and employees’ information security behavior. As discussed in the introduction, this can be a valuable addition to the limited amount of literature on the organizational information security climate. In the next chapter, the theories which are used to explain employees’ information security behavior are explored. Additionally, methods to measure this behavior are reviewed.
Employees’ information security behavior

A review of the literature and supporting theories on employees’ information security behavior is discussed in this paragraph. Based on what drives employee behavior in general, scholars developed several theories to explain employees information security behavior. Many differences in interpretations of concepts such as awareness can be found, together with a big variety of theories and related research models. These theories are explored, together with methods to measure the information security behavior of employees. The findings of the part of literature review will provide the answer to the second sub-question: "Which theories are used to explain employees' information security behavior?"

3.1. Methodology

Searches on Scopus, IEEE, Web of Science and Google Scholar are performed to review the literature on theories to explain the information security behavior of employees and the measurement of this behavior. The keyword used are: information security behavior, theories, measure, employee and combinations thereof. The search was limited to papers written in English. The publishing data was not an exclusion criterion. The literature achieved via these searches was roughly screened by reading abstracts to filter on relevance. In a second round, full reading was done to identify theories and possible options to measure employee information security behavior. Additionally, references from literature reviews and papers achieved via a fore and backward search were analyzed.

3.2. Security awareness and behavior

In the IS security literature many definitions of information security awareness are described. They cover three different perspectives which are cognitive, procedural and behavioral. The cognitive perspective is commonly used among researchers, with the focus on employees’ knowledge and understanding of safe information security behavior and their roles and responsibilities. In this case information security awareness refers to the state where employees are aware and conscious of the potential security related issues of the organization (Haeussinger & Kranz, 2013; Siponen, 2000a).

The second perspective is related to employee behavior, and includes the commitment of employees to behave in line with the information security policies, rules and guidelines (Haeussinger & Kranz, 2013). Parsons, McCormac, Pattinson, Butavicius, and Jerram (2014) state that both the understanding and behavior aspect should be taken into consideration.

A third perspective is added by Bulgurcu et al. (2010) by making a difference between information security policy awareness (ISPA) and general information security awareness (GISA). Employees knowledge and understanding of the IS issues and consequences are covered in GISA, were ISPA relates to the understanding and knowledge of the IS policy of the organization. Bulgurcu et al. (2010) found a positive relation between GISA and the employees’ security behavior. Also other scholars reported this positive relation, from security awareness measures to employee behavior (D’Arcy & Hovav, 2007; Dinev & Hu, 2007; Herath & Rao, 2009a). However, Lee, Lee, and Yoo (2004) did conclude that security awareness did not result in more positive behavior.

As discussed in the introduction in this paper, the definition of ISA is based on the first perspective: Employees’ cognitive ability to recognize and understand information security threats and risks in the context of their organization’s information security requirements (Bauer & Bernroider, 2017).
3.2.1. Security awareness and knowing-doing
As discussed in the introduction, employees’ knowledge and awareness, does not necessarily result in secure IS behavior. To illustrate this, take for example a driver on the highway. The driver sees a traffic sign with the maximum speed. Therefore, the driver knows what the maximum speed is. The driver looks on the speedometer and observes that he is driving slightly more than allowed. Although the driver is aware that the vehicle is going too fast, he may still decide to not alter its speed. So, knowledge and awareness do not guarantee the desired behavior.

This gap between knowledge on information security behavior and the actual IS behavior is referred to as the knowing-doing gap (Cox, 2012). A clear indicating for this gap is the study by Haeussinger and Kranz (2013). ISA had a significant relation with the compliance intention, however with a path weight of 0.3 this relation is not very strong.

3.2.2. Security awareness and employees’ attitude
In the literature several theories are used to further analyze this knowing-doing gap. The relation between ISA and employees’ attitude is often included in these studies. In the analyzed studies ISA has a significant effect, on the attitude of employees towards information security (Bulgurcu et al., 2010; Rocha Flores & Ekstedt, 2016; Safa et al., 2015). The path weights of Bulgurcu et al. (2010) and Rocha Flores and Ekstedt (2016) are quite similar (0.31 & 0.27). However, the relation is much stronger (0.64) in the research of Safa et al. (2015).

The influence of employees’ attitude on their behavioral intention is part of the theory of planned behavior (Ajzen, 1991). Therefore, this construct is often included by scholars in their studies. In almost all of the studies included in the literature review, the attitude has a significant influence, on the security intentions of employees (Bauer & Bernroider, 2015, 2017; Bulgurcu et al., 2010; Cox, 2012; Q. Hu et al., 2012; Ifinedo, 2012, 2014; Rocha Flores & Ekstedt, 2016; Safa et al., 2015; Sommestad, Karlzén, & Hallberg, 2017). Only in the studies by Herath and Rao (2009b) and Safa et al. (2016) this relation was not significant. However, in most of the papers this relation is significant. The conclusion from these studies is that only focussing on information security knowledge does not necessarily result in compliant behavior of employees and that more factors should be taken into consideration. The theory of planned behavior and the other theories commonly used to explain this knowing doing-gap are discussed in more detail in the next section.

3.3. Theories and models on employees’ information security behavior
Within the field of information security many theories are used to explain the behavior of employees. Lebek, Uffen, et al. (2014) did a literature review on information security awareness and behavior. In this review they present an overview of recent research, the main behavioral theories used and the factors influencing employees’ behavioral intention. In their study 54 different theories were identified. The main theories are the Theory of Planned behavior (TPB), the General Deterrence Theory (GDT), the Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM). All these theories are adopting different factors to explain the behavioral intention (BI) or actual behavior (AB) of employees. This is resulting in many different factors which could influence security awareness and behavior. Figure 3.1 gives an overview of the 7 most used behavioral theories.

Figure 3.1: Distribution among 7 primary theories identified by Lebek, Uffen, et al. (2014)
3.3. Theories and models on employees' information security behavior

For further understanding the main 5 theories used in the literature are briefly discussed in the upcoming sections. Figure 3.2 provides a schematic overview of these theories with their underlying constructs and relations.

![Figure 3.2: Meta-model of primary used theories partially adopted from Lebek, Uffen, et al. (2014)](image)

3.3.1. Theory of reasoned action and planned behavior

The mean idea in the theory of reasoned action (TRA) is that the behavioral intention of an individuals is shaped by their attitudes and the subjective norms (Fishbein & Ajzen, 1975, 2010). In this context, subjective norms can be described as "the perceived social pressure to perform or not to perform the behavior" (Ajzen, 1991, p. 188). Later, the TRA was extended to the theory of planned behavior (TPB) to fit situations where the behavior cannot fully be controlled by the individual. In the TPB the perceived behavioral control is added to adjust for the level in which the individual can control the behavior (Ajzen, 1985, 1991). More specifically the perceived behavioral control entails "the perceived ease or difficulty of performing the behavior and it is assumed to reflect past experience as well as anticipated impediments and obstacles" (Ajzen, 1991, p. 188).

3.3.2. Protection motivation theory

In the protection motivation theory (PMT) the behavior is based on the combination of the threat appraisal and the coping appraisal (Maddux & Rogers, 1983; Rogers, 1975). The coping appraisal is determined by the severity of the risk and its occurrence probability, which is sometimes compensated by rewards. On the other hand, the threat appraisal is determined by the self-efficacy (individual belief about its ability to perform the required behavior), the response-efficacy (individual belief about the effectiveness of its actions to properly deal with the threat) and the response cost (i.e. effort and time required).
3.3.3. General deterrence theory
The general deterrence theory (GDT), which originates from criminology, takes a different approach by focusing on the negative behavior of employees. In this theory the certainty of deterrence mechanisms and the severity of the threat are suggested to influence behavior (Williams & Hawkins, 1986). More severe and certain deterrence mechanisms are proposed to reduce unwanted behaviors. Normative validation (i.e. by observing the punishment of unwanted behavior) plays an important role in the perceived certainty of sanctions (Williams & Hawkins, 1986). In the context of information security, deterrence mechanisms can for example be sanctions like reduction of bonuses and promotions, or in extreme cases discontinuation of the employment. Besides the sanctions itself the application in practice is important, as the deterrent, will be negated when the perceived certainty thereof is observed to be low.

3.3.4. Technology acceptance model
An extension of the TRA model is the theory acceptance model (TAM) by Davis, Bagozzi, and Warshaw (1989). In this model the influence of the perceived usefulness and the perceived ease of use is added to explain the acceptance of new technology. Within information security this theory can for example be used to analyze the adoption of an email authentication service (Herath et al., 2012).

3.3.5. Knowledge, attitude and behavior model
Another model which is recently used to explain the information security behavior of employees is the knowledge, attitude and behavior (KAB) model (Khan, Alghathbar, Nabi, & Khan, 2011; Parsons, McCormac, Butavičius, Pattinson, & Jerram, 2014). The KAB-model which originates from the social psychology is extensively used in healthcare studies to analyze the link between knowledge and behavior (Baranowski et al., 2003). The model incorporates the idea that the accumulation of knowledge results in changes in the attitude of individuals. Triggered by the changes in attitude this eventually influence the behavior of individuals (Baranowski et al., 2003; Chaffee & Roser, 1986; Fabrigar et al., 2006; Fishbein & Ajzen, 1975). Therefore, this model is suitable to investigate how environmental factors (i.e. ISP provisioning and peer behavior) influence the knowledge, attitude and behavior of employees.

![Knowledge, attitude and behavior model](image)

3.3.6. Measuring behavior
Several scholars have found inconsistent results on factors that could influence employees' IS behavior (Lebek, Uffen, et al., 2014; Parsons et al., 2017; Siponen & Vance, 2014). In line with these suggestions, Cram et al. (2017) conclude in their literature review on policy compliance that the inconsistency in results requires more research to clarify the direct influence or mediating effects of variables, such as motivation and management support. Besides the differences in theories used, also the measurement of IS behavior are suggested to play a role. Thereby they suggest, like many other scholars, to measure security behavior on a more detailed level (Cram et al., 2017; Lebek, Uffen, et al., 2014; Parsons et al., 2017). In many studies generic questions are used to measure security behavior, i.e. "I intend to comply with the requirements of the ISP of my organization" (Bulgurcu et al., 2010, p. 536). The many different interpretations of those questions are suggested as possible cause of conflicting results (Parsons et al., 2017).

The advantage of such generic terms to measure IS behavior is that theoretically all aspects of the desired employee security behavior are captured by the survey questions. However, such generic questions leave ample room for different interpretations among respondents. This is especially the case when the knowledge among the respondents on the security policies is lacking. Therefore, Parsons et al. (2017) suggest to measure the security behavior on a more detailed level. Their human aspects of information security questionnaire (HAIS-Q), which is based on the KAB-model, can be used as input for more specific security behavior questions (see appendix A). This questionnaire contains questions on 7 specific focus areas: password
management, email use, internet use, social media use, mobile devices, information handling, and incident reporting. Another approach to capture more specific security behavior is the use of scenarios. After the respondents have read an information security misuse (IS) scenario, they answer the scenario specific questions. This approach was used by Vance, Siponen, and Pahnila (2012) to analyze whether the employee security intentions differ between scenarios. They, for example, found out that the intention to obey the policy to not share passwords differed from the intention to comply with not sharing their work laptop with children. Also, D’Arcy, Hovav, and Galletta (2009) used scenarios to improve the measurement of security intention. The security intention was determined by calculating the composite sum of the scenarios on individual level. Therefore, no comparison between scenarios was made.

Reading each scenario takes quite some time of the respondents. This may result in respondent fatigue. Additionally, the longer duration can decrease the number of respondents which successfully complete the survey. Therefore, using the HAIS-Q questionnaire seems to be the most suitable option for this thesis.

3.4. Conclusion

The knowledge and awareness of information security risks do not necessarily result in secure IS behavior. Many different theories are used in the IS literature to analyze this knowing-doing gap. Within the IS behavior literature scholars often used the theory of planned behavior (TPB) or the protection motivation theory (PMT) to explain IS behavior. However, the results of the studies are often conflicting. This is not only due to the differences in the theory used, but also because of the way the behavior is measured. In many studies security behavior is measured on a very generic level. Several scholars pointed out that this may affect the results as the influence of certain factors and mechanisms may depend on the type of security handling. Therefore, several scholars call for a more specific measurement. The HAIS questionnaire, based on the KAB model, seems to be the most suitable for this research. In chapter 6, the use of the KAB model is further described.

In the following chapter, a review of the literature on organizational factors and their influence on employees’ information security behavior is discussed.
Organizational climate and employee information security behavior

As discussed in section 2.1., the impact of the organizational context on the behavior of employees in general gained increasing attention over the last years. Both organizational culture and organizational climate theories are used to identify and explain how the organizational environment affects the behavior of employees. Although both research streams followed a different scientific path, the organizational antecedents which are suggested to influence employees’ behavior have many similarities (Ehrhart et al., 2014). Due to these relationships between culture and climate, their terminology is often interchanged by scholars.

The relation between organizational environment and employees’ behavior in general is demonstrated by many scholars (Baker, 1980; Ehrhart et al., 2014; Hartnell, Ou, & Kinicki, 2011; Hofstede, 2001; Q. Hu et al., 2012). However, scholars state that this relation in the context of information security still lacks thorough analysis (Connolly et al., 2017; Q. Hu et al., 2012). A first analysis of this link was made in a conceptual paper by Vroom and von Solms (2004). Their results suggest that the organizational environment can be a predictor of the IS behavior of employees.

Several scholars included one or more elements of the organizational climate in their studies on employees IS behavior. In the following paragraphs, the results of these studies and their relationships are discussed and will provide the answer of the third sub-question “Which factors and processes that influence employees’ information security behavior are described in the literature?”

4.1. Methodology
In order to gain more insight in the relation of organizational factors and the information security behavior of employees, an extensive literature review is conducted. The search terms to identify relevant literature via Scopus, Web of Science, IEEE Xplore and Google Scholar are: information security, combined with organization, management, employee, knowledge, awareness, attitude and behavior. Several variations of these key words are used to acquire a broad overview of literature. Additionally, the search is limited to papers written in English.

The non-duplicate articles are roughly screened, based on title, publisher and keywords, to check the relevance for information security in an organizational context in general. The remaining articles are further selected, based on the mentioning of employee, worker or manager and behavior in the abstract. Papers only focusing on technical measures to influence employees’ information security behavior are not considered relevant for this review. Finally, articles are fully assessed with the before mentioned criteria. Additionally, references from literature reviews and papers are derived via a fore and backward search are analyzed.

Special attention is payed on the well established, often cited, works and authors thereof. From the reviewed articles, organizational factors influencing employee behavior are identified and study results are extracted. The findings are combined in several categories and discussed in detail in the upcoming sections.

4.2. Management
The management of an organization is suggested to play an in important role in improving the information security behavior of employees. This can be the top management of an organization as well as lower levels of managers in organizations. Management can for example influence information security behavior by setting
the strategic direction, providing resources, specifying information security policies. The effect of management support, commitment, participation and transformational leadership on employees’ security behavior is analyzed by several scholars.

4.2.1. Management support
The effect of IS support by senior management is analyzed by few scholars. Managerial support is often considered as the prioritization and attention for IS in business strategy and planning (Knapp, Marshall, Rainer Jr., & Ford, 2006; Kolkowska & Dhillon, 2013). An important part of top management support is to align the security goal settings with the work values. In a case study at a social service organization in Sweden this was an important reason why awareness did not satisfactorily improved employee behavior (Kolkowska & Dhillon, 2013).

A quantitative analysis of management support among certified information system security professionals across 23 countries was performed by Knapp et al. (2006). Management support significantly influenced the level of policy enforcement and the organization’s culture. Cuganesan, Steele, and Hart (2018) investigated the effect of senior management support on IS behavior within a Australian law enforcement agency. Within this firm the management had a significant effect on attitude of employees and norms within the company. However, no significant effect was found between senior management support and the self-efficacy of employees. In contrary with the latter, Warkentin, Johnston, and Shropshire (2011) did find a significant relation between management support and the self-efficacy of healthcare professionals in US. A possible explanation, besides the different company types, is the focus on more direct management by Warkentin et al. (2011) than only the senior management.

4.2.2. Management commitment
The commitment of management to IS by actively championing security goals and adhering security policies is researched. According to D’Arcy and Greene (2014) commitment of top management to IS has, via the organizational culture, a significant influence on security compliance intentions of employees. In this research, also the organizational support had a significant role on employee IS intentions. The same positive impact of top management commitment was found by AlKalbani, Deng, and Kam (2015).

4.2.3. Management participation
Besides commitment and management support also the participation of the management in IS activities is suggested to be important. In an action based research by Puhakainen and Siponen (2010) the participation and support of top management had a considerable role in motivating employees to comply with IS policies.

The influence of perceived (top) management participation (PMP) by setting clear goals, strategy and vision among alumni of MBA and MIS programs of a public US university is analyzed by Q. Hu et al. (2012). The management participation had a significant role on the social norms within the company and the perceived behavioral control. Additionally, a significant relation between the PMP on the goal- and rules orientation of the companies was found. Surprisingly, no significant effect of PMP on employees’ attitude was found. The significant effect of PMP on perceived behavioral control and social norms was also found in a study among 200 German employees (Mayer, Gerber, McDermott, Volkamer, & Vogt, 2017).

4.2.4. Transformational leadership
A more active approach towards supporting IS security activities is via transformational leadership. Transformational leadership is considered as a way management can encourage employees to increase performance and to influence their attitude and behavior (Bass, 1985; Rafferty and Griffin 2004, Walumbwa et al. 2008).

In the research of Lebek, Uffen, et al. (2014) transformational leadership had only a significant influence on intentions of employees to participate in information security activities. No significant effect was found on employees’ security motivation, intentions to comply and perception of the information security climate.

This contrasts with the research by Rocha Flores and Ekstedt (2016). In their study a significant effect of transformation leadership on information security awareness and information security culture was found. A small difference in the measurement questions of transformational leadership and organizational climate / culture can possibly explanation these contradictory findings.
4.2.5. Key findings
The outcomes of studies on the role of management on employee security behavior are sometimes contradicting. Overall there seems to be evidence that management support and commitment can influence employees' IS behavior. The influence of management participation and transformational leadership is ambiguous.

4.3. Knowledge and awareness improvement measures
In the literature several measures are mentioned which (senior)-management can use to improve the security behaviors of employees by increasing their knowledge, skill and awareness via information systems security policy provisioning, trainings and internal communications. The effect of the employee capabilities itself are discussed in the next section. Other measures like monitoring and sanctions are discussed in 2.4.5.

4.3.1. ISP provisioning and quality
The provisioning of information systems security policies (ISP) is often mentioned as a way to improve security behavior. ISP can provide guidance for employee on proper information security behavior specifying information security goals, guidelines, rules, procedures and responsibilities (Boss, Kirsch, Angermeier, Shin- gler, & Boss, 2009; D'Arcy et al., 2009; Kirsch & Boss, 2007).

Boss et al. (2009) analyzed the effect of ISP specification on perception of mandatoriness for secure IS behavior and the effect thereof on the behavior of employees. Both the former and the latter relations are significant.

In the research of Cuganesan et al. (2018) the effect of ISP specification within a law enforcement agency had a significant effect on the norms and self-efficacy of employees. However, there was no significant effect on the attitude of employees. Safa et al. (2015) also found a significant positive relation between organizational policies and the subjective norms. Additionally, in the study by Haeussinger and Kranz (2013) the provisioning of ISP had a significant effect on the information security awareness of employees.

No significant effect was found on high versus low quality security policies and implicit versus explicit ISP (Ifinedo, 2014; Mayer et al., 2017). An important side-note is that in the research of Ifinedo (2014) implicit versus explicit ISP was only included as control variable. The perceived legitimacy on the other hand did have a significant effect on the self-reported compliance among US employees which were knew their companies ISP (0.38) (Son, 2011).

4.3.2. Training and internal communication
Another measure is the use of training programs to improve the knowledge, skills and awareness of employees. Only a weak significant relation was found between security education training and awareness programs and information security awareness in a study among employees in west-Europe (Haeussinger & Kranz, 2013). Bauer and Bernroider (2015) analyzed the effect of information security awareness (ISA) programs among German bank employees. The use of ISA-programs had a weak significant relation with the perceived vulnerability and severity of cyber security incidents.

In their research under 500 Australian employees, Parsons, McCormac, Butavicius, et al. (2014) reported that the influence of employees’ knowledge of policies and procedures on attitudes was much stronger than on the self-reported behavior. They suggest that training is more effective if the focus is not only on knowledge improvement, but also includes understanding, for example with the use of case studies. Many other authors state that training of employees is essential to deal with the information security threats, and that these trainings should be provided on a regular base (Aloul, 2012; Cone, Irvine, Thompson, & Nguyen, 2007).

In the research among American employees Herath and Rao (2009b) found a significant relation between the availability of resources, which include ISP provisioning and security training and communication) and the self-efficacy of employees. In the research of D’Arcy and Greene (2014) the use of internal communication about information security had (via the formative construct organizational security culture) a significant effect on the compliance intention. Bauer and Bernroider (2017) also analyzed the effect of internal communication. They found a significant effect on the intentions towards secure behavior.
4.3.3. Key findings
In most studies ISP provisioning, training and internal communication have a direct positive effect on IS behavior or indirect via subjective norms. No supporting evidence was reported on the relation between ISP quality and IS behavior. In (almost) all analyzed studies internal communication and training have a positive relation with awareness, self-efficacy and intended security behavior.

4.4. Employees’ capabilities and risk perception
The increased knowledge and awareness via the measures mentioned in the previous section do not necessarily result in fully secure or compliant IS behavior. As discussed in section 3.2 employees which are aware of certain risks sometimes decide to behave less secure than desired.

Several scholars have investigated this issue via the general deterrence and protection motivation theory. Via these theories the effect of employees’ capabilities, perception of the risk and impact of mitigating measures on IS behavior is analyzed. The risk perception can be influenced by organizational culture and climate, for example via knowledge improvement measures. Additionally, deterrence measures, such as monitoring and sanctioning non-secure behavior, could be used to increase the risk perception.

Besides the perception of the risk, the capabilities of the employee to deal with the risks and the impact of mitigating measures is suggested to play a role. An employee might choose for less secure behavior when the perceived risk is considered to be low in comparison with the amount of effort which is required to (partly) mitigate the risk. For example, not reporting phishing e-mails if it requires a lot of effort and time. Besides the beforementioned measures to increase employees’ capabilities, other measures to make secure behavior a more attractive option can be used. For example, compensating the increased effort via rewards.

4.4.1. Risk perception
The perception of risk or the threat appraisal of an employee depends on the perceived vulnerability and severity or impact of that risk. A high impact risk with an extremely low occurrence could be perceived by the employee as a lower risk than a less high impact event with a higher occurrence probability. The influence the perceived risks on employees’ security behavior is analyzed by several scholars, however there are differences between the perspectives which are taken into account. As discussed in the upcoming paragraphs, some scholars focused in their operationalization of risk more on the effect on the company, others are more focused on the consequences for the employee itself. Also, measures to increase the perceived risk the employee itself are discussed.

Severity of risk on company level
The literature shows very contradictory findings on the relation between the perceived severity of the risks and the intention towards compliant information security behavior. Cox (2012) did not find a significant relation. The negative significant relation determined by Ifinedo (2012) seems to be a bit counterintuitive. Other scholars also found a significant relation, however in their studies this relation is positive (Bauer & Bernroider, 2017; Vance et al., 2012). The perceived severity also effects the security breach concern level of employees, which effects the attitude of employees (Herath & Rao, 2009b). Additionally, the perceived severity of the IS risk significantly reduces the intention for non-malicious policy violations (Guo, Yuan, Archer, & Connelly, 2011).

Vulnerability to risk on company level
The effect of the perceived vulnerability to information security incidents and intention towards compliance was found to be significant by Cox (2012) and Ifinedo (2012). Additionally, Bulgurcu et al. (2010) found a significant relation between the perceived vulnerability and the perceived cost of non-compliance, which has a significant relation to the compliance intention.

However, Vance et al. (2012) and Bauer and Bernroider (2015) did not find a significant relation. This might be due to cultural differences, panels in the USA and Canada versus panels in Finland and Germany. The strength of the signification relations also differs a lot (0.90 vs 0.20). Similarly, Herath and Rao (2009b) determined that the security breach concern level was not significantly affected by the perceived probability of a security incident.

Severity of risk on personal level
The use of sanctions to increase the perceived severity of certain IS risks and to deter employees away from non-secure behavior is analyzed in multiple studies. Also, the effect of other downsides of non-secure behav-
In the research model from Bulgurcu et al. (2010), the effect of sanctions and intrinsic cost (embarrassment, stress, shame, guilt) on the perceived cost of non-compliance was studied. Sanctions and intrinsic cost both have a significant effect on the perceived cost of non-compliance. The perceived cost of non-compliance also has a significant relation on the compliance intention via the employees’ attitude. Similarly, in the study by Chen, Ramamurthy, and Wen (2012) the severity had a significant effect on the intention to comply.

In the sample of Cuganesan et al. (2018) among employees of an Australian law enforcement agency sanctions had no significant effect on the attitude, norms and self-efficacy of employees. Also, the severity of the deterrent did not seem to have a relation with the self-reported compliance with the ISP among US employees (Son, 2011). Studies on the effect of sanction severity on violation and misuse intention of IS security are conflicting. D’Arcy et al. (2009) and Cheng, Li, Li, Holm, and Zhai (2013) did report a significant relation. Guo et al. (2011) on the other hand did not find a significant relation. Siponen and Vance (2010) also did not find a significant effect of formal and informal sanctions on the intention to violate the IS security policy when taking neutralizations techniques into account (e.g. denial of responsibility into account). Even more surprising is the significant negative relation between sanction severity and compliance intention reported by Herath and Rao (2009a).

Vulnerability to risk on personal level and detecting certainty

The deterrent effect of a possible sanction depends on the certainty that non-compliant information security behavior of employees will be detected. For example, in case the chance of getting caught for the misuse of certain information systems is very low, the effect of the sanction itself will be reduced.

Herath and Rao (2009a, 2009b) found a significant, but weak (0.16, 0.26) relation between detection certainty and the compliance intention of employees. Besides the aforementioned significant relation, Chen et al. (2012) also found a significant moderating effect of detection certainty on the perceived severity of sanctions. Also, in the research by D’Arcy and Greene (2014), computer monitoring had, via the formative construct ‘security culture’, a significant effect on the security compliance intention.

The beforementioned findings slightly contradict with findings by D’Arcy et al. (2009), Cheng et al. (2013) and Son (2011). In this studies certainty detection did not have a significant relation with the employees’ IS intention. The focus on misuse intention in the former two studies rather than compliance intention could be a possible explanation for these contradicting findings.

The perceived computer monitoring also had a significant mediating effect (0.18) on the relation between intention and the actual (self-reported) behavior (Bauer & Bernroider, 2015).

Other scholars investigated the indirect effects of increased monitoring. Frequent assessment, examining and evaluation of employees’ information security behavior by management of individuals can increase the perceived mandatoriness of security measures (Boss et al., 2009). The perception of mandatoriness itself also has a significant influence on the self-reported behavior. Cuganesan et al. (2018) hypothesized that the monitoring and evaluation techniques will, via the promotion of accountability and obligatory for safe IS behavior, improve the attitude and workplace norms. Only the relation with the latter was significant. They also suggest that, via evaluation and feedback, monitoring can improve the self-efficacy of employees. This statement is supported by their statistical analysis (0.14). Additionally, a high possibility to be held accountable, i.e. via monitoring, has a significant effect on the information security compliance (AlKalbani et al., 2015).

4.4.2. Employees’ capabilities and impact of risk mitigation measures

Besides the risk perception of employees’, also the effort required and the effectiveness of information security measures on the threat are suggested to influence employees’ IS behavior. In case of a high impediment to their work efficiency which does not outweigh a very low perceived impact on the IS risk, an employee could decide to take the risk of non-secure behavior. The work impediment and perceived effectiveness of security measures itself partly depend on the capabilities of the employees. Therefore, these are discussed alongside the work impediment.Compensating measures to make the secure option more attractive, like the use of rewards, are also included.

Impact of information security measures (response cost, work impediment)

Based on the protection motivation theory, it is suggested that increased response costs (i.e. via work impediment) have a negative impact on the protection motivation of employees. Therefore, Herath and Rao (2009b)
analyzed the effect of response cost on the attitude towards the security policy. This indeed turned out to be a significant negative relation (-0.20).

According to the research by Bulgurcu et al. (2010) the work impediment caused by the information security policy has a strong significant effect on the perceived cost of compliance (0.82). These costs have a significant negative relation with the attitude of employees (-0.15). Similar findings were also reported by Vance et al. (2012). Ifinedo (2012) on the other hand did not find this relation to be significant. The effect on non-malicious IS violations is also analyzed in the study by Guo et al. (2011). The relative advantage for job performance increased the chance of non-malicious IS violations.

**Impact of rewards**
Compliance with information security policies can also have a positive side for the employee. Employers can give employees rewards (i.e. promotions, pay raises, appreciation) in return for their compliance with the company's ISP. Another upside of compliance can be intrinsic benefits, like the feeling of accomplishment, satisfaction and fulfillment (Bulgurcu et al., 2010).

In the study by Bulgurcu et al. (2010) intrinsic benefit and rewards for secure behavior both had a significant effect on the perceived benefit of compliance (0.32, 0.24). The benefit of compliance itself has a significant effect on the attitude of employees (0.15). In line with these findings, Chen et al. (2012) reported that rewards significant increase the compliance intention. The certainty of actually obtaining these rewards did not influence this relation. However, Cuganesan et al. (2018) did not find a significant relation between rewards and the attitude. Rewards also had not significant effect on the subjective norms and self-efficacy of employees. Mayer et al. (2017) took a different approach by looking at the downside of rewards. In case rewards result in performance incentives for a goal achievement other than information security (i.e. productivity), rewards can have a significant negative effect on the security compliance.

**Impact of employees’ capabilities**
Several scholars studied the effect of employees’ capabilities on their information security behavior or compliance intention. In case less effort is required to execute a task on a secure manner an employee could be more likely to do so. The same is suggested for employees’ ability to work safely. Also, the perceived impact of their behavior on the information security risk is suggested to play a role.

- **Perceived behavioral control**
As part of the theory of planned behavior, perceived behavioral control is often included in research models. PBC refers to “people's perception of the ease or difficulty of performing the behavior of interest” (Ajzen, 1991, p. 183). Cox (2012) found a significant effect of PBC on the intended and (self-reported) actual behavior of employees. Mayer et al. (2017) also found a significant relation between PBC and the employees’ intentions. However, other scholars did not find significant relations between PBC and the intended behavior (Bauer & Bernroider, 2017; Safa et al., 2015).

- **Self-efficacy**
Self-efficacy entails “how well one can execute courses of action required to deal with prospective situations” (Bandura, 1982, p. 122). In this context it means how well an employee can behave according to the information security expectation of their company.

In a research among employees from 78 different companies in the US, the self-efficacy of employees had significant relation with their attitude (0.15) and behavior (0.17) (Herath & Rao, 2009b). A similar significant effect on the intention to comply (0.22) was found by Bulgurcu et al. (2010) among US employees. Important to note is that these researches excluded all respondents from companies that did not have an ISP and respondents which did not know their company’s ISP. In other studies in the US among full-time employees, students and university staff, and healthcare professionals self-efficacy also had significant influence on compliance intention and self-reported IS security behaviors (Boss et al., 2009; Johnston & Warkentin, 2010; Son, 2011; Warkentin et al., 2011).

The same significant relation (0.17) was found among IS and non-IS mangers in Canada (Ifinedo, 2012, 2014). In a study among German bank employees, Bauer and Bernroider (2015) also found a significant relation between self-efficacy and the behavioral intention (0.22). In line with the other results Vance et al. (2012) conclude that self-efficacy has a significant relation with the intention to comply with ISPs among employees of companies in Finland. Surprisingly, in the research of Safa et al. (2015) the significant path coefficient between self-efficacy and intention is quite high (0.62). A possible explanation is that the respondents were
4.5. Social environment

IS experts and IT professionals from Malaysia. Rocha Flores and Ekstedt (2016) on the other hand found a very weak significant path coefficient of 0.09. Overall, there seems to be a well-established relation between self-efficacy and intention to comply with an ISP or with secure IS behavior. However, contradicting findings were reported by Wall, Palvia, and Lowry (2013). They did not find a significant relation among employees from several municipal governments in the US.

-Response efficacy
Response efficacy entails "the belief in the perceived benefits of the coping action by removing the threat" (Vance et al., 2012, p. 190). (Herath & Rao, 2009b) found a significant effect (0.29) of response efficacy on the attitude of employees (Herath & Rao, 2009b). In another study they found a relation between the perceived effectiveness of the security measure and the policy compliance intention (Herath & Rao, 2009a). Other scholars analyzed the direct effect of response efficacy on employees' behavioral intention. In the studies of Johnston and Warkentin (2010), Ifinedo (2012), and Bauer and Bernroider (2015), the effect on the intention towards ISP compliance behavior was significant (0.22, 0.27, 0.31). Surprisingly, in the study of Vance et al. (2012) a higher response efficacy significantly reduces the intention towards ISP compliance (-0.21). However, considered without the other factors of PMT model the direction was the opposite. Bulgurcu et al. (2010) took a slightly different approach by focussing on the relation between the safety of the resources and the perceived benefit of compliance. The safety of the resources entails "employee's perception that her information and technology resources at work are safeguarded as a result of her compliance with the requirements of the ISP" (Bulgurcu et al., 2010, p. 531). In their research among aware employees in the US this relation was indeed significant (0.32).

-Locus of control
Similarly, to response efficacy, locus of control "[...] refers to the degree to which persons expect that a reinforcement or an outcome of their behavior is contingent on their own behavior [...]" (Rotter, 1990, p. 489). In this context it is about the belief of the employee that their information security behavior actually can make a difference. In the study of Ifinedo (2014) the locus of control had a significant (0.17) effect on the compliance intention. However, in another study by Cox (2012) the locus of control did not even have a significant effect on the perceived behavioral control.

4.4.3. Key findings
Overall, the findings on the influence of the severity of IS risk and the vulnerability to IS risks on both company and personal level seem the be contradictory. The studies on the severity and certainty of sanctions show mixed results. This may partly be due to the different modelling of the relations and slightly different formulation of the questions used to measure the constructs. Additionally, individual differences in risk appetite (preparedness to accept risks) could be an explanation for these inconclusive findings. In general, the effort required to execute the required secure behavior, or more specifically the work impediment of IS measures, has a significant negative impact on the intention towards secure behavior.

In most of the analyzed studies, rewards and intrinsic benefits for information security significantly increase the intention towards compliance behavior. However, one study showed that these rewards can also have a negative impact on compliance intention, when they are set on productivity targets, rather than IS goals (Mayer et al., 2017). The relation between self-efficacy and perceived behavioral control (PBC) on the ISP compliance intention seems to be well-established in the literature. Increased self-efficacy or PBC has a positive relation with employees' security intentions. Also, the perceived effectiveness of secure IS behavior appears to be of importance. In general, this response efficacy has a positive influence on the intention towards secure behavior. However, the results of a closely related concept, locus of control, are inconclusive.

4.5. Social environment
Several elements of employees' social environment are suggested to influence the decision towards the desired information security behavior. This could be the direct organizational environment, the bond with the organization and influences from colleagues and external sources.
4.5.1. Organizational environment

It is suggested that a positive safety climate can stimulate safe behavior Neal et al. (2000). Therefore, Lebek, Guhr, and Breitner (2014) investigated the effect of the perceived organizational security climate on the motivation and intentions of employees. The organizational climate has a significant effect on the security motivation (0.39) and the security compliance intention (0.34). However, no significant effect was found on the security participation intention. It is important to note that the security climate is included as single construct based on 5 questions of Chan, Woon, and Kankanahalli (2005), which are mainly focused on the concerns and prioritization of management and supervisors. The findings of Lebek, Guhr, and Breitner (2014) on the relation between information secure climate is consistent with the research by Chan et al. (2005).

The relation of different organizational culture types on awareness programs, the information security policy, senior management support and employee related IS incidents, was studied by Donahue (2011). To measure the organizational culture, the OCAI questionnaire based on the CVF framework of Cameron and Quinn (2011) was used. Differences were noted in the culture types and their influence. For instance, the clan culture was related to more IS incidents, the hierarchy type to fewer incidents. The clan, advocated hierarchy and clan type had a positive relation with senior management support. The results were based on a survey amongst 115 information security managers in the US. This relatively small sample size forms one of the limitations of the research. Other limitations were that results among industries were not compared and the fact that the study was only performed in the US. Based on the insights from Hofstede (2001) different results can be expected in the relation of culture types with information security in other countries.

Q. Hu et al. (2012) investigated the effect of organization culture via two of the four organizational dimensions of van Muijen et al. (1999). “The rules orientation emphasizes respect for authority, rationality of procedures, and division of work. The structure is hierarchical and communication is often written and top-down” (van Muijen et al., 1999, p. 556). Q. Hu et al. (2012) hypothesized that the rules orientation can improve the social norms, perceived behavioral control, intention and attitude, by emphasizing the importance of the rules via communication and trainings. The rules orientation only has a significant relation the perceived behavioral control (0.15) and attitude (0.19). “The goal orientation emphasizes concepts such as rationality, performance indicators, accomplishment, accountability, and contingent reward” (van Muijen et al., 1999, p. 556). This orientation only has a significant relation with attitude (0.19). No significant relation was found with the social norms, perceived behavioral control and intention.

The effect of error management culture was analyzed by Mayer et al. (2017). The error management culture is hypothesized to improve the employee compliance, via early detection of errors, help with errors and quick handling of errors (van Dyck, Frese, Baer, & Sonnentag, 2005). A high error aversion culture on the other hand can decrease compliance due to reduced learning possibilities as employees are less likely to talk about errors. Only the latter hypothesis was significant.

Additionally, they investigated the effect of conflicting goals on employees’ compliance. Often a trade-off must be made between security goals and productivity goals. Therefore, the authors suggest that rewards on productivity goals can reduce employee compliance. This is also supported by their research. Mayer et al. (2017) also investigated the relation between compliance and the quality of the goal setting process. Lower quality goal setting, i.e. very unrealistic goals and low information quality, could result in a lower level of compliance. However, no significant relation was found.

In the research by Spears and Barki (2010) the alignment between the business and security risk management had, via organizational awareness, a significant impact on the performance of information security measures. In another study the alignment of goals and values between employees and company had significant effect on self-reported compliance with ISP (Son, 2011).

Recently, (Connolly et al., 2017) published their research on the influence of perceived culture values on the security behavior of employees in Ireland and the US. In this qualitative study, with 19 interviews in various companies, the influence of several organisational factors, such as people orientation, solidarity, sociability, task orientation and a flat structure on employee information secure behavior was investigated.

People orientation is defined as “concerned with people issues” (Cooke and Lafferty, 1987, p. 52), and showed to be closely related to job satisfaction. Employees will feel job satisfaction when their organization takes good care of them, for example with a good reward system, growth opportunities and good working conditions. A higher job satisfaction has a positive relation with employee motivation and compliant behavior. This finding is accordance with prior research (Cheng et al., 2013; Probst & Brubaker, 2001; Danish & Usman, 2010; Xue, Liang, & Wu, 2011). Therefore, “organizations should strive to increase employee satisfac-
tion with their jobs in order to encourage compliance with information security rules” (Connolly et al., 2017, p. 129).

Solidarity, which is defined as “the degree to which organization’s members pursue shared objectives quickly and effectively regardless of personal ties” (Connolly, 2015, p. 25) shows a narrow relation with shared information security goals. Employees are more empowered to comply with the safety requirements of their organization when they have a shared goal to protect the companies; sensitive information. Even when not enforced, employees will show complaint behavior when they understand the importance for the organization.

Sociability, which is defined as “the measure of sincere friendliness among members of a community” (Goffee & Jones, 1996, p. 134) is found to result in non compliant behavior. A high sociability creates an informal atmosphere in which authority is not taking seriously, leading to ignorance of instructions and rules.

Task orientation, defined as “concern for efficiency” (Cooke and Lafferty, 1987, p.54) can lead to non-compliant behavior, when employees strives to satisfy customers. Connolly reports that often unrealistic deadlines are pushing employees to find shortcuts and break rules. It make no sense to implement rules if they cannot be followed in practice Therefore management should “find the balance between employee workload and their obligations related to information security” (Connolly, 2015, p. 165).

The last element studied by Connolly is the influence of the flat structure, which is defined as “an organizational structure that aims to reduce “the number of layers of management hierarchy” (Kettley, 1995, p.1). Research indicates that an organisation in which management is easy accessible and approachable, the visibility for information security is improved, resulting in an increased level of information security. The dialog with employees is important to ensure policies are not hindering employees in their daily routine.

4.5.2. Influence of colleagues
Several scholars analyzed the effect of the behavior and workgroup norms of colleagues on employees. It is suggested that both the positive and negative norms and behavior of colleagues could influence the information security behavior of employees.

Work-group norms
Subjective norms can be explained as "the perceived social pressure to perform or not to perform the behavior” (Ajzen, 1991, p. 188). This social pressure of others (i.e. colleagues) is suggested to stimulate employees to improve their information security behavior. Many scholars have analyzed the effect of subjective norms on the intended information security behavior. As suggested in the theory of planned behavior, the relation between subjective norms and IS behavior is significant in most studies, however the relation is quite weak (0.14-0.37) (Bulgurcu et al., 2010; Cheng et al., 2013; Herath & Rao, 2009b; Q. Hu et al., 2012; Ifinedo, 2012, 2014; Mayer et al., 2017; Rocha Flores & Ekstedt, 2016; Safa et al., 2015).

The study of Cox (2012) is, with a strong relation (0.73), an exemption. Cuganesan et al. (2018) investigated the effect of subjective norms on the attitude and self-efficacy of employees. These relations are significant, but not strong (0.32, 0.20). In a study among employees in the US, the normative beliefs from management and direct colleagues and the peer behavior of other employees also significantly affected the policy compliance intention (0.40, 0.16) (Herath & Rao, 2009a).

Similarly, co-worker and supervisor norms are also found to significantly influence the security intentions of employees (Guo et al., 2011; Johnston & Warkentin, 2010). In the study of Guo et al. (2011) the focus was on intention towards non malicious security violations. Johnston and Warkentin (2010) on the other hand, focus on intentions towards compliance with security recommendations.

Not only norms of colleagues, but also verbal persuasion via feedback on security behavior has been studied (Warkentin et al., 2011). In their study among healthcare professionals in the US, verbal persuasion had, via increased self-efficacy, a positive influence on the behavioral intention.

Peer behavior
The behavior of colleagues is suggested to influence the behavior of other employees through socialization, communication and observation. This can be positive and negative. For example, by showing how things could be done securely. The effect of peer behavior on the information security awareness is researched by Haeussinger and Kranz (2013). Only a very weak significant relation was found (0.09). Herath and Rao (2009b) have investigated a closely related factor, the descriptive norm. However, based on the operationalisation of this construct, the focus is mostly on the belief that other employees comply to the information security policy. The descriptive norm also has a weak (0.10) significant relation.
Rocha Flores and Ekstedt (2016) analyzed the effect of information security culture (ISC) on the information security awareness, attitude and normative beliefs of employees. The construct ISC was formed based on 7 questions which are mostly about warning colleagues and collective responsibility. ISC has a significant relation with all factors. The strength of the relation with normative belief is moderate. ISA and attitude have only weak relations with ISC (0.17, 0.24).

Cheng et al. (2013) researched the influence of co-worker behavior on the intention to violate the IS security policy among Chinese employees. They found a weak (0.14), but significant relation between co-worker behavior and employee’s violation intention.

Warkentin et al. (2011) took a slightly different approach by analyzing the relation between the intention and the opportunity to learn from others (i.e. their mistakes), i.e. via vicarious experience. Vicarious experiences had, via self-efficacy, influence on the intention towards secure behavior.

4.5.3. Bond with the organization
The social control theory (SCT), also known as social bond theory, is also (partly) used to explain employee IS behavior. The SCT originates from the criminology research field (Hirschi, 2002). The social bond of an individual is determined by their commitment, attachment, involvement and personal norms. A stronger bond with the organization suggested to decrease the risk of non-compliant IS behavior.

Commitment
According to Mowday, Steers, and Porter (1979, p. 226) organizational commitment can be characterized by "(1) a strong belief in and acceptance of the organization's goals and values; (2) a willingness to exert considerable effort on behalf of the organization; and (3) a strong desire to maintain membership in the organization". As organizational commitment could be an important element to improve employees’ security behavior, several scholars investigated this relation. In an early study by Stanton, Stam, Guzman, and Caledra (2003) the effect of organizational commitment on low skill security behaviors was analyzed. Although only small effects were found, the authors suggest that organizational commitment could predict several security behaviors. A counterintuitive finding was the negative relation between organizational commitment and the compliance with acceptable use policies.

In response to the research by Stanton et al. (2003) and Herath and Rao (2009b) also included organizational commitment in their research model. In their sample among employees in the US organizational commitment had a significant relation with response efficacy (0.43) and with the compliance intention (0.20). Ifinedo (2014) did find a significant relation on the attitude of IS experts and IT professionals in Canada. However, no significant effect on their subjective norms was found.

In a recent study by Mayer et al. (2017) no significant effect on the intention was observed. The use of different statistical methods could be an explanation (hierarchical regression procedure vs MANOVA & SEM-PLS). Employee commitment to the company in general can also have a significant negative relation with the intention to violate the information security policies, as shown by Cheng et al. (2013) in their study among employees in China.

Attachment & job satisfaction
The attachment with the work and colleagues is suggested to play a role in security behavior via the fear that their negative behavior reduces the attachment with co-workers. Therefore, Ifinedo (2014) included the effect of attachment on attitude and subjective norms in his research model. In the sample collected among IS and non-IS managers in Canada, attachment only had a significant relation with the subjective norms (0.19).

Cheng et al. (2013) also included attachment in their research among employees in China. No significant relation was found between attachment and the intention to violate IS security policy (Cheng et al., 2013). Other scholars also studied the relation between attachment and malicious behavior by insiders. In their study, among employees and MBA students in Korea, no significant effect of attachment with co-workers on the computer abuse of employees via illegal software use and authorization was found (Lee et al., 2004).

Besides attachment, the job satisfaction of employees could also influence their information security behavior. D’Arcy and Greene (2014) argue that the positive feelings about their company can stimulate an employee to comply with the information security policies. They support this statement with the social exchange theory, in which people are more likely to reciprocate the people that benefit them. In their research job satisfaction indeed had a significant relation with the information security compliance intention, albeit only a weak relation (0.21).
4.5. Social environment

Involvement
Involvement of employees is this context means the engagement and participation in information security activities. The participation of users in the development of information systems significantly increases the awareness of an organization and improves the alignment between security and business (Sommestad et al., 2017; Spears & Barki, 2010). Similarly, in a research about computer abuse, based on social control theory, the involvement of employees had a significant effect (0.22) on the intentional illegal software use and malicious authorization (Lee et al., 2004). Another scholar found a significant relation with attitude (0.23), but did not find a significant relation between involvement and subjective norms (Ifinedo, 2014). The research from Safa et al. (2015) also showed that user experience combined with involvement has a significant relation with the perceived behavioral control necessary for secure IS behavior.

Contrasting is the influence of involvement in general, non-IS related, work activities. In a study among employees in China no significant relation between general involvement and the intention to violate could be identified (Cheng et al., 2013). Similarly, in the research among employees and students in Korea, generic employee involvement with the work had no significant relation with the intention towards malicious behavior (Lee et al., 2004).

4.5.4. External influences
There are also factors outside the organization which are suggested to influence the behavior of employees. As suggested by Bulgurcu et al. (2010) also external influences could play role. An example thereof is of course mass media on cyber security incidents, i.e. news items on a widespread ransomware, like “WannaCry”. Additionally, stakeholder expectations and changing regulatory requirement could increase the pressure on employees to improve their information security behavior.

In a research among home computer users mass media had, via subjective norms, a significant influence on their intention towards secure information security behavior (Ng & Rahim, 2005). Based on this finding, Haeussinger and Kranz (2013) analyzed the influence of secondary sources (internet, TV, newspapers and radio) on the ISA of employees. Although significant, the relation is quite weak (0.12). Bauer and Bernroder (2017) the relation between the use of external channels on the ISA of employees. In addition to the sources mentioned by Haeussinger and Kranz (2013), they also included self-organized learning and informal talks with friends and family in their construct. They also found a significant effect on employees’ ISA.

Another external influence, social pressure, was studied by AlKalbani et al. (2015). In their study they looked at the moderating influence of social pressure. The social pressure did not have a moderating effect on the relation between IS compliance and the management commitment. The same result was found for the ISA of employees. However, the social pressure did have a significant moderating effect on the relation between the IS compliance and the perceived accountability.

4.5.5. Key findings
Several elements of the organizational climate are analyzed. It is important to note that some scholars include climate or culture as one variable in their research. Other scholars focus more on specific parts of the organizational climate. The organizational climate has a significant relation with the compliance intention in two studies in which the climate was considered as a single variable. The scarce amount of research on the effect of rule- and goals is inconclusive.

In the literature colleagues can influence the behavior of an employee. The significant influence of subjective norms of colleagues is well-established in the literature. There is also evidence supporting the influence of peer behavior, however most of the few studies show a very weak relation. Additionally, the operationalisation and proposed relations differ too much to be conclusive.

The commitment of employees to the organization is suggested to influence their behavior. Both significant and non-significant findings were reported. In one study even a significant negative relation was reported. Therefore, the findings are to contradicting to make a conclusion. In the three studies which included attachment, no significant effect on the intention and attitude was reported. Only in 1 study attachment had a significant relation with the subjective norms. In general employee involvement in IS activities has a positive influence on their intentions. Involvement with the company in general shows no significant effect. This might be due to increased alignment of security and business based on the involvement of employees. Another explanation could be the geographical differences. The studies which include general involvement focus on Asian employees.
4.6. Other factors

Scholars sometimes include personal and business demographic information as control variable in their research model. Most of the variables turn out to be insignificant on the intention towards secure behavior.

4.6.1. Age & gender

The age of employees has no significant effect in most studies (Bauer & Bernroider, 2017; Herath & Rao, 2009a, 2009b; Ifinedo, 2014; Rocha Flores & Ekstedt, 2016; Siponen & Vance, 2010; Son, 2011). Only in the study by Haeussinger and Kranz (2013) a significant relation was found. The gender however, has a significant effect in 4 of the 8 studies (Bauer & Bernroider, 2017; Herath & Rao, 2009a, 2009b; Ifinedo, 2014; Siponen & Vance, 2010; Son, 2011; Vance et al., 2012).

4.6.2. Personality

A little amount of research is done on the influence of personality traits on the behavioral intention of employees. However, there are indications that personality can play a moderating role in the behavioral intention. Johnston, Warkentin, McBride, and Carter (2016) for example found a significant moderating influence of some of the meta-traits on the relation between situational factors and intentions to violate the ISP.

4.6.3. Education, knowledge and experience

The general education level (i.e. high school, university) and work experience does have a significant relation with the reported security behavior intention (Bulgurcu et al., 2010; Herath & Rao, 2009b; Q. Hu et al., 2012; Ifinedo, 2014). However, the findings of other scholars suggest the opposite (Herath & Rao, 2009a; Siponen & Vance, 2010; Son, 2011). Surprisingly, also general IT knowledge did have no effect (Bulgurcu et al., 2010; Herath & Rao, 2009b). Negative experiences with information security, i.e. ransomware on an employee’s pc, is suggested to affect the information security awareness of employees. This relation was investigated by Haeussinger and Kranz (2013) which found a significant relation with a very low path coefficient (0.07).

4.6.4. Job

In the studies by Ifinedo (2014) no significant effect was found of job tenure, occupation and work rank. Similarly, Son (2011) did not find a significant influence of job tenure. Q. Hu et al. (2012) also found no significant relation with job type and dutifulness. Haeussinger and Kranz (2017) did find a significant differences for employees with an IT function and work rank. However, in the studies by other scholars Herath and Rao (2009a) this relation was not significant (Herath & Rao, 2009a; Vance et al., 2012).

4.6.5. Company characteristics

On company characteristics the findings are contradicting, this might be related to the difference in national culture. Another explanation could be the measurement of employee behavior by explicitly asking for the compliance the companies ISP. ISPs are likely to differ between companies and industries, which could influence the results. In a study among German companies by Haeussinger and Kranz (2013) a significant effect of industry and company size on the reported intention to comply was found. Herath and Rao (2009a) on the other hand did not find a significant relation between company size and the behavioral intention. Bulgurcu et al. (2010) did not find a significant relation between ISP compliance and the industry. Additionally, in their study the information-intensity of the company had no significant influence on ISP compliance intention.

4.6.6. Key findings

The findings on demographical variables are very contradicting. For many variables, studies show evidence for both significance and non-significance influence. An exemption is the non-significant influence of age on employees’ behavioral intention, which is confirmed in most studies.

4.7. Conclusion

The extensive review of organizational factors and their relation with employees’ information security behavior results in many different elements and quite some variety of study designs and theories used. This results in a broad insight, although results of studies are not always comparable. Due to different interpretations of behavior, results may also fluctuate. The majority of the studies is quite generic, for example with questions such as "I intend to comply with the requirements of the ISP of my organization (Bulgurcu et al., 2010, p. 536)."
This makes it harder to compare IS behavior among companies. Additionally, it requires thorough knowledge of the ISP by the respondent. In theory, an expert with thorough knowledge of the ISP may report a lower compliance for the same behavior as an employee which has little knowledge on the handlings required for compliance.

Taken this limitation into account, some general conclusions can be made. More nuanced and detailed information is provided in the sub-chapters and their related key findings.

Management plays an important role, although their influence is not always positive. This is in contrary to training and communication, which generally shows a positive effect on the behavior of employees. Mixed results are reported for the influence of risk severity and vulnerability. Work impediment, has significant negative impact, whilst rewards increase the intention towards compliant behavior in most studies. Self-efficacy and perceived behavioral controls have a well-established positive relation.

The scarce amount of research on rule or goal orientation is inconclusive. Also, no conclusion can be made for peer behavior, due to differences in operationalization and proposed relations. The involvement of employees on information security activities has a positive effect on their intentional behavior, Finally, findings for demographic variables are very contradicting, with an exemption for the age of employees. These general conclusions are visualized in table 4.1. For a quick insight, the factors with a significant positive relation on employee information security knowledge, attitude or behavior are colored green. In case this relation is unclear, as results are contradictory, the factors are colored grey. The factors with a significant negative relation received a blue color.

Table 4.1: Overview of identified factors and their influence on knowledge, attitude and behavior

<table>
<thead>
<tr>
<th>Category</th>
<th>Knowledge</th>
<th>Attitude</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>support</td>
<td>commitment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>participation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge and awareness</td>
<td>transformational leadership</td>
<td></td>
<td></td>
</tr>
<tr>
<td>improvement measures</td>
<td>ISP provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>training</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>internal communication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>severity of risk on company</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vulnerability to risks on company</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>severity of risk on personal level (sanctions)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>vulnerability to risks on employee level (monitoring)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>impact of IS measures (work impediment)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee capabilities and</td>
<td>impact of rewards</td>
<td></td>
<td></td>
</tr>
<tr>
<td>risk perception</td>
<td>impact of employee capabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>perceived behavioral control</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>self-efficacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>response efficacy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>organizational environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>rule orientation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>goal orientation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>subjective norms</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>peer behavior</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social environment</td>
<td>commitment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>attachment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>employee involvement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legend</td>
<td>positive relation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mixed results</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>negative relation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The findings of this extensive review of the literature, as described in this chapter and the previous two chapters are combined to acquire a picture of the current research on what influences the behavior of employees in an organizational context. These outcomes are used in the next chapter, in which the findings from literature are compared with the experiences in practice.
Semi-structured expert interviews are conducted to determine whether the insights identified in the literature review are also observed in practice. Additionally, the findings from the desk research can be enriched with missing factors or mechanisms from practice. The output of the interview will provide the answer on the third research question: “Which of the identified (and additional) factors and processes are observed in practice by experts?”

5.1. Interview approach
The experts for the interviews were recruited via the network of Deloitte. In total 8 security consultants and company experts were interviewed to get a broad picture based on an inside and outside view.

Table 5.1: Overview interviewed experts

<table>
<thead>
<tr>
<th>Expert</th>
<th>Position</th>
<th>Company focus</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CISO</td>
<td>International</td>
<td>Financial</td>
</tr>
<tr>
<td>2</td>
<td>GISO</td>
<td>National</td>
<td>Insurance</td>
</tr>
<tr>
<td>3</td>
<td>Senior awareness officer</td>
<td>International</td>
<td>Commercial</td>
</tr>
<tr>
<td>4</td>
<td>CISO</td>
<td>International</td>
<td>Consultancy</td>
</tr>
<tr>
<td>5</td>
<td>CISO</td>
<td>National</td>
<td>Public</td>
</tr>
<tr>
<td>6</td>
<td>Senior awareness officer</td>
<td>International</td>
<td>Consultancy</td>
</tr>
<tr>
<td>7</td>
<td>IS consultant</td>
<td>International</td>
<td>Consultancy</td>
</tr>
<tr>
<td>8</td>
<td>IS consultant</td>
<td>International</td>
<td>Consultancy</td>
</tr>
</tbody>
</table>

After a short introduction, the interviews started with general questions to capture the context in which the organization operates and to determine the experts experience with (near) information security incidents in their organization. Thereafter, more guided questions related to influences identified in the literature were discussed. The guidance document as used for the interviews is attached in appendix B.

The face to face interviews took on average 50 minutes. After written consent, the interviews were, with 1 exemption, recorded and fully transcribed. One expert preferred not to record the interview. In this case notes were taken during the interview and processed in more detail afterwards. All experts were very open and supportive to answer the questions and provided a good insight in the information security practices, issues and vulnerabilities of their organization.

5.2. Coding process
The transcribed data from the interviews are processed using provisional coding. This coding method is appropriate, as a provisional start list of codes could be generated from the review of the literature (Saldaña, 2015). This type of coding needs to be performed with some caution, as the preconceptions of what to expect can distort the interpretation of what’s really said. During the coding process, the provisional codes were revised, and new codes were added to capture the input from the interviews.

The qualitative data analysis software tool MAXQDA\textsuperscript{1} is used to assign codes to citations and to bundle the

\textsuperscript{1}A software package for qualitative research, see maxqda.com
classified information from all interviews. During the coding process all interview data was handled anony-
mously to reduce the chance of social desirability bias. Based on the coding, an overview of the results is
made. Next to that, a detailed interpretation of the interviews is performed to provide a more in-depth view,
as suggested by Schmidt (2004). Also, some individual quotes are selected for clarification and to ground the
choice for new coding categories.

Figure 5.1: Wordcloud of codings used for the expert interviews

5.3. Results
In this chapter the results of the expert interviews are discussed. The input of experts is combined per coded
category of influencing factors. For some categories, all experts provided input. In other cases, not all ele-
ments were touched during the interview. This due to the position and amount of insight of the expert on the
specific elements of information security covered by the questions. Figure 5.2 shows an overview of the final
coding and the factors on which an opinion was given by the experts.

Figure 5.2: Overview of codings of expert interviews in MAXQDA
5.3. Results

5.3.1. Management

Management support / resources

The support of management is unanimously mentioned as important by the experts. Support can have different meanings, therefore in the interviews support was expressed as resources. The allocation of resources for information security related measures is mentioned by experts #7 and 8 to be quite problematic during the development of public IT projects. This due to lack of targets on information security, expertise or clarity in responsibilities. Five experts expressed to have enough resources, although not unlimited.

Resources can also be used indirectly. One of the experts (#4) explained that the management appointed a stress coach to support employees in handling the work pressure, which can lead to reduction of failures.

Management commitment

Likewise, the commitment from (top) management is experienced as critical, in expressing the priority of security for the business. That can be indirectly via a statement which is cascaded down through all management layers. Alternatively, a direct message from the top management can have a strong influence, especially when it is brought by the CEO instead of the CISO. This experience is shared among most experts.

In the negative situation, when commitment of the management lacks, or is not visible, this will negatively influence the information security behavior of employees. Expert #7 states: “hospitals now have an information security officer, but without support from the board, he will be bypassed from all sides and have a very difficult job”.

Management behavior

Management behavior, in line with their commitment, is crucial. To emphasize the importance of compliant information security behavior for the organization, management should lead by example. This holds true for all disciplines and layers of management. This viewpoint is shared by all experts. Experts 5, 7 and 8 expressed their worry about lack of knowledge and ownership of top management in the public sector environment.

Security as part of business

During nearly all interviews, the experts stressed the importance to embed information security in all business activities. When reviewing the information security literature, this point was barely touched explicitly by scholars. However, ensuring that that the security of information is an integral part of all business decisions and projects, is not so easy in practice.

Within the organizations from which experts are interviewed, big differences were seen in the trade-off between business and security. Expert #4 says “most important is to take decisions together, not only from a business or security perspective. The choice can be good or bad, but it’s at least a common and deliberate decision”.

5.3.2. Knowledge and awareness improvement measures

The companies in which our experts are employed, all provide information security training programs to improve the knowledge and awareness on IS in the company. In this section insight is given in their practical experience with these programs and the relation to the behavior of employees.

ISP provisioning

Informing employees about the company’s policy on information security, by explaining the rules and standards, is often the first element of the training program. Only providing a policy, sometimes with the request to sign, does not automatically ensures awareness and secure behavior. Experts see the provisioning of the policy only as the first step in the training program.

Base training

A base training for all employees is available in the companies of the interviewed experts. This training, often in the format of an e-learning, is not always mandatory. Without further in-dept or tailored training, the effectiveness of such a base training is questioned by experts #1, 2, 3 and 4. However, all experts agree on the need for IS training in general. This is seen as very important to increase the knowledge of the employees. Expert #3 states that it’s crucial to make the training mandatory, to stress the importance the company gives to information security.
5.3. Results

Tailored or thematic training
Besides the base training, many different approaches to enhance the knowledge and awareness of employees were discussed during the interviews. All experts emphasized the importance to align the training elements with the daily practice of the company and to focus on some of the vulnerabilities of the company. Often the choice is made to focus on phishing campaigns and physical access control of the building.

Also training on risk evaluation is mentioned to be important. The focus should be on triggering employees to think about their actions and the implications of non-secure behavior. As mentioned by expert #7 “making the 10 golden rules of security is not enough, in most cases employees have to think instead of simply following the rules. Therefore, you need knowledge and awareness of the vulnerabilities”. A specific way to engage employees, is the gamification of the information security training. As experienced by experts #1, 2, 3 and 4 the competitive element triggers employees and makes this training format very successful.

Frequency
Another repeatedly mentioned point of attention is the frequency of training. Nearly all experts stress that rolling out a large e-learning on a yearly or two-yearly base is not the way to go. The effect of such a training fades away within 1 to 2 months. Regular training, for example on a monthly base, with small chunks of information or actual topics proves to be more effective and does take only a limited amount of time of the employee. Expert #5: “it is a continuous process that never ends”.

Communication
All experts express that communication about information security risk and incidents is important. How this brought into practice varies quite a lot between companies, depending the business focus and company culture. Expert #5 explains that in his company it’s not accepted to give openness about incidents or near-incidents, as people feel this as ‘naming and shaming’, even when no names are mentioned.

This in contrary to another company, where incidents are discussed in walk-in sessions. Expert #4 encounters transparency about incidents and the way these were solved as a means to push awareness. Similarly, experts #2, 3, 6 and 7 also suggest that openness on incidents or near misses is the most effective way to increase the awareness. In some cases, the management only allows communication on a specific page on the intranet, or limits communication to maximum 2 times per year, in order not to disturb the business focus. As stated by expert #3: “it’s about finding the balance between doing the right things and offering information without creating an information overload”.

5.3.3. Employee capabilities and risk perception
Risk perception
In the opinion of experts (#1, 4, 6), employees’ perception of the information security risks is not always realistic, and mostly the risk is judged much too low. This can result in non-compliance. For example, employees which refuse to wear a badge, as they are already working a long time for the company, so everybody should know them. Or leaving the laptop in the car, out of convenience, as it’s not their own property.

Training and communication can contribute to a correct risk perception and compliant behavior. Expert #4 warn that over-estimation of employees’ own capabilities can also cause non-compliant behavior, due to a wrong risk judgment. Several experts express that the best way to create awareness about risks, is a real incident. Another option is to hire an actor, as done by expert #4. Showing with selfies how easy this actor could enter the building and several departments, contributed to a realistic perception of this risk.

Work impediment & user-friendliness
One of the most important triggers of (non)compliant behavior of employees mentioned by experts, is the user-friendliness or ease of use of security measures. The more difficult it is to implement certain measures in the daily practice, the quicker employees will search for alternative solutions. Expert #1 emphasizes hat technology should facilitate as much as possible. More handling steps, for instance the effort required to encrypt confidential information, can lead to more non-compliance.

Additionally, expert #3 explains: “behavior is influenced by both motivation and ability. Awareness campaigns can positively influence the awareness, but what we forget is the ability, how easy is it to implement security measures. This is often overlooked by IT. And in some cases, you must be very motivated to go through all the additional hassle that’s required to be compliant”. These opinions are confirmed by expert #4, stating that security is always seen as a business blocker, as regularly additional handling is required. Therefore, it is important to find a balance between information security and user-friendliness and to find solutions that
are accepted in practice. The facilitation of accepted and good working security measures leads to the best results.

**Monitoring**

All companies included in this study perform some kind of monitoring. This varies from monitoring of outgoing mails on personally identifiable information and the completion of e-learnings, to completing internal audits. The results of phishing campaigns are often monitored. All experts are uniform in their opinion that monitoring is very important, but can also frighten employees. Therefore, feedback should be given either very carefully, or only on department level. Monitoring should be used to find black spots in the measures, sharpen campaigns and improve awareness. Not to punish people. As stated by one of the experts "if security is used to denigrate employees, then I can better quit my job".

**Rewards and sanctions**

In line with their opinion about monitoring, experts are very reluctant to use sanctions to push information security compliance. Without exemption they do not believe that punishing employees for non-secure behavior will have a positive effect. Expert 3: "sanctions are not the way to go". This in contrary to quite some literature, as discussed in section 4.4.2. Only in very extreme situations, for example with fraud, a sanction is judged as acceptable. To the experts’ view, sanctions create fear which will lead to less openness and reporting of incidents. In only one company, the expert has a budget to reward good information security initiatives with an incentive. To his view this contributes to a pleasant and open work climate, in which people feel free to address things that need improvement.

5.3.4. Organizational characteristics

**Sector & department**

The matureness of information security can differ quite a lot between organization, but also between different departments within one organization. As stated by expert #2, banking organization are used to deal with sensitive information and therefore very aware of the risks of non-secure behavior. This in contrary to service organizations or hospitals, were both awareness and secure behavior are in general much lower. Expert #1 explains that also within the organization, differences are experienced. Some departments, for example sales and marketing, are less strict in following information security measures. This in comparison with their colleagues from the finance and IT departments. Also, experts #2, 3 and 4 confirmed these differences within the organization.

**Information sensitivity**

Some experts (#1, 2, 3 and 4) indicate a clear relationship between the sensitivity of information and the information security behavior of employees. These employees are aware of the confidentiality of the information, and often receive additional training. As mentioned by expert #4: “people working with sensitive information are sharper, more aware, more paranoia”. This in contrary to experience of experts #5, 7 and 8, stating that even when employees are aware that they are dealing with sensitive information, their behavior is sometimes not influenced by this knowledge. This could be due to their service-oriented focus.

5.3.5. Organizational & social environment

**Hierarchy/formal-informal**

The influence of hierarchy in the organization is seen as both positive and negative. In a more formal or hierarchic organization, such as a bank, rules are followed. However, in a rule-oriented organization, the intrinsic motivation of employees is experienced as lower than in an informal organization. In a less formal organization, people will easier remind each other on non-secure behavior. By talking about information security, and inviting employees to challenge the measures, a buy-in can be created.

However, a negative side of an informal business culture can be the leakage of confidential information via informal chats with colleagues. Another mentioned downside of an informal organization is that users have and take more freedom, for example with the installation of software. This can result in additional IS risks.

**User involvement**

Nearly all experts express that the involvement of employees in information security measures is crucial to stimulate compliant behavior. By involving people in projects and the development of security measures,
visibility, knowledge, acceptance and shared responsibility can be created. Information security should not block the activities of the business. Together with the employees, acceptable solutions must be found. Expert #5 states: “result = quality x acceptance”, so you need the acceptance, otherwise it makes no sense. A high acceptance rate with poor quality secure measures on the other hand also will not in lead to the desirable results. It is about finding the right balance between the quality of the information security measures and the acceptance of the employees, which requires involvement of employees. In line with this statement, expert #4 argues that: “we trust and need our employees, they have an important role, information security is not possible without them”.

However, experts emphasize that it’s not always feasible or easy to involve employees, due to resources and business priorities. Expert #2 states that at least some people, other than IT, should be involved in the development of new information security measures.

**Interaction with colleagues**

Social monitoring, reminding colleagues that they perform non-secure behavior, is experienced as quite difficult. Depending on the culture of the organization, this might be possible, or is seen as really ‘not done’. Although most experts point that an open interaction with colleagues would be very supportive to improve secure behavior, employees can experience this as threatening.

In practice, interaction with colleagues is not experienced to improve secure behavior. In contrary, people are hesitant to address non-secure behavior to their colleagues, as this could been seen as distrusting them. Experts #2 and 4 also stated that giving feedback on colleagues about their behavior, is much easier in smaller organization. In a bigger company, people are less familiar with each other, which makes is more difficult to address topics.

**Peer behavior**

The influence of the information security behavior of colleagues is seen as very high. If some security rules are neglected collectively, the impact can be enormous. One of the experts remarks that the impact depends on the position of the peer. For example, non-secure behavior of the manager or a member of the executive board would be ‘killing’.

**Rule/goal orientation**

The focus of employees on achieving their goals is mentioned as an important trigger of non-secure behavior. Helping the customer, client or the patient is one of the core values and therefore main focus in some organizations. This focus can lead to violation of the security rules, albeit often unconscious. An example is the access to medical records, which should be very restricted due to its sensitive nature. However, in practice, many carers have access, or do share passwords, in order to help the patient as good as possible. Another example mentioned by expert #7 is the work pressure in delivering a project on time, leading to a delay in the implementation of security measures in the project. The (other) business goals prevails over security.

Rule orientation is more experienced in legal or financial oriented organizations, as rules or legislation are part of their heritage and common practice. Some countries or cultures are also seen as more rule or hierarchy oriented. In general, implementing security measures in a rule-oriented organization is experienced to be easier. However, experts #3, 4 and 5 warn that simply following the procedures does not directly guarantee secure behavior.

**5.3.6. Cause of incidents**

One of the questions of the interview was what the expert experienced as the main cause of information security incidents in their organization. Without exemption, all experts refer to the human behavior as cause of IS incidents. Expert #3: “it is a combination of multiple factors, but it’s often the human component which is not covered by technology”. The reasons for non-secure employee behavior given by experts are various. Sloppiness is often mentioned. The fact that employees are distracted from their work and forget or overlook to be critical in clicking on a mail, is also seen as an important reason. This distraction can be due to private circumstances, work pressure or stress. The experts’ opinion is that in general unconscious behavior leads to incidents. In more service oriented organizations or departments, the customer or patient oriented focus of employees is, without exemption, named as main course of incidents. Expert #7 remarks “you can enter everywhere, computers are not locked, passwords are stuck to the screen, that’s reality”.


5.4. Conclusion
The interviews with the 8 information security experts provided valuable information and insights from practice. Although most of the findings from literature are confirmed, also some factors are identified in which literature is not linked with the experiences from the experts. Additionally, nuance is added to literature review findings and important complementary insights, some of them scarcely touched in literature, are noted. The factors and processes that influence employees' IS behavior as identified via the interviews with experts in practice forms an essential contribution to the choices made for the construction of a conceptual model. This model is used to statistically analyze the relations and underlying hypotheses of organizational factors and employee information security behavior and will be fully described in next chapter.

In line with the findings from literature:

- The positive effect of employee user involvement in information security measures
- The impact of peer behavior
- A confirmation of the positive effect of knowledge improving activities and communication.
- The negative effect of work impediment on information security behavior is confirmed. Finding balance is important, next to the acceptance and ability to implement security measures
- Monitoring is important. Feedback of monitoring results can cause fear in the organization. The goal should never be to blame employees, but to learn from monitoring results and adopt information security measures where needed.
- The positive effect of rewards, although only 1 company used rewards for information security behavior
- Communication and openness about information security issues is important to increase knowledge, attitude and compliant behavior.

Conflicting with literature:

- Goal-orientation is found inconclusive in literature. In practice this is often observed as cause of non-compliance
- Contradicting results for management support, commitment and behavior in literature, in practice these management attributes are experienced as crucial
- Interaction with colleagues shows positive results in literature. In practice social monitoring is not accepted.
- The studies with sanctions were inconclusive. Experts report that sanctions are not used in practice, as it is perceived that they create fear and leave less openness and not reporting incidents

Additional insights from experts:

- Security should be embedded in all business activities
- Security training and awareness programs varies from a one-time formality to an integrated and continuous part of business. The latter is experienced to be effective, especially when practical and actual topics are touched
- Employees are not just a big risk. They are also the human sensors and line of defense of the organization
- Information security should be a shared responsibility, not only an IT thing
5.5. Relation between literature and practice

Based on the findings from the expert interviews, as summarized in the previous section, a set of factors and processes that influences employees’ information security behavior in practice is extracted. The relations between those factors and the factors identified from literature is presented in table 5.2.

Table 5.2: Overview of influential factors and processes identified in practice

<table>
<thead>
<tr>
<th>Factor</th>
<th>Experienced relation</th>
<th>Relation with literature review</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Top)management commitment</td>
<td>High commitment of top management positively influence the attitude and behavior of employees</td>
<td>Mixed effect in literature. Stated as crucial for implementation of information security measures by experts</td>
</tr>
<tr>
<td>Management priority</td>
<td>Priority of management of IS as part of business is very important and influences employees’ attitude to secure IS behavior.</td>
<td>Inconclusive effect of goal orientation of mngt in literature, in practice observed as very influencial</td>
</tr>
<tr>
<td>ISP provisioning &amp;</td>
<td>Regular provisioning of ISP and security education improves knowledge, attitude and behavior</td>
<td>Confirmation of effect of frequent and practical education on knowledge, but mixed results on behavior in literature.</td>
</tr>
<tr>
<td>Openness on information security</td>
<td>Being open about the IS risk and incidents helps to increase knowledge and attitude towards IS requirements</td>
<td>Positive effect in literature. Also in practice, but restrictions to implement in some organizations</td>
</tr>
<tr>
<td>Employee involvement</td>
<td>High involvement of employees will increase their knowledge, understanding and acceptance of IS measures</td>
<td>Both literature and practice shows positive effect</td>
</tr>
<tr>
<td>Work impediment &amp; work pressure</td>
<td>High work impediment and work pressure are expected to decrease the attitude of employees</td>
<td>Both literature and practice shows negative effect</td>
</tr>
<tr>
<td>Subjective norms</td>
<td>Norms are influencing IS behavior, can be both positive as negative.</td>
<td>Importance and influence stressed in both literature and practice</td>
</tr>
<tr>
<td>Peer behavior</td>
<td>Behavior of peers, i.e. colleagues influences the attitude and behavior of employees, both positive and negative.</td>
<td>Influence of peers stressed in literature. Also in practice, influence depending on type of organization</td>
</tr>
</tbody>
</table>

The factors and processes that influence employees’ IS behavior as identified via the interviews with experts in practice forms an essential contribution to the choices made for the construction of a conceptual model. This model is used to statistically analyze the relations and underlying hypotheses of organizational factors and employee information security behavior and will be thoroughly described in next chapter.
Research model

The insights derived from the reviewed literature, combined with the practical insights from information security experts form the basis of the conceptual research model. This conceptual model and its underlying hypotheses are used as input for the statistical analysis (see chapter 7). This analysis is used to determine the relation, effect and magnitude of the identified factors and processes on the information security behavior of employees, answering the fifth underlying research question.

6.1. Level of detail
A challenge for the development of the conceptual model is to capture enough detail to explain the employees’ IS behavior while keeping the model as parsimonious (simple) as possible. Besides the prevention of overfitting, it is also required to limit the required sample size. The sample size increases when more variables and relations are added to model. As discussed in more detail in 5.2, surveys are used to collect the data required for the statistical analysis of the model. Another limitation is the number of questions which can be asked to the respondents before respondent fatigue sets in.

6.2. Types of behavior (dependent variables)
As discussed in section 3.3, information security behavior is often measured on a very generic level. Behavior is usually included as self-reported compliance with the ISP in general. However, no detail on specific behaviors, i.e. internet-use or password management, is measured. Scholars suggested that the strength and significance of relations between organizational factors and behavior is likely to vary among different security handlings (Cram et al., 2017; Lebek, Uffen, et al., 2014; Parsons et al., 2017; Parsons, McCormac, Butavicius, et al., 2014). For example, the relation between openness within an organization on incident reporting behavior versus secure internet behavior. A positive relationship between the knowledge, attitude and self-reported behavior of employees on the IS policies and requirements was proven by Parsons, McCormac, Butavicius, et al. (2014). The results also indicate that attitude is mediating the strong influencing effect of knowledge on behavior.

6.3. Theoretical basis
Many theories have been used to analyze employee information security behavior (see chapter 3). The knowledge-attitude-behavior model with the relations as suggested by Chaffee and Roser (1986) is used as theoretical basis. This model seems to be the best fit with this research, due to its parsimonious characteristics.

Additionally, this theory is used as basis for the human aspects of information security questionnaire (HAIS-Q) (Parsons et al., 2017). This questionnaire, which is validated in multiple studies with in total 1681 participants, allows for the measurement of behavior via detailed statements on different information security handlings (McCormac, Calic, et al., 2017; McCormac, Zwaans, et al., 2017; Parsons et al., 2017; Parsons, McCormac, Butavicius, et al., 2014; Pattinson, Butavicius, Parsons, McCormac, & Calic, 2017). The combination of the detailed measurement of IS behavior and the limited amount of predictors in the underlying model, makes the HAIS-Q a suitable instrument for this research.
6.4. Organizational climate (independent variables)

The total set of factors to be measured should reflect the main elements of organizational climate. As discussed in chapter 2, 3 and 4, many factors which can influence employee IS behavior are mentioned in the literature and expert interviews. However, due to restrictions in resources and the reasons mentioned in 6.1 only a selected number of variables can be included in further analysis. The findings from the qualitative analyses (i.e. the expert interviews and literature reviews) is used to select these factors based on the expected importance and influence on employees’ IS behavior. Additionally, factors which require more research because of limited or contradicting findings are included.

In this section, grounding for the chosen factors is provided, including the expected influence on the behavior of employees. In section 6.4.2. the exclusion of organizational factors is discussed. In table 6.1 an overview of the included variables is presented. A more elaborate discussion on the selection is included in appendix C.

6.4.1. Variables included in the model

Information security education and communication

Both findings from literature and input form experts suggest the importance of adequate security education of employees. By provisioning the information security policy of the organization and educate employees why these rules should be followed, and what their responsibilities are to protect the companies’ vital information, the knowledge of the employees can be increased. Regular communication about information security rules, including the potential consequences of a security breach, is also expected to contribute to a higher level of knowledge. This can lead to an higher awareness and attitude, which in turn, will encourage compliant information security behavior (Bulgurcu et al., 2010; Connolly et al., 2017; Q. Hu et al., 2012).

To reduce the number of constructs, the closely related elements training, communication and ISP provisioning are combined in this construct, with a focus on the transfer of knowledge.

Openness on information security

Openness in the organization on information security risks and (near) incidents is expected to increase the knowledge and improve the attitude and behavior of employees. As suggested by the experts, being open on IS risks and incidents, can increase the awareness and understanding of IS. However, it is difficult to gain support for openness on IS in some companies. In industrial settings this openness on safety risks and incidents is more widely accepted (Kines et al., 2011; Neal et al., 2000).

Employee involvement

The engagement and participation of employees in information security activities is expected to increase their knowledge and awareness. Additionally, involvement also can improve understanding for information security measures and the alignment between security and business (Sommestad et al., 2017; Spears & Barki, 2010).

A positive relation with attitude and behavior is also mentioned in both safety climate research (Cooper, 2016; Neal et al., 2000) and information security research (Safa et al., 2015). Experts expressed the importance of employee involvement to improve their knowledge and acceptance of IS measures. Involvement might also lead to an improvement of these IS measures.

Work impediment

The extent to which IS requirements form an impediment to the work of the employee is reported by some scholars to decrease the intention towards secure IS behavior of employees (Bulgurcu et al., 2010; Herath & Rao, 2009a; Vance et al., 2012). Experts named the impediment of IS measures on the daily work as one of the main reasons for non-compliant behavior.

Perceived management commitment

Higher management commitment entails that the management champions IS and adheres to the IS requirements. A higher commitment is expected to positively influence employees’ attitude towards IS behavior (AlKalbani et al., 2015; D’Arcy & Greene, 2014). Also safety climate research confirms the important role of management in the employees’ behavior (Kines et al., 2011; Neal et al., 2000).

Experts emphasize that perceived (top) management commitment has a high influence on the IS behavior of employees. This influence can be both positive as negative. When this commitment lacks, this will directly negatively influence the IS behavior of employees.
Table 6.1: Overview of research construct and their expected influence

<table>
<thead>
<tr>
<th>Organizational IS climate factor</th>
<th>Expected effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS education and communication</td>
<td>[+ ] Security education via IS training, the provisioning of IS policies and IS communications can improve the IS knowledge, which can improve the IS attitude and behavior of employees.</td>
</tr>
<tr>
<td>Openness on IS</td>
<td>[+ ] Openness on information security risks and (near) incidents. Being open is expected to increase employees’ knowledge on IS and improve their attitude and behavior towards IS requirements.</td>
</tr>
<tr>
<td>Employee involvement</td>
<td>[+ ] Involvement of employees in IS decision making activities. A high involvement is expected to increase employees’ knowledge. Additionally, involvement of employees is expected to result in a better understanding and/or more accepted IS decisions. Thereby, involvement could improve employees’ attitude towards IS.</td>
</tr>
<tr>
<td>Management commitment</td>
<td>[+ ] Higher commitment entails that the management champions IS and adheres to the IS requirements. A higher commitment is expected to positively influence employees’ attitude towards IS behavior.</td>
</tr>
<tr>
<td>Task orientation</td>
<td>[- ] The orientation on completing the task. A high priority on productivity over IS could result in ignoring IS requirements to fulfill business goals (i.e. work done in time).</td>
</tr>
<tr>
<td>Work impediment</td>
<td>[- ] The extent to which IS requirements form an impediment to the work of the employee. A high work impediment is expected to decrease the attitude towards secure IS behavior.</td>
</tr>
</tbody>
</table>

**Task orientation**

A high orientation on completing tasks, also expressed as priority on productivity over information security could result in ignoring information security actions. Especially when workload and the time to complete tasks is in imbalance, employees will tend to break rules and take shortcuts (Albrechtsen, 2007; Bulgurcu et al., 2010).

Experts expressed that management has in important role in defining business priority for information security, finding the balance between orientation on goals and tasks and meeting the information security requirements.

**6.4.2. Variables not included in the model**

Not all variables identified during the review of literature and during the interviews of experts are included in the research model. The reasons for the exclusion are various. The management related variables such as management support and transformational leadership are party covered with management commitment. Employees risk severity and vulnerability cannot be monitored in practice due to legal restrictions. These restrictions are also reason for excluding the impact of rewards.

Other variables (employee commitment, response efficacy, locus of control, norms, job satisfaction, attachment) were excluded as these were not mentioned nor advised to include during the expert interviews. The influence of the variables perceived behavioral control and self-efficacy is well established in literature, and therefore also these variables were not included.

A complete overview of the factors and the explanation for (not) including them in the further analysis is provided in appendix C.
6.5. Conclusion

Based on the findings discussed in this chapter, the following hypotheses are formulated:

- **H1**: Information security education and communication is, via improved knowledge, positively related to employees’ behavior
- **H2**: Openness on information security is, via improved knowledge and attitude, positively related to employees’ behavior
- **H3**: Employee involvement is, via improved knowledge and attitude, positively related to employees’ behavior
- **H4**: Work impediment is negatively related to employees’ attitude and behavior
- **H5**: Perceived management commitment is positively related to employees’ attitude and behavior
- **H6**: Task orientation is positively related to employees’ attitude and behavior

The expected relations are visualized in the research model shown in figure 6.1. The model is used for the statistical analysis in the next chapters.

![Research model](image)

**Figure 6.1: Research model**

In the next chapter the methodology to collect and analyze the data that will be used to test the model and its hypotheses is discussed.
Methodology of quantitative analysis

This chapter contains a discussion on the methodology of the quantitative data analysis, which is required to determine the significance and total effect of the factors and relations from the conceptual model. The methodology of qualitative analyses (i.e. literature reviews and expert interviews) is discussed at the start of the chapters in which these qualitative methods are applied.

In this chapter the data collection methodology and the data analysis method are discussed. First the methodology for measuring employee behavior and organizational climate is described, followed by the explanation of the data collection approach. Finally, the methodology for analyzing the collected data is discussed.

7.1. Methodology: measuring employee behavior & organizational climate

7.1.1. Measuring employee behavior

In the literature several ways are proposed to analyze the security behavior of employees. The most objective way is to measure the actual behavior via observation of employees. However, it is very difficult to capture all aspects of information security (e.g. password strength) and underlying motivations via observations (Lebek, Uffen, et al., 2014). Additionally, many companies are reluctant to share IS related information, due to its sensitive nature (Kotulic & Clark, 2004). Therefore, scholars often measure behavioral intention rather than the actual behavior. A strong relation between behavioral intention and the actual behavior is reported in the literature (Lebek, Uffen, et al., 2014). The measurement of the actual behavior of employees is very challenging and enough for a complete additional research. Therefore, the self-reported behavioral intention via a questionnaire is used.

As discussed in section 3.3.6 there are several ways to measure self-reported behavior via a questionnaire. Very generic questions like "I intend to comply with the requirements of the ISP of my organization" are prone to many different possible interpretations (Bulgurcu et al., 2010, p. 536). As mentioned before, therefore the HAIS questionnaire is used to capture a broad spectrum of different security areas for employees’ knowledge, attitude and behavior. The full set of the HAIS questions is shown in appendix A.

7.1.2. Measuring organizational climate

Similarly to the measurement of the security behavior, the by the employee reported state of the organizational climate factors is considered. Hereby, the actual experience of the employee is captured, rather than observed values or values reported in formal documents, like organizational charts. This approach allows for a broader selection of different companies, as not all company related information must be collected manually, but can be derived from the survey. Additionally, combined with the anonymous processing of the data, this can decrease the chance of social desirability bias (Bradburn et al., 1979; Nederhof, 1985; Paulhus, 1984).

Each of the included organizational climate factors is measured with multiple questions to increase the measurement accuracy. The questions are mainly based on existing questionnaires of other scholars, to enhance the measurement adequacy of the factors. For example the questions developed by Bulgurcu et al. (2010) to measure work impediment. A complete overview of the organizational climate questions and their grounding in literature is included in appendix F.

7.1.3. Collecting responses

The questionnaire is distributed via Surveymonkey, an online questionnaire service. The advantage of online questionnaires, over paper based surveys and / or interviews, is that it is easier and faster to collect and...
7.1.4. Questionnaire outline
The introduction of the questionnaire starts with an explanation of the study objective and how the answers are processed. Thereafter, the instructions for filling out the questionnaire are provided and the terms used in the questionnaire are explained.

After the introduction, first all HAIS-Q statements are provided. The order and instructions for the HAIS-Q statements are aligned with the process used by Parsons et al. (2017). First the knowledge related statements are shown. Thereafter, the attitude related statements, followed by the behavioral statements. Within each of the three parts the statements are presented in a random order.

According to Parsons et al. (2017) the HAIS-Q allows for modular use. Therefore, the initial plan was to analyze the effect of the organizational climate factors on three focus areas separately. However, the construct reliability within the focus areas on knowledge, attitude and behavior was too low for further analysis (see appendix D). To use the complete HAIS questionnaire, the statements of the remaining four focus areas were included in a second survey. The data of both surveys is combined based on the identifier of the service discussed in section 7.2.2.

Similarly to the HAIS-Q statements, the order of the organizational climate (OC) statements is randomized. All of the OC statements contain the same 5-point Likert answering scale, which ranges from strongly disagree to strongly agree.

All statements are shown in a random order within each block of statements and have a 5-point Likert answer scale.

Figure 7.1: Overview survey outline

7.1.5. Test questionnaire
The questionnaire is tested among several participants to determine the questionnaire duration, and to identify possible unclarity in the statements and other areas of improvement.

Based on the feedback of the participants the following changes are made:

- Improved explanation of definitions in introduction with examples
- Task orientated statements with "within the organization" were too ambiguous. Therefore, replaced organization with management specific statements.
- Cosmetic changes to the layout to improve the user experience (progress bar, questions per page etc.).

7.2. Data collection

7.2.1. Population
The target population for the survey are employees which have to deal with information security in their work. Working on information security climate can be seen as stage of a IS maturity which comes after setting information security requirements (ISO/IEC 21827:2008). When a company has no information security
guidelines, requirements, rules or procedures whatsoever, then the company is to immature on information security to focus on the IS climate. Considering the effort needed to reach a certain level of IS maturity and the lower probability of any information security guidelines, employees of small companies are excluded from this research. Additionally, to limit possible cultural influences as suggest by Connolly et al. (2017) and Hofstede (2001), the quantitative part of the research is targeted to US employees only. These considerations eventually result in the following respondent requirements:

- Company size is larger than 50 employees
- Employer poses any form of information security requirements
- Respondent uses a computer at work for at least 10 hours per week
- Respondent is working in the US

7.2.2. Sample
The respondents are recruited via the crowd-sourcing platform Amazon Mechanical Turk (AMT)\(^1\). AMT has the advantage that a large group of respondents can be reached within a short time-frame. This is helpful, as the research method for the data analysis, structural equation modeling, generally requires a large sample size (Hair et al., 2010; Kline, 2010). Additionally, it allows for the execution of longitudinal studies, as the responses of workers over multiple surveys can be combined based on the worker id.

To ensure that the workers from AMT meet the before-mentioned requirements and to safeguard the response quality, a qualification survey was send out to 2000 workers selected of AMT which meet the following criteria:

- Approval rate of previous work > 98%
- Experience of at least 100 assignments
- Located in US\(^2\)
- Non duplicate IP addresses\(^2\)
- Non duplicate and/or suspicious geolocation\(^2\)
- Verified location based on country IP\(^2\)

The qualification survey contained questions on current employment, company size, company IS requirements and computer use (see appendix E). From the 2000 workers a total number of 723 met the sample requirements. The latter group was targeted via their worker id to fill out the final survey. Due to budget constraints the total amount of paid spots was limited, which resulted in a total response from 325 workers. Due to the issues on the modular use of the HAIS-Q survey, as discussed in 7.1.4, an additional set of questions was send out to the respondents of the first survey. Thereby, the total number of responses was reduced to 310. An additional benefit of splitting the questionnaire in two parts is the reduced chance of respondent fatigue due to the reduced time per questionnaire.

In addition to the qualifications needed to fill in the questionnaire checks on the respondent attention and consistency were included in the questionnaires. Each of the attention checks contain the same 5-point Likert scale as the other statements. The attention checks exists of 5 simple statements, for example "select strongly disagree". Respondent consistency is determined based on the repetition of 2 equal statements in the questionnaire. Respondents which deviate 2 Likert steps or more are excluded from the further analysis due to limited consistency. Beside unengaged responses another explanation could be that the statements of the questionnaire itself made respondents change initial response. From the consistency statements with a deviation of 1, only the first response is included in the final dataset.

\(^1\) Amazon Mechanical Turk, see mturk.com
\(^2\) via TurkPrime's Mechanical Turk Toolkit, see turkprime.com
7.3. Methodology: structural equation modeling

Structural equation modeling (SEM) is a family of statistical models which can be used to analyze the dependence relationships among multiple factors (Hair et al., 2010; Kline, 2010). It consists of a combination of a measurement model and a structural model. The measurement model, which is based on factor analysis, is used to assess the representation of the unobserved factors (also known as latent constructs) by the observed indicator variable (statement used in the questionnaire). For the structural model a path analysis is used to analyze the significance and strength of the interrelationships between those latent constructs.

7.3.1. Suitability for study

The behavior of employees is a result of a whole complex of interactions between different security climate related factors and more generic factors (i.e. knowledge, attitude and behavior). The model presented in chapter 6 contains multiple factors with dependence relationships with other factors in the model. Almost all of these factors are latent factors which are measured via statements of the questionnaire. In short, SEM is suitable for this study as it enables (Hair et al., 2010, p. 635):

- The estimation of multiple and interrelated dependence relationships
- The representation of concepts in these relationships
- The ability to account for measurement error
- The definition of a model to explain the entire set of relationships

7.3.2. Application of SEM

As mentioned before the SEM-based model exists of two parts, the measurement model and the structural model. For each of these parts modeling choices and assumptions are made.

Measurement model

A factor analysis is used to analyze the measurement model. This can be done via an exploratory factor analysis (EFA) and / or a confirmatory factor analysis (CFA) (Kahn, 2006). Exploratory factor analysis (EFA) can be used to identify factors and to determine which variables (in this case statements of questionnaire) load on the factor. In the EFA no a priori assumptions are made on which factor a variable loads. Thereby, it allows for the identification of other factors than assumed during the construction of the questionnaire. During the analysis it may become clear that combining two factor or the opposite, splitting factors can improve the measurement model. In the confirmatory factor analysis the factors and its loading variables are (in contrary to EFA) fixed. As the name suggest this analysis is used to confirm the validity of the measurement model.

Although most of the factors and their loading statements are (in a slightly adjusted form) used in other studies, the combination of statements for the organizational climate related factors is not validated in other studies. It is important to obtain an unidimensional measurement model, which entails that the variables of the factors do not (partly) measure other factors. Otherwise the relation between certain factors can be wrongly embedded via cross loading of statements. Therefore, as suggested by Cabrera-Nguyen (2010) and Worthington and Whittaker (2006) a combination of both EFA and CFA is used as both techniques can complement each other.

The maximum likelihood function is used to estimate the model parameters for the EFA, CFA and the causal model itself. Thereby, it is important to keep in mind that this function, which is commonly used in SEM, requires a normal multivariate distribution (discussed in more detail later in this section). An oblique based rotation (promax) is used for the EFA, as it is very likely that the organizational climate factors correlate with each other. Additionally, the criteria shown in table 7.1 are used as thresholds for the EFA. The criteria to validate the CFA based measurement model and to determine the model fit, are shown in table 7.2 and table 7.3.
7.3. Methodology: structural equation modeling

Table 7.1: Criteria for factor analysis Hair et al. (2010)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Measure of Sampling Adequacy</td>
<td>≥ 0.50</td>
</tr>
<tr>
<td>Bartlett’s Test of Sphericity</td>
<td>&lt;0.05</td>
</tr>
<tr>
<td>Communalities</td>
<td>&gt;0.25</td>
</tr>
<tr>
<td>Factor loadings</td>
<td>&gt;0.50</td>
</tr>
<tr>
<td>Cronbach’s alpha</td>
<td>&gt;0.70</td>
</tr>
</tbody>
</table>

Table 7.2: Validity and reliability thresholds, based on Hair et al. (2010) and L. Hu and Bentler (1999)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Composite Reliability (CR)</td>
<td>&gt;0.7</td>
</tr>
<tr>
<td>Average Variance Extracted (AVE)</td>
<td>&gt;0.5</td>
</tr>
<tr>
<td>Discriminant Validity</td>
<td>Maximum Shared Variance (MSV) &lt; Average Variance Extracted (AVE)</td>
</tr>
<tr>
<td></td>
<td>√AVE &gt; inter-construct correlations</td>
</tr>
</tbody>
</table>

Causal model, summated scales and measurement error

The causal model is combined with the measurement to a SEM-based model in AMOS. It is possible to incorporate all separately measured variables in the SEM model, however with the amount of measured statements this hugely increases the model complexity. Alternatively, a summated scale or factor score can be used. With the sum-score each statement is weighted equal in the score. In the case of factor scores, the weight of statements on the factor can differ. However, these weights are more likely to be specific for the sample. Thereby, the generalization and reproducibility of the results may become challenging. Therefore, like in the study by Molin (2005), the summated scales are used.

For each factor a scale is formed via the summation of the high loading variables (statements of questionnaire) identified in the CFA. The reliability of the summated scale is determined by the Chronbach’s alpha. To improve the accuracy of the estimations of the causal model, the measurement error of the summated scale is taken into account. This is done via the procedure as outlined in Jöreskog and Sörbom (2001) and Molin (2005). Thereby, the measurement error of associated summated scale is set to the variance multiplied by 1 minus the reliability (Cronbach’s alpha).

Maximum likelihood assumption

An important assumption in a maximum likelihood based multivariate analysis, is the multivariate normal distribution of the data (Hair et al., 2010). The univariate normality is used to assess the multivariate normality assumption. This can give a good indication of multivariate normality (Hair et al., 2010). The univariate normality is based on visual validation of graphically represented distributions and by analyzing the skewness and kurtosis of the variables. No severe deviations from the normal distribution are shown in the plots of the variables. The skewness and kurtosis are analyzed based on the cut-off values (i.e. 2 and 7) for an acceptable degree of non-normality (Curran, West, & Finch, 1996; Finney & DiStefano, 2006). All variable meet the requirements of skewness and kurtosis, except for a few variables of the 63-item HAIS questionnaire. However, as discussed earlier in this section, these items are combined to form a summated scale. This summated scale meets the requirements of skewness and kurtosis.
7.3. Methodology: structural equation modeling

Table 7.3: Overview of measurement criteria based on (Bentler & Bonett, 1980; Bentler, 1990; Hair et al., 2010; Hooper, Coughlan, & Mullen, 2008; L. Hu & Bentler, 1999; Kline, 2010; Schermelleh-Engel et al., 2003).

<table>
<thead>
<tr>
<th>Measure</th>
<th>Description</th>
<th>Cutoff criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Terrible</td>
</tr>
<tr>
<td>$\chi^2$/DF</td>
<td>Chi-Square value assessed by the degree of discrepancy between the estimated and the observed covariances matrices, divided by the degrees of freedom to correct for the impact of sample size.</td>
<td>$&gt;5$</td>
</tr>
<tr>
<td>CFI</td>
<td>Comparative fit index which compares the $\chi^2$ of the model with the $\chi^2$ of the null model, while taking the sample size into account.</td>
<td>$&lt;0.90$</td>
</tr>
<tr>
<td>SRMR</td>
<td>The standardized average squared differences between the residuals of the estimated covariances and the sample covariances.</td>
<td>$&gt;0.10$</td>
</tr>
<tr>
<td>RMSEA</td>
<td>Root mean squared error of approximation. Determines the model fit to the populations covariance matrix with unknown, but optimally chosen estimates of the parameters. Thereby, favoring parsimonious models.</td>
<td>$&gt;0.08$</td>
</tr>
<tr>
<td>PClose</td>
<td>A one-sided test on to determine the probability that the model is close-fitting ($H_0$: RMSEA $\leq 0.05$)</td>
<td>$&lt;0.01$</td>
</tr>
</tbody>
</table>

7.3.3. Assessment of model fit

In a structural equation model the variables in the model are included with their measurement error. This inclusion of the measurement errors complicates the assessment of the model fit. The model fit needs to be evaluated via the simultaneous measurement of multiple criteria as there is "[...] no single statistical significance test that identifies a correct model given the sample data [...]" (Schermelleh-Engel, Moosbrugger, & Müller, 2003, p. 31).

Multiple (estimation method specific) fit indices have been developed to determine the model fit. The only statistically based absolute fit index is the $\chi^2$ test. However, scholars do not rely on this static anymore to reject or accept a model, due to its sensitivity to sample size and discrimination towards complex, sometimes overparameterized, models (Schermelleh-Engel et al., 2003; Van den Berg, 2006). As suggested by Jöreskog and Sörbom (1993), the ratio between the degrees of freedom and the $\chi^2$ is therefore used instead of the $\chi^2$ test. As this ratio based test is still sensitive to sample size (Bollen, 1989), the additional measures, shown in table 7.3, are used also to determine the model fit. Changes can be made to the model to improve the model fit, though these changes should be supported by theory.
In this chapter the results of the quantitative analysis are described. First the characteristics of the collected sample are described. Thereafter, the analysis of the measured model factors is presented. Finally, the analysis of the relations between the organizational climate factors and employees’ behavior is discussed.

### 8.1. Sample

#### 8.1.1. Response rates

After the changes discussed in section 7.1.5 the survey was distributed via Amazon mechanical Turk to 723 workers which meet the requirements stated in section 7.2.1. To enable the measurement of non-response bias among the workers, the topic of the questionnaire was not explicitly disclosed in the qualification survey. This resulted in the collection of 310 responses on the available paid questionnaire spots, with a response rate of over 42%.

#### 8.1.2. Data pre-processing

The data was pre-processed by the application of the attention and consistency checks discussed in section 7.2.2. Table 8.1 contains an overview of the number of respondents after the application of these checks. For the attention checks with specific assignment to select a value (e.g. select disagree for this statement) only responses with that specific value are approved. More tolerance was given for less specific statements, for example both disagree and strongly disagree responses were approved for the statement “usually, the color of grass is purple, red or blue”. For the consistency checks a deviation of 1 was considered to be acceptable. A higher tolerance, e.g. 2 steps, could result in the approval of responses with both disagree and agree for the same statement. For a complete overview of all checks, see appendix G. The application of all checks resulted in a final sample of 289 responses. All questions of the questionnaire are mandatory, therefore the collected data did not contain any missing values.

<table>
<thead>
<tr>
<th>Check</th>
<th>Number of checks</th>
<th>Failed responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attention</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>Consistency</td>
<td>2</td>
<td>19</td>
</tr>
<tr>
<td>Combined</td>
<td>7</td>
<td>21</td>
</tr>
</tbody>
</table>

#### 8.1.3. Sample composition and representativity

Before analyzing the collected data with SEM it is important to gain insight in the representativeness of the sample for the population. As discussed in 7.2.2 respondents were selected for the study on specific requirements (e.g. company size & computer hours). Thereby a specific part of the employed US population was targeted. Unfortunately, no information is available on the parts of the population which meet those specific requirements. Therefore, it is hard to make an accurate comparison between the sample and the population. However, to still give an indication of the representativeness of the sample a comparison is made with

The ratio between males and females, with slightly more working males, is in line with the ratio within the US working population. However, the age distribution within the sample shows a relatively high amount of respondents in the category 30-39 years. The proportion of older employees (above 50 years) seem to be less than expected based on the overall working population of the USA. Additionally, within the sample the education level is relatively high. This can have consequences for the translation of the sample based results towards the whole population. Though, it is important to keep the influence of the sample requirements in mind. For example, the requirement of at least 10 computer hours per week can result in a decrease of respondents with more hand-skilled jobs, which generally require a lower education level.

![Figure 8.1: US population vs sample](image)

Table 8.2 shows the other demographics, like the computer usage hours per week, of the sample are shown. The company size is relatively equally distributed among the categories. A relatively large part (79%) of the employees in the sample use the computer more than 25 hours per week.

Table 8.2: Overview of distribution of sector, company size, job level and computer hours within the sample

<table>
<thead>
<tr>
<th>Demographic</th>
<th>Label</th>
<th>Abs.</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sector</td>
<td>private sector</td>
<td>183</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>public Sector</td>
<td>82</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>non-profit sector</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>Company size (# employees)</td>
<td>51 - 200</td>
<td>65</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>201 - 500</td>
<td>52</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>501 - 1,000</td>
<td>44</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>1,001 - 5,000</td>
<td>42</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>5,001 - 10,000</td>
<td>31</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>10,000+</td>
<td>55</td>
<td>19</td>
</tr>
<tr>
<td>Job level</td>
<td>Entry Level</td>
<td>39</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Intermediate</td>
<td>139</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>Middle Management</td>
<td>90</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Senior Management</td>
<td>15</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Other</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Weekly computer hours</td>
<td>11-15</td>
<td>17</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>16-20</td>
<td>31</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>21-25</td>
<td>12</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>More than 25</td>
<td>229</td>
<td>79</td>
</tr>
</tbody>
</table>
8.2. Factor analysis

Multiple statements per (intended) factor are made in the questionnaire to measure each specific factor. Before using these statements to measure the factors, it is important to check whether the statements are unidimensional. This entails that they are only measuring 1 factor and do not load on other factors. According to Gerbing and Anderson (1988), it is important for the interpretation of the results that statements load only on 1 factor. As discussed in section 7.3.2, this is achieved via an exploratory and confirmatory factor analysis.

8.2.1. Exploratory factor analysis

The EFA is only performed on the organizational climate related factors, not on HAIS-Q factors (see section 8.2.3 for HAIS-Q explanation). The ML function is used for the EFA fitting procedure and for the rotation ProMax 4, as explained in 7.3.2. The Bartlett's test shows that it is possible to reduce the data. Also, the Kaiser-Meyer-Olkin Measure of Sampling Adequacy test is higher than the threshold of $\geq 0.50$.

For estimating the model, a minimal communality of 0.25 is required. Additionally, only factor loadings of 0.5 or higher are taken into account for the measurement model. Statements which load on multiple factors or statements which load far below the thresholds, are iteratively removed from the model. A full overview of the excluded statements is presented in appendix F. All of the statements for the organizational climate related factors meet the required communality of $> 0.25$.

Combining these criteria resulted in a 6 factor solution. Unfortunately, 1 of the 3 statements loading on the task factor is with 0.44 quite low. Additionally, the Cronbach's alpha is with 0.676 slightly less than the cut-off value of 0.70. As shown in appendix H all other factors have high loadings and a Cronbach's alpha $> 0.70$. The fitting of the task factor is quite close to the cut-off values, therefore this factor was included in a CFA model. However, as discussed in the next section, this did not result in a satisfying solution. A new EFA without the task items, results in a good model in which all remaining items have high factor loading. Additionally, the Cronbach's alpha of these factors is more than $> 0.70$.

8.2.2. Confirmatory factor analysis

The solution obtained in the EFA is analyzed in a measurement model in AMOS in which all of the latent factors are correlated. Based on this model the fit and validity measures of the measurement model are determined (using the criteria of table 7.3). Additionally, the model validity is calculated based on the criteria mentioned in section 7.3.2. The analysis of the 6 factor solution with task results in the values presented in table 8.3.

![Table 8.3: Validity and reliability analysis of 6 factor model](image)

Based on the values of table 8.3 the following observations can be made:

- The reliability: the CR for task is less than 0.70.
- Convergent Validity: the AVE for task is less than 0.50
- Discriminant Validity: the AVE for task is less than the MSV.
- Discriminant Validity: the square root of the AVE for task is less than its correlation with management.
Although the model fit of the 6 factor model is acceptable (see appendix H), the validity and reliability of the measurement model is problematic. It has a low Cronbach’s alpha, a low construct reliability, convergent validity and discriminant validity issues. Removing additional items from the task factor did not resolve the problems. Therefore, it was decided to drop the task construct from further analysis.

Fortunately, the solution with 5 factors performs considerably better (see table 8.4). The values of table 8.4 result in the conclusion that there are no validity concerns for this measurement model. Additionally, as shown in table 8.5, the model fit is also excellent. Therefore, this 5 factor combination with loading statements, as presented in table 8.6 is used for further analysis.

Table 8.4: Validity and reliability analysis of 5 factor model

<table>
<thead>
<tr>
<th></th>
<th>CR</th>
<th>AVE</th>
<th>MSV</th>
<th>MaxR(H)</th>
<th>Mngt</th>
<th>Workim</th>
<th>Involv</th>
<th>Edu</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mngt</td>
<td>0.912</td>
<td>0.635</td>
<td>0.531</td>
<td>0.928</td>
<td>0.797</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workim</td>
<td>0.894</td>
<td>0.679</td>
<td>0.196</td>
<td>0.91</td>
<td>0.336***</td>
<td>0.824</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Involv</td>
<td>0.864</td>
<td>0.615</td>
<td>0.267</td>
<td>0.867</td>
<td>0.517***</td>
<td>0.442***</td>
<td>0.784</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edu</td>
<td>0.84</td>
<td>0.569</td>
<td>0.531</td>
<td>0.852</td>
<td>0.728***</td>
<td>0.304***</td>
<td>0.426***</td>
<td>0.754</td>
<td></td>
</tr>
<tr>
<td>Open</td>
<td>0.797</td>
<td>0.568</td>
<td>0.161</td>
<td>0.8</td>
<td>0.385***</td>
<td>0.171*</td>
<td>0.304***</td>
<td>0.401***</td>
<td>0.753</td>
</tr>
</tbody>
</table>

*p < 0.050, ** p < 0.010, *** p < 0.001

Table 8.5: Model fit of CFA

<table>
<thead>
<tr>
<th>Measure</th>
<th>Estimate</th>
<th>Threshold</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMIN</td>
<td>344,742</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DF</td>
<td>179</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMIN/DF</td>
<td>1,926</td>
<td>Between 1 and 3</td>
<td>Excellent</td>
</tr>
<tr>
<td>CFI</td>
<td>0.952</td>
<td>&gt;0.95</td>
<td>Excellent</td>
</tr>
<tr>
<td>SRMR</td>
<td>0.058</td>
<td>&lt;0.08</td>
<td>Excellent</td>
</tr>
<tr>
<td>RMSEA</td>
<td>0.057</td>
<td>&lt;0.06</td>
<td>Excellent</td>
</tr>
<tr>
<td>PClose</td>
<td>0.109</td>
<td>&gt;0.05</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

8.2.3. HAIS-Q

The human aspects of information security questionnaire (HAIS-Q) contains 63 statements on 7 different focus areas (password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting). Each of these focus areas has 3 statements on knowledge, attitude and behavior.

When the knowledge, attitude and behavior for each focus area is considered separately, the reliability (measured via Cronbach's alpha) is too low (see appendix D). Hence, it is not possible to (reliably) determine the score of the respondent on knowledge, attitude and behavior for a specific focus area.

Alternatively, the scores on knowledge, attitude and behavior can be measured by combining the statements of all focus areas. Thereby, more items, 21 instead of 3, are used to measure these constructs. The resulting Cronbach's alpha values indicate that this results in a reliable scale. As all statements are measured on a 5-point Likert scale, this results in a range of possible scores between 21 and 105. Similar to the organizational climate factors, the Likert scale of the reversed coded statements is corrected in such a way that a higher score on the construct represent a better knowledge on IS, a higher attitude towards IS or more secure IS behavior.
8.2. Factor analysis

Table 8.6: Organizational climate factors and their measurement statements, see appendix F for references

<table>
<thead>
<tr>
<th>Factor</th>
<th>Question</th>
</tr>
</thead>
</table>
| Education             | - My organization educates employees on their information security responsibilities  
|                       | - Business communications (e.g. notices, posters, newsletters) are used to promote security awareness multiple times per year  
|                       | - The information security requirements (e.g. policies) of my company are clear, understandable and readily available  |
| Involvement           | - In my organization employees’ suggestions regarding information security are never considered  
|                       | - In my organization employees are never asked for their opinions before making decisions regarding information security  
|                       | - In my organization employees are involved in decisions regarding information security  
|                       | - Information security suggestions of employees from all function levels are taken seriously  |
| Management commitment | - Senior management is interested in information security issues  
|                       | - Senior management’s words and actions demonstrate that information management is a priority  
|                       | - Visible support for information management goals by senior management is obvious  
|                       | - Senior management actively champions information security goals  
|                       | - Top managers adhere to information security policies themselves  |
| Openness              | - In my organization we seldom talk about information security errors  
|                       | - In my organization we always discuss information security issues when such issues come up  
|                       | - In my organization we can talk freely and openly about information security risks  |
| Work impediment       | - Complying with the company’ information security requirements holds me back from doing my actual work  
|                       | - Complying with the company’ information security requirements slows down my response time to my colleagues, customers, managers etc.  
|                       | - Complying with the company’ information security requirements hinders my productivity at work  
|                       | - My efficiency at work is not affected by complying with the company’ information security requirements  |

Note: all statements are answered on a 5-point Likert scale, ranging from strongly disagree to strongly agree. For the reversed coded statements, the Likert score is reversed in such a way that a high score on these construct represent a higher degree / more of that construct. For example a higher score on education means that the organization does more on education.

The HAIS questionnaire is already validated in multiple studies (see Parsons et al. (2017)). Therefore, no factor analysis is done on the HAIS-Q statements. As shown in table 8.7, the measurement reliability of the constructs is comparable with other studies.

Table 8.7: Comparison Cronbach’s alpha with values reported in literature

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>113</td>
<td>500</td>
<td>197</td>
<td>289</td>
</tr>
<tr>
<td>Knowledge</td>
<td>0.88</td>
<td>0.84</td>
<td>0.84</td>
<td>0.82</td>
</tr>
<tr>
<td>Attitude</td>
<td>0.88</td>
<td>0.88</td>
<td>0.93</td>
<td>0.88</td>
</tr>
<tr>
<td>Behavior</td>
<td>0.91</td>
<td>0.92</td>
<td>0.90</td>
<td>0.86</td>
</tr>
</tbody>
</table>
8.3. Structural equation model

In this section the results of the SEM-based analysis are presented. The factors and their measurement error identified in the factor analysis are combined with the expected relations between the factors. As discussed in chapter 6, the expectations for these relations are based on the literature review and expert interviews.

8.3.1. Model-fit

Before testing the significance and effect of the relations between the factors it is required that the model fits. Therefore, if the model does not fit the requirements stated in section 7.3.3, no conclusions can be made on the relations and factors in the model.

The model fit measures of the original model are presented in table 8.8. Although the model shows a good fit on some of measures, the model fit value of the root mean squared error of approximation is terrible. Additionally, the values of CMIN/DF and PClose indicate a barely acceptable model fit value. Therefore, it is concluded that the model does not fit well enough.

Table 8.8: Model-fit of original version SEM model

<table>
<thead>
<tr>
<th>Measure</th>
<th>Estimate</th>
<th>Threshold</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMIN</td>
<td>18.49</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DF</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMIN/DF</td>
<td>4.623</td>
<td>Between 1 and 3</td>
<td>Acceptable</td>
</tr>
<tr>
<td>CFI</td>
<td>0.987</td>
<td>&gt;0.95</td>
<td>Excellent</td>
</tr>
<tr>
<td>SRMR</td>
<td>0.031</td>
<td>&lt;0.08</td>
<td>Excellent</td>
</tr>
<tr>
<td>RMSEA</td>
<td>0.112</td>
<td>&lt;0.06</td>
<td>Terrible</td>
</tr>
<tr>
<td>PClose</td>
<td>0.02</td>
<td>&gt;0.05</td>
<td>Acceptable</td>
</tr>
</tbody>
</table>

To increase the model fit some improvements have to be made to the original model. First all non-significant paths were removed. This did not result in a good model fit. Therefore, the relations of the original model were revised. For this step only relations were added which are supported by theory from literature and/or the expert interviews.

The most important changes in the revised model are the relations from education & communication and involvement to work impediment. The substantiation for this relation is based on a combination of literature and expert interviews, in which repeatedly the importance of practice based education and communication about the vulnerabilities of the company, to the acceptance of information security measures was mentioned. A higher acceptance and understanding of measures, combined with improved skills, leads to an decrease in the perception of work impediment.

This is strongly linked to the relation between employee involvement and work impediment. Nearly all experts express that involvement of employees is crucial to develop high quality balanced information security measures. By listing to employees’ suggestions and by incorporating employees’ feedback on the impact of security measures on their daily work, more balanced security measures can be developed. Thereby, the work impediment can be reduced and employee acceptance can increase.

The positive relation of both education and involvement to work impediment is confirmed in several studies. More education and higher involvement of employees can result in better alignment or more practical and less burdensome information security measures, which on its turn influence the perception of work impediment (Bauer & Bernroeder, 2017; Connolly et al., 2017; D’Arcy & Greene, 2014; Kines et al., 2011; Neal et al., 2000; Spears & Barki, 2010).

Another revision in the model is the direct relation from work impediment to behavior. In case of a high work impediment this can, even when the attitude of an employee on the risk of not following certain IS handlings is adequate, still result in non-secure behavior. As mentioned by Vance et al. (2012), employees perceives measures to comply with the information security policy often as a barrier to productivity, since
these measures requires time and effort. Bulgurcu et al. (2010) confirmed the direct relation from work impediment to the perceived cost of compliance. This perceived impediment on their work directly influences the behavior of employees. Experts mention the ease of use and impact of security measures as one of the most important triggers of (non)compliant behavior of employees. The more difficult it is to implement certain measures in the daily practice, the quicker employees will search for alternative solutions. For example, expert #1 emphasis that more handling steps, for instance, to encrypt confidential information, directly lead to more non-compliant behavior.

The final model with the discussed revisions is illustrated in figure 8.2. As shown in table 8.9, this revised model has an excellent model fit.

Table 8.9: Model-fit of revised version SEM model

<table>
<thead>
<tr>
<th>Measure</th>
<th>Estimate</th>
<th>Threshold</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMIN</td>
<td>25,211</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DF</td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMIN/DF</td>
<td>1,939</td>
<td>Between 1 and 3</td>
<td>Excellent</td>
</tr>
<tr>
<td>CFI</td>
<td>0,989</td>
<td>&gt;0.95</td>
<td>Excellent</td>
</tr>
<tr>
<td>SRMR</td>
<td>0,035</td>
<td>&lt;0.08</td>
<td>Excellent</td>
</tr>
<tr>
<td>RMSEA</td>
<td>0,057</td>
<td>&lt;0.06</td>
<td>Excellent</td>
</tr>
<tr>
<td>PClose</td>
<td>0,326</td>
<td>&gt;0.05</td>
<td>Excellent</td>
</tr>
</tbody>
</table>

8.3.2. Significant relations

In figure 8.2 the path coefficients and portion explained variance of the revised model are shown. All relations shown in the figure are all significant on .05 level. With SEM it is possible to calculate the direct and indirect effects of the factors on the other endogenous factors in the model. In table 8.10 the standardized total of the direct and indirect effects are presented. In the next section the model findings are discussed in more detail.

Figure 8.2: Estimated revised model with standardized direct effects. All relations shown are significant on the .05 level. For more details on the model, see appendix I
8.3. Structural equation model

Table 8.10: Total effect from factors in the model on Attitude, Behavior, Knowledge and Workimpediment

<table>
<thead>
<tr>
<th>To</th>
<th>Total effect from:</th>
<th>Mngt</th>
<th>Educ</th>
<th>Invo</th>
<th>Open</th>
<th>Knowledge</th>
<th>Workimp</th>
<th>Attitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Workimp</td>
<td>0</td>
<td>0</td>
<td>-0.165</td>
<td>-0.375</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Attitude</td>
<td>0.105</td>
<td>0.49</td>
<td>0</td>
<td>0.161</td>
<td>0.883</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Behavior</td>
<td>0.097</td>
<td>0.466</td>
<td>0.033</td>
<td>0.148</td>
<td>0.813</td>
<td>-0.088</td>
<td>0.921</td>
<td></td>
</tr>
</tbody>
</table>

8.3.3. Model findings

The model findings on the significant relations, the direct and indirect effects of the factors, and the explained variances presented in figure 8.2 are discussed in this section. A more detailed discussion on how these findings relate to the observations by IS experts and the findings of other scholars is included in section 9.1. For the interpretation of the modeled relations, it is important to realize that it is not possible to quantitatively determine the direction of the relations within the SEM model. Therefore, the findings from the experts interviews and literature are used.

Endogenous factors and explained variance

Before going into detail on the organizational climate factors, it is important to first look at the main building blocks of the model; the endogenous factors knowledge, attitude, behavior and work impediment. As discussed in section 8.2.3 a higher score on these items stands for more IS knowledge, a better attitude towards IS and a more secure IS behavior.

Within figure 8.2 it is clear that the relation between knowledge and attitude is very strong (0.88). Even stronger is the relation between attitude and behavior (0.92). However, the direct relation between knowledge and behavior, as shown in figure 3.3, turns out to be not significant when added to the revised model (see figure 8.2). This in contrary to the findings reported by Parsons, McCormac, Butavicius, et al. (2014) which found this relation to be significant with a strength of 0.19. In their study, the relation between knowledge and attitude is less strong (0.81). Also, the relation between attitude and behavior is less strong (0.74) than the value found in this study. Additionally, Parsons, McCormac, Butavicius, et al. (2014) do not use a variation of structural equation modeling. Thereby, no correction for the measurement error is included in their model.

Explained variance (shown in green in figure 8.2) entails the amount of variance that can be explained by the factors and relations in the model. The explained variance of attitude and behavior is high (0.88 - 0.90). Especially the relations knowledge - attitude and attitude - behavior contribute to the high variance of these factors. Due to the less strong relations in the before mentioned model of Parsons, McCormac, Butavicius, et al. (2014), the variance of attitude and behavior is also less high (0.66 - 0.78). The strong relations from knowledge to attitude and from attitude to behavior can contribute to the non-significance of the relation from knowledge to behavior. An additional explanation can be found in the formulation of the HAIS statements. The use of normative language on the knowledge items may have (unintentionally) strengthened the relation between knowledge and attitude.

The explained variance of knowledge (0.42) and work impediment (0.23) is limited in comparison with the variance of attitude and behavior. This non-surprising difference is mainly due to the strong relations between knowledge, attitude and behavior. The relatively low variance of work impediment and knowledge, suggest that other factors, not included in the model can account for the remaining variance of work impediment and knowledge. For example the unexplained variance of information security knowledge might partly be explained by the trainings provided by a former employer.
IS education and communication
The factor education and communication has a significant relation with the knowledge of employees. This factor has with 0.56 a relatively strong positive direct effect on the knowledge, meaning that more education and communication is related to a higher knowledge on information security. This factor has the largest total effect (0.47) on information security behavior of all organizational climate factors.

The factor education and communication also has a significant negative relation (-0.17) with the perceived work impediment. This suggests that IS training and communication is related to reduced work impediment. For example, via improved IS skills which reduce the effort needed to meet the IS requirements. Additionally, it could, via better understanding of the importance of information security, change the perception that IS measures pose a burden.

Work impediment
Work impediment has in the model a significant, but weak, negative direct relation with behavior. Increased work impediment can result in less secure behavior. So, when certain security handlings are very time consuming or burdensome, it is expected that also less secure behavior can be observed. Though, the magnitude of the total effect from work impediment on employees' IS behavior is limited (-0.09).

Employee involvement
Employee involvement entails listening to, and asking for suggestions regarding information security. This has in the model a significant negative direct effect (-0.38) on the perceived work impediment. Thereby, the effect is more than twice the direct effect of education and communication on the work impediment. This suggests that involving employees in IS can help to reduce the work impediment, i.e. via better alignment of IS measures. So, increased employee involvement can, via decreased work impediment, improve employees' IS behavior. However, the total effect of employee involvement on IS behavior is very low (-0.03).

Management commitment
Within the model the commitment of the management has a significant positive direct effect on the attitude of employees. This direct effect is with 0.11 relatively low in comparison with the effect of knowledge (0.88).

Although management commitment has a significant relation with attitude, the total effect of management commitment on IS behavior is with a value of 0.10 lower than expected based on the expert interviews. More on this relation is discussed in section 9.1.5. However, it is important to note that management also has influence on the other factors, which is not captured in the management commitment construct. For example by making decisions on the resources for IS education. Concluding, the significant relation between management commitment and attitude is as expected, however weaker than one would expect based on the expert interviews.

Openness on IS
The openness on information security has a positive significant relation (0.18) with the knowledge of employees. When added to the model shown in figure 8.2, the relation between openness and attitude is not significant. This suggest that openness does not directly effect the attitude of employees. However, indirectly, via increased IS knowledge, openness can still affect employees' attitude towards IS. As suggested by the IS experts, being open on information security errors and risks is related with more knowledge on IS. Due to the large influence of knowledge on IS behavior (0.81), openness has via its positive relation with IS knowledge the second largest total effect (0.15) of the organizational climate factors.

8.4. Conclusion
After filtering the out the failed responses on the attention and consistency checks, a sample of 289 respondents is available for the analysis. In comparison with the data of the US bureau of labor statistics, the sample contains relatively many respondents in the age category of 30-39 years old. However, this can partly be caused by the requirements mentioned in section 7.2.1. It is important to keep this in mind for the generalization of the results.

In the factor analysis the task orientation construct showed reliability, discriminant validity and convergent validity issues. Additionally, the measurement model with the task orientation construct did not have a good model fit. Therefore, this construct was dropped from further analysis. The measurement model without the task construct showed no validity issues and has in a good model fit.
8.4. Conclusion

The original research model, presented in chapter 6, results in a SEM model with a bad model fit. It is essential to have a good model fit to be able to make any statements on the significance and weight of the modeled relations. Therefore, the original model is improved. Only adjustments which are supported by literature and/or the expert interviews were made. The most important changes are the removal of non-significant relations and the addition of other relations, like the indirect relation of employee involvement via work impediment rather than directly to attitude, the relation from education and communication to work impediment and the direct relation from work impediment to the behavior of employees.

The revised model, shown in figure 8.2, has an excellent model fit. In this model education has the strongest standardized total effect on behavior (0.47), followed by openness (0.15). The standardized total effect of management involvement and work impediment on employees’ behavior is with 0.10 and -0.09 limited, but still significant.
Conclusion and discussion

This chapter provides the conclusion of this research on the influence of organizational climate factors on the behavior of employees. The results of the quantitative analyses are discussed in relation to the reviewed literature and experiences from the information security (IS) experts. Based on the SEM-based analysis of the final model, the hypotheses, as formulated in chapter 6, are discussed. In this section (9.1) also the main findings are discussed and conclusions drawn. Additionally, the main research question is answered. Thereafter, the limitations of this thesis are discussed and recommendations are provided. Finally, the scientific, managerial and societal implications are discussed.

9.1. Main findings

In this section the findings from the quantitative analysis are discussed in relation to the findings from the qualitative analysis. So, the findings from the structural equation modeling (SEM) analysis are compared with the findings from the safety climate literature, the information security climate literature and the experts interviews. For this comparison it is important to keep in mind that many different theories are used to analyze the information security behavior of employees (see chapter 3).

The use of different theories and a wide variety in operationalization of the factors, combined with the use of different modeling techniques (e.g. SEM vs SEM-PLS), limits the possibilities for a completely objective and fair comparison. However, this comparison can still give some indication on the similarities to the findings reported in the literature.

Furthermore, it is important to realize that it is not possible to quantitatively determine the causality of the relations within the SEM model. However, findings from the experts interviews can give an indication of the expected causality. Additionally, the discussion on the findings of the quantitative analysis is combined with the findings from the qualitative analysis (literature review and expert interviews) to provide a more enriched context and explanation.

9.1.1. IS education and communication

Hypothesis 1: Information security education and communication is, via improved knowledge, positively related to employees' behavior

Information security policy requirements and IS knowledge

In the quantitative analysis, the factor IS education and communication has a strong (.56) significant positive relation with knowledge, which on its turn positively relates, via attitude, to the self-reported behavior of employees.

For the comparison of this relation with findings reported by other scholars it is important to keep the operationalization of the construct in mind (see table 8.6). In this study this factor combines education, communication and the availability of requirements (e.g. policies).

Several scholars have analyzed the effect of information security policy (ISP) requirements on the intention towards secure or compliant IS behavior and self-reported IS behavior. In the study by Boss et al. (2009) this has via the perceived mandatoriness of IS a significant effect on the reported behavior. Similarly, ISP specification has, via increased information security awareness (operationalization mainly focused on knowledge), a significant positive effect on the intention towards ISP compliance (Haeussinger & Kranz, 2013). In a study by Cuganesan et al. (2018) no significant relation was found on between ISP specification...
and the attitude of employees. However, ISP specification had a significant relation on the self-efficacy (skills, knowledge, competencies and required effort) of employees.

Haeussinger and Kranz (2013) also found that security education is, via an increased ISA, significant related to a higher intention towards ISP compliance. In several other studies, a factor based on a combination of ISP, communication and training is used. In the study from Bauer and Bernroider (2017), education and communication had, via ISA and attitude, a significant effect on the intention. Similarly, Herath and Rao (2009b) reported a significant relation from education and communication to employees’ intentions. Also, a combination from ISP provisioning and education is reported to have a significant relation with employees’ intention.

The interviewed experts mentioned that ISP provisioning is just a first step. Additional trainings are considered to be very important to increase the knowledge and awareness of employees. Thereby, relevant tailored and frequent training are important.

Overall, it can be concluded that the findings on the relation between the factor education and communication and the knowledge of employees is in line with the findings of other studies. However, due to the many operationalization and modeling differences, the strength of the relation cannot be compared.

**IS education and communication and work impediment**

IS education and communication also have a significant negative (-.17) relation to work impediment. This relation is addressed by some security experts. They state that education can contribute to more insight in the vulnerabilities of the organizations, which result in improved understanding and acceptance of the required measures. Additionally, IS education can improve the skills of employees. These improved skills can decrease the effort needed to perform certain security handling, which explains the negative relation with work impediment. No reportings on this specific relation was found in the IS literature. However, increased information security awareness (which is reported to be effected by education) was reported by Bulgurcu et al. (2010) to have a significant negative relation (-0.24) with work impediment. Additionally, the safety climate studies from Neal et al. (2000) and Neal and Griffin (2006) confirm the effect of education on work impediment.

In summary, the findings from the expert interviews, the safety climate literature and the study by Bulgurcu et al. (2010) are in line with the findings of this thesis.

Concluding, findings of the quantitative analysis are in line with the findings reported by the security experts and scholars. Based on the standardized total effect, security education and communication has the largest effect on the employees' behavior from all included organizational climate factors. Therefore, it can be concluded that these findings provide support for the hypothesis.

**9.1.2. Openness on information security**

**Hypothesis 2**: Openness on information security is, via improved knowledge and attitude, positively related to employees’ behavior

In the estimated model, openness in an organization on information security risks and (near) incidents is, as expected, significantly and positively related with increased knowledge on information security (.18). However, no direct relation was found on the attitude of employees. The attitude of employees is related with openness on IS, but only via increased knowledge. This results in a total standardized effect of .15 on the behavior of employees.

The experts mentioned that discussing a (near) incident is the best way to increase employees knowledge and attitude towards information security. Additionally, an atmosphere which allows for openness on information security risk and issues can improve the attitude and behavior of employees. However, despite the presumed benefit, it remains difficult to obtain wide acceptance for openness in practice.

The openness on security errors and risks as operationalized in this study is barely touched in the IS literature. However, it is identified as important driver of safety in the safety climate literature (Neal et al., 2000; Kline, 2010). It is also suggested that, in contrary to the difficult acceptance of openness on IS, openness about safety risks and incidents in industrial settings is more commonly accepted (Kines et al., 2011; Neal et al., 2000).
The findings from the data analysis provide support for the relation between openness and employees’ behavior, albeit not directly via increased attitude, but only via knowledge. This makes that the hypothesis is only partly supported. More research within the field of information security on the effect of openness on IS risks and error could be interesting as the total effect is quite large and the IS literature on this factor is scarce.

9.1.3. Employee involvement

Hypothesis 3: Employee involvement is, via improved knowledge and attitude, positively related to employees’ behavior

Another interesting finding is the significant negative relation from involvement to work impediment. Limited research has been conducted on this specific relation. Spears and Barki (2010) studied the relation between user participation and information security risk management. In their study the participation of employees in IS turns out to have a significant (0.49) relation with the alignment between business and security. The participation of employees has overlap with the employee involvement construct of this study. Additionally, the alignment mentioned in the study by Spears and Barki (2010) has some similarity with the work impediment construct, which includes statements on the relation between IS requirements and the work productivity and efficiency. This suggests that a higher involvement of employees can result in better alignment or more practical information security measures, which on its turn will lead to more compliant behavior.

The relation between involvement and work impediment is not surprising, as nearly all experts express that involvement of employees can be useful to develop of high quality IS measures that are aligned with the business. Thereby, it is crucial to find a balance between the impact of the security measures and the level of security. Eventually, this can result in a higher acceptance of security measures by the business. Additionally, involving employees can help to identify risk which usually remain undetected.

Overall, the significant relation between employee involvement and work impediment seems to be in line with the findings from literature and practice. Although significant, the standardized effect of employee involvement on the reported behavior is very limited (0.03). So, hypothesis 3 is supported, but the effect of involvement is limited.

9.1.4. Work impediment

Hypothesis 4: Work impediment is negatively related to employees’ attitude and behavior

The estimated model shows a significant negative relation between the work impediment on the behavior of employees. This relation is, with a total standardized effect of -0.09 on behavior, relatively weak.

In the literature work impediment is included under the description “perceived cost of compliance”. Generally, it is about the time and effort required by the security requirements and the impacts of those requirements on the work. As mentioned by Bulgurcu et al. (2010) and Vance et al. (2012), employees perceives measures to comply with the information security policy often as a barrier to productivity. In the studies by Bulgurcu et al. (2010), Guo et al. (2011), Herath and Rao (2009b) and Vance et al. (2012) work impediment has a significant negative relation with the intention towards secure IS behavior. An exemption is the study by Ifinedo (2012) were no significant relation was found. A possible explanation for the latter finding is that in the operationalization a scale with “exceeds the benefits - lower than the benefits” was used, rather than the scale, from strongly agree to strongly disagree, used by the other scholars.

The interviewed experts mentioned that work impediment is one of the most important triggers for non-complaint behavior. More difficult security handling are more likely to be circumvented. Therefore, reducing work impediment by increasing the ease of use of the security measures is suggested to be important.

As mentioned before, involvement of employees in the development of information security can help to find practical and less burdensome measures that are accepted by the employees (Sommestad et al., 2017). As discussed in chapter 8, the impact of a positive attitude towards IS, can be negatively affected by a high work impediment. Though, the relation of work impediment with employee behavior is not strong (-0.09), it
still provides evidence for the fourth hypothesis. Concluding, the significance of the relation between work impediment and behavior is in line with the findings from literature and practice.

9.1.5. Management commitment

**Hypothesis 5**: Perceived management commitment is positively related to employees’ attitude and behavior

Management commitment has a positive significant relation with employees’ IS attitude. In comparison with the direct effect of knowledge, the direct effect of management commitment is rather low (0.88 vs 0.11).

Similarly, Cuganesan et al. (2018) found that management support, from which the statements are comparable to management commitment in this research, has a significant positive relation with attitude. Though, with 0.19 this relation is a bit higher than the value found in this paper (0.11). A possible explanation is that a large proportion of the variance is already explained by the knowledge construct. On the other hand, in the study by Q. Hu et al. (2012), the management participation, operationalized more as IS vision of management, had no significant relation with attitude.

Other scholars also reported a significant relation between management commitment and employees’ intention towards IS (AlKalbani et al., 2015; D’Arcy & Greene, 2014; Puhakainen & Siponen, 2010). Additionally, the importance of management commitment for employee’s behavior, is mentioned in the safety climate literature (Kines et al., 2011; Neal et al., 2000).

During the interviews the expert indicated that management commitment is critical. Experts mention that the influence of (top) management commitment can be either positive or negative on the IS behavior of employees. When this commitment lacks, this will directly negatively influence the IS behavior of employees. The commitment of management can also make a positive difference, for example by emphasizing the importance of IS for the business and leading by example.

As expected from the analysis of the literature and expert interviews, the estimated SEM model shows a significant relation between management commitment and attitude. This results, via the attitude in a total standardized effect on behavior of 0.10. This effect is relatively small. However, management commitment is also crucial for education, communication and openness. Despite the limited strength of the relation, the hypothesis 5 is still supported by the estimated model.

**Hypothesis 6**: Task orientation is positively related to employees’ attitude and behavior

The sixth hypothesis could not be analyzed, as it had to be dropped due to reliability issues combined with discriminant and convergent validity problems.

**Main research question**: What is the influence of the organizational information security climate on the information security behavior of employees?

The organizational information security climate of a company can be characterized by many different factors. Based on an extensive literature review and semi-structured interviews with 8 information security experts, a set of organizational IS climate factors, which are suggested to influence employees’ information security behavior, are selected. Based on a SEM model on a sample of 289 employees, five organizational climate factors are confirmed to be significant. Though, the total effect on the behavior of some factors is limited.

Overall it can be concluded that the organizational IS climate (in this case represented by education and communication, managerial commitment, employee involvement, openness on IS and work impediment) is positively related to (and thereby likely to influence) the information security behavior of employees.

However, as discussed in chapter 7, more research is required to provide more solid evidence for the influence of the organizational information security climate.
9.2. Limitations

Like all research, this research has its assumptions and limitations. Although countermeasures for methodological limitations have been used, some limitations remain. The limitations are discussed per research method, as most limitations are related to the research methods used.

9.2.1. Expert interviews

To integrate insights from practice, expert interviews were conducted with 8 information security experts from different companies in the Netherlands. The number of interviewed experts is too small to be representative for the whole population. Additionally, all experts were recruited via the network of Deloitte. Thereby, these companies have a certain amount of attention to information security which is clearly visible from the levels of IS matureness. The latter also has its advantages, as the experts of those companies have a high level of expertise.

Due to the sensitive nature of the topic, experts can be reluctant to fully disclose the limitations with regard to managing the IS behavior of their employees. To reduce this possible bias, all interviewed experts were promised anonymous processing of their statements.

Most information security experts fulfill a role of ensuring IS of the company. Thereby, they are likely to have a different perspective on IS than the employees themselves. To incorporate other perspectives, information security consultants were also interviewed, as these consultants can provide an outside view.

Due to time and budget constraints it was not possible to interview employees about their behavior. However, the view of employees is captured via the questionnaire. Because of budget constraints, this questionnaire was targeted to US employees. This difference between nationalities of experts and employees could have influenced the research results, though the international focused role of some experts can partly compensate this difference.

9.2.2. Questionnaire design and data collection

For the quantitative analysis, data collected via an online questionnaire was used. The measurement of IS behavior is based on self-reported behavior of employees. To limit different interpretations on "secure" or compliant IS behavior, a more granular measurement based on the HAIS questionnaire, was used. Although a link between behavioral intention and actual behavior is mentioned in the literature (Lebek, Uffen, et al., 2014), this cannot be guaranteed and verified for the sample. To increase the likelihood of fair responses, anonymous processing of the responses was promised to the respondents.

Although a modular use of the HAIS questionnaire was suggested by Parsons et al. (2017), the internal reliability of the knowledge, attitude and behavior parts for specific focus areas was too low to conduct an analysis on the specific focus areas. Therefore, all focus areas were combined, rather than analyzing each focus area separately. It is very well possible that some of relations between the organizational climate factors and the behavior of employees, differs between focus areas (e.g. influence of openness on incident reporting versus internet use). Additionally, the HAIS questionnaire has some shortcomings. The formulation of some HAIS statements seem to be outdated (e.g. focus on paper based information in the information handling focus area and not including a password manager or two factor authentication in the password management focus area). Additionally, the correlation between the knowledge and attitude items is high. A possible explanation is the use of normative language in the knowledge items, which results in overlap with the attitude statements.

The respondents for the questionnaire were recruited via Amazon mechanical turk (AMT). The choice for AMT to recruit employees was driven by the time and budget constraints. Targeting employees in the Netherlands would cost either more money (via paid panel service) or more time to gather the required responses. However, there are some limitations on the use of AMT for academic research (Goodman, Cryder, & Cheema, 2013; Mason & Suri, 2012). Especially the representation of AMT workers for the population can be challenging. To improve the sample quality a qualification survey was used to determine which respondents are part of the targeted population. As described in more detail in chapter 7, this survey contained checks on employment status and the use of a computer for work. Thereby, homemakers and unemployed are ruled out for the study. To limit the chance of false answers the exact topic of the study was not disclosed in the qualification survey. Additionally, only workers with a good reputation (% hits approved) and workers from the US were included (checked via IPs and other technical measures). Combined with the attention and con-
9.3. Recommendations

9.3.1. Recommendations for organizations

Based on the findings from both the qualitative and quantitative analyses, identifying organizational climate factors which influence the behavior of employees, a set of (preliminary) recommendations is formulated. Organizations can use these recommendations to improve and strengthen their information security climate and thereby the employees’ information security behavior in the organization. It is important to realize that, although some of recommendations seem to focus on the perception of individual employees, the combination of all employees’ experiences en perceptions are forming the information security climate within an organization. Ultimately, a strong information security climate can result in an increased security of companies’ information.

Before applying these (preliminary) recommendations, it is important to take note of the research limitations, as discussed in section 9.2. Additionally, more research might be required to confirm these findings (see section 9.3.2).

Education and communication

Most obvious, but also proven to be most important and effective to improve the information security climate, is the communication to, and education of employees. This factor has by far the largest effect in the quantitative analysis. As indicated by the scholars and the interviewed IS experts, providing information security policies and procedures is just a basis and will on itself not lead to improved IS behavior. More effective is to facilitate training about security rules and measures on a regular base, offering practical information in small chunks and related to the daily practice. Providing communication and training on a regular and frequent basis can help to ensure that the knowledge will not fade away. When connecting this information with appealing or actual topics, either related to the company itself, or recent events which employees get aware about via media, the training is suggested to be more effective. Thereby, education and communication can
contribute to better insights of employees in the vulnerabilities of the organization, which on its turn leads to improved knowledge and attitude. The improved and shared understanding of employees will lead to a higher acceptance of the required information security measures, resulting in a stronger information security climate and more secure information security behavior.

**Openness**
Closely related to the above suggestions is the recommendation to provide openness about (near) incidents and the current information security threats for the company. In the quantitative analysis this has, via increased knowledge, the second largest effect on the IS behavior of employees. As suggested by almost all experts, being open about (near) incidents can help to learn from the mistakes and increase the understanding of employees. In contrary to the findings from literature, the majority of the experts oppose actively sanctioning employee's IS mistakes (apart from extreme cases). This can result into a situation in which employees feel reluctant to be open on IS mistakes, which hampers the organizational learning and adequate early reporting of (near) incidents. Although openness on IS might be not easy to realize in practice, an open communication about safety risks and incidents has proven to be very effective to reduce the number of safety incidents in industrial settings. In line with the experiences with safety climate, openness can contribute to an information security climate which enables employees to share their experiences and to learn from incidents and mistakes.

**Involvement and work impediment**
This openness is also required for the involvement of employees in the improvement of information security measures. By involving employees, and aligning about possible measures, more practical solutions can be developed. For example, by identifying alternative handlings to reduce the work impediment of burdensome security measures. This can result in a lower impact of these measures on the daily work and thereby a higher acceptance and increased information security behavior. Additionally, this involvement opens up the possibility to identify not covered information security risks. Ensuring that measures are user-friendly is extremely important. Where possible, experts suggest to implement technical measures which can relieve the effort required by employees. Otherwise, involve employees to find acceptable and less burdensome solutions. This can result in an organizational climate, in which information security measures are formed via the shared effort of the employees in the organization, rather than dictated from an isolated IS department. As mentioned by an expert, it’s all about finding the balance.

**Management commitment**
Finally, it is extremely important to realize that these recommendations cannot be followed without the commitment of management. To emphasize the importance of compliant information security behavior for the organization, management should lead by example. Additionally, management should ensure that information security gets enough priority and is considered as an integral part of all business decisions and projects. It requires investments in time, money and trust of the management to create an organizational climate in which the employees are not seen as the biggest risk. Employees are the human sensors of the organization, and the first line of defense. Therefore, with the support and commitment of management, employees can positively contribute to the information security of the organization.

By providing education and information, involving employees where possible, creating openness, and embedding information security in all business activities, the combined effort from the whole organization can help to build a strong information security climate and to reach a higher level of information security.

**9.3.2. Recommendations for further research**
Based on these limitations, several recommendations for further research are discussed. In addition to the suggestions made in the previous chapters, other interesting research opportunities exist.

A study which incorporates the measurement of real IS behavior instead of self-reported behavior to increase the reliability of the results could be interesting. By combining this with another research method, the influence of the chosen data analysis method (SEM) can be ruled out. Additionally, this can provide more insight in the generalizability of the research results.

Other directions for further research are parts which did not fit in the scope of this study. As suggested by Connolly et al. (2017), cultural differences can play an important moderating role in the influence of organizational climate measures and employees’ IS behavior. In this research, this influence was kept constant by
focusing on a single country, however it can be interesting to investigate this influence. Similarly, it would be interesting to repeat the research in other countries, e.g. the Netherlands and to compare the differences.

Finally, in the quantitative analysis the relation between of openness on information security incidents and errors has a significant effect on the IS behavior of employees. However, the research on this relation within the field of information security is scarce. Therefore, this can be an interesting direction for further research.

9.4. Implications
In this section the implications of the research findings are discussed. The scientific contributions to the academic literature will be addressed first. Thereafter the societal contributions of identifying the relation of the organizational climate to employees’ behavior is discussed.

9.4.1. Scientific implications
This research contributes in various ways to the research on employees information security behavior in an organizational context. First, by an extensive review of the literature of organization climate, safety climate literature, and literature on information security and employee behavior. This resulted in an unique overview of potential influencing organizational climate factors and their relation to employees’ information security behavior.

Second, by combining these insights from research with the experiences from informations security experts, via semi-structured interviews. The aggregated input provides a good insight in which factors and processes can contribute to a change in employees’ behavior.

The third contribution results from the formulating and statistically testing of research model. The results confirm some expected relations and provide also new surprising insights, which add to the currently scarce amount of quantitative scientific research on the relation of the organizations’ climate to employee information security behavior in a business environment.

9.4.2. Managerial and societal implications
The insights from this research can be beneficial for organizations to increase their employees’ security behavior. The results from this research, can be used to focus on specific factors or processes, which are identified as influential. Organizations can use this knowledge as input for their information security approach and activities to improve employee security behavior, for example by involving employees in the discussion about security measures. The can lead to a reduction of the work impediment and more compliant employee information security behavior, contributing to a higher information security in organizations.

The proven importance of education and communication on employee behavior, combined with the effect of openness on security risks can trigger organizations to further improve their information security programs. Via these improved information security measures, this study can ultimately contribute to a reduction of cyber security incidents due to human behavior.
This chapter contains a reflection on the choices made during the project and the process of the project itself.

10.1. Choices in project
The information security behavior of employees is an intriguing research area. Many different factors are suggested to play some role in the IS decisions of employees. In this project the choice was made not to include the influences of personality traits and cultural differences. It would be interesting to analyze whether the effect of organizational climate factors is moderated by personality traits. However, due to the limited time available the decision was good, as it allowed for a more in depth focus on the remaining part.

The choice for a panel from the US in combination with experts of the Netherlands was not optimal, as cultural differences could play a role. Therefore, it would be better to have experts from the same country as the questionnaire is send out. The first plan was to target Dutch employees, however, due to cost constraints the choice was eventually made for US employees.

US employees were targeted via Amazon mechanical turk. This platform has the advantage of being a relatively cheap and fast way to get responses. However, it remains difficult to make sure that the respondents are part of the target population. Therefore, checks were added to exclude non-relevant respondents, like homemakers. Additionally, attention and consistency checks were included in the questionnaire. Although this increase the assurance that the respondents actually paid attention, it may also have excluded “sloppy” employees, which could be an interesting target for an adversary. The choice for targeting specific employees could have been optimized slightly better, by correcting for the age differences of the AMT population.

Looking back on the choice for the HAIS questionnaire, it can be concluded that it did not turn out to be usable as instrument for separate analysis on specific focus areas, which made an additional survey round required. It would have been nice to investigate the differences in effect of the organizational climate OC between IS focus areas. The knowledge, attitude and behavior factors of the HAIS-Q have a very strong correlation. Therefore, limited unexplained variance remains left for the OC factors. A more granular model (e.g. TPB) could also be interesting. However, there is currently no well tested instrument with granular IS measurement, like HAIS-Q, for that theory. Another limitation of the HAIS-Q is that it is quite easy for respondents to obtain high scores, more advanced and recent security statements, e.g. the use of two factor authentication and password managers, could be added to measure beyond the basic level. Although the HAIS-Q has its limitations, from the available options the HAIS-Q was an overall good choice. However, ample room remains for the improved measurement instruments on IS behavior.

10.2. Project process
I was provided the possibility to write this thesis at Deloitte. This unique opportunity allowed me to gain knowledge from the expertise of my colleagues and to integrate more insights from practice. As mentioned before, the research area of information security behavior has many interesting topics to research. Therefore, it can be challenging to determine a reasonable scope. The extensive literature review and discussions on the elements to include in the research took quite some time. However, these valuable discussion with my supervisor really helped out to sharper my focus to obtain a better result.

My colleagues provided me the amazing opportunity to use their contacts to recruit IS experts for the interviews. These interviews provided very valuable insights on experiences from practice, which allowed for a better alignment of this research with practice. However, the expert interviews took much more time than
expected. Especially, the combination with the summer holidays made it more difficult to reach the experts. Additionally, the travel to each of the experts, combined with the full transcription of the interviews took quite some time. This made the planning of the research more challenging, but the obtained insights were definitely worth it.

10.3. Link with curriculum
The curriculum for a master of Complex Systems Engineering and Management requires a focus on a complex socio-technical problem, in which technical, ethical and managerial choices are addressed. This thesis, with a focus on information security and employee behavior in an organizational context, covers these aspects.

The socio-technical problem central in this thesis is the human aspect in information security, as the behavior of employees in organizations is crucial to protect the information security of companies. Although this thesis is about a large contemporary socio-technical problem, one might criticize that it is more research than design oriented. However, this study is about the engineering of an information security climate that facilitates the information security behavior of employees.

In this thesis the several artifacts which can contribute to the design of such a climate are analyzed via a literature review, interviews with experts and a quantitative analysis. The design of such an organizational climate requires analyzing the complexity of human behavior in relation to information security measures with a combination of technical and more process related knowledge. Thereby, it is important to realize that these interactions within the organizational information security climate are so complex that it is not possible to address these complex interactions in a single design within the limited time available for this thesis.

To study the relation between organizational information security climate and employees’ information security behavior a combination of aspects from computer science and management are used. Thereby, it fits with the information architecture track as it focuses on the alignment between engineering opportunities (e.g. the monitoring of employees) and organizational needs. For this analysis various actor perspectives, such as management versus employees, and their underlying motives, are considered. For example, the management decisions to monitor and reward or sanction employees’ behavior. The effect of these managerial decisions and ethical choices on employees’ behavior was discussed during expert interviews, the employee perspective in the quantitative analysis. Especially, during the expert interviews both technical and business process knowledge helped to discuss their experiences from practice. Additionally, the knowledge and skills obtained during the master were useful in the design and analysis of the model.

Overall, the combination of technical knowledge on information security and insights in organizational and managerial aspects proved to be valuable to develop a balanced view.
References


References


References


Appendices
<table>
<thead>
<tr>
<th>Focus area</th>
<th>Topic</th>
<th>Knowledge</th>
<th>Attitude</th>
<th>Behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password management</td>
<td>Using the same password</td>
<td>It’s acceptable to use my social media passwords on my work accounts.*</td>
<td>It’s safe to use the same password for social media and work accounts.</td>
<td>I use a different password for my social media and work accounts.</td>
</tr>
<tr>
<td>Password management</td>
<td>Sharing passwords</td>
<td>It’s a bad idea to share my work passwords with colleagues.*</td>
<td>It’s safe to have a work password with just letters.*</td>
<td>I share my work passwords with colleagues.*</td>
</tr>
<tr>
<td>Password management</td>
<td>Using a strong password</td>
<td>A mixture of letters, numbers and symbols is necessary for work passwords.</td>
<td></td>
<td>I use a combination of letters, numbers and symbols in my work passwords.</td>
</tr>
<tr>
<td>Email use</td>
<td>Clicking on links in emails from known senders</td>
<td>It’s always safe to click on links in emails from people I know.*</td>
<td>It’s risky to click on a link in an email from an unknown sender.*</td>
<td>I don’t always click on links in emails just because they come from someone I know.</td>
</tr>
<tr>
<td>Email use</td>
<td>Clicking on links in emails from unknown senders</td>
<td>Nothing bad can happen if I click on a link in an email from an unknown sender.*</td>
<td></td>
<td>I don’t open email attachments if the senders are unknown to me.</td>
</tr>
<tr>
<td>Email use</td>
<td>Opening attachments in emails from unknown senders</td>
<td>It’s risky to open an email attachment from an unknown sender.*</td>
<td></td>
<td>I don’t open email attachments if the senders are unknown to me.</td>
</tr>
<tr>
<td>Internet use</td>
<td>Downloading files</td>
<td>I am allowed to download any files onto my work computer if they help me to do my job.*</td>
<td></td>
<td>I download any files onto my work computer that will help me get the job done.*</td>
</tr>
<tr>
<td>Internet use</td>
<td>Accessing dubious websites</td>
<td>While I am at work, I shouldn’t access certain websites.*</td>
<td>Just because I can access a website at work, doesn’t mean that it’s safe.*</td>
<td></td>
</tr>
<tr>
<td>Internet use</td>
<td>Entering information online</td>
<td>I am allowed to enter any information on any website if it helps me do my job.*</td>
<td></td>
<td>I assess the safety of websites before entering information.</td>
</tr>
<tr>
<td>Social media use</td>
<td>SM privacy settings</td>
<td>It’s a good idea to regularly review my social media privacy settings.</td>
<td></td>
<td>I don’t regularly review my social media privacy settings.*</td>
</tr>
<tr>
<td>Social media use</td>
<td>Considering consequences</td>
<td>It doesn’t matter if I post things on social media that I wouldn’t normally say in public.*</td>
<td></td>
<td>I don’t post anything on social media before considering any negative consequences.</td>
</tr>
<tr>
<td>Social media use</td>
<td>Posting about work</td>
<td>I can post what I want about work on social media.*</td>
<td></td>
<td>I post whatever I want about my work on social media.*</td>
</tr>
<tr>
<td>Mobile devices</td>
<td>Physically securing mobile devices</td>
<td>When working in a public place, I have to keep my laptop with me at all times.</td>
<td></td>
<td>I leave my laptop unattended.</td>
</tr>
<tr>
<td>Mobile devices</td>
<td>Sending sensitive information via Wi-Fi</td>
<td>It’s risky to send sensitive work files via a public Wi-Fi network.*</td>
<td></td>
<td>I send sensitive work files using a public Wi-Fi network.*</td>
</tr>
<tr>
<td>Mobile devices</td>
<td>Shoulder surfing</td>
<td>When working on a sensitive document, I must ensure that strangers can’t see my laptop screen.*</td>
<td></td>
<td>I check that strangers can’t see my laptop screen if I’m working on a sensitive document.*</td>
</tr>
<tr>
<td>Information handling</td>
<td>Disposing of sensitive print-outs</td>
<td>Sensitive print-outs can be disposed of in the same way as non-sensitive ones.*</td>
<td>Disposing of sensitive print-outs by putting them in the rubbish bin is safe.*</td>
<td></td>
</tr>
<tr>
<td>Information handling</td>
<td>Inserting removable media</td>
<td>If I find a USB stick in a public place, I shouldn’t plug it into my work computer.*</td>
<td>If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer.*</td>
<td>I wouldn’t plug a USB stick found in a public place into my work computer.*</td>
</tr>
<tr>
<td>Information handling</td>
<td>Leaving sensitive material</td>
<td>I am allowed to leave print-outs containing sensitive information on my desk overnight.*</td>
<td>It’s risky to leave print-outs that contain sensitive information on my desk overnight.*</td>
<td>I leave print-outs that contain sensitive information on my desk when I’m not there.*</td>
</tr>
<tr>
<td>Incident reporting</td>
<td>Reporting suspicious behaviour</td>
<td>If I see someone acting suspiciously in my workplace, I should report it.</td>
<td></td>
<td>When I saw someone acting suspiciously in my workplace, I would do something about it.*</td>
</tr>
<tr>
<td>Incident reporting</td>
<td>Ignoring poor security behaviour by colleagues</td>
<td>I must not ignore poor security behaviour by my colleagues.</td>
<td></td>
<td>If I ignored my colleague ignoring security rules, I wouldn’t take any action.*</td>
</tr>
<tr>
<td>Incident reporting</td>
<td>Reporting all incidents</td>
<td>It’s optimal to report security incidents.*</td>
<td></td>
<td>If I ignored a security incident, I would report it.</td>
</tr>
</tbody>
</table>

Participants are instructed to respond to each item on a five-point scale from "Strongly Disagree" to "Strongly Agree." Reverse scoring was used on this item.
Interview guidance scheme

Overview of questions asked in during the expert interviews.
All expert interviews were held in person on the location of the experts.

- Kunt u me wat vertellen over uw functie en uw rol binnen de organisatie?
- Wordt u geïnformeerd over information security (IS) incidenten binnen uw organisatie?
  Zo ja, op welke wijze bent u betrokken?
  Zo nee, waar en met wie wordt informatie over IS incidenten gedeeld?
- Wat ziet u als de belangrijkste oorzaak van IS incidenten?
- Heeft uw organisatie IS richtlijnen?
  Zo ja, hoe zorgt u of uw organisatie ervoor dat medewerkers op de hoogte zijn van deze richtlijnen?
  Zo nee, waarom niet
- Wat is volgens u de meest effectieve manier om te zorgen dat medewerkers geïnformeerd zijn over de IS richtlijnen en IS risico’s van uw organisatie?
- Welke vormen van training zijn volgens u minder effectief?
- Denkt u dat kennis over IS invloed heeft op het gedrag van medewerkers?
  Zo ja, op welke wijze?
  Zo nee, waarom niet?
- Speelt het management een rol bij het IS gedrag van medewerkers.
  Zo ja, op welke wijze?
  Wat is de invloed van resources en commitment
  Wat is de invloed van het gedrag van het management
  Zo nee, waarom niet?
- Denkt u dat directe collega’s invloed hebben op het IS gedrag van medewerkers?
  Zo ja, op welke wijze? Kunt u voorbeelden geven?
  Zo nee, waarom niet?
- Wordt IS gedrag van medewerkers in uw organisatie gemeten / gemonitord?
  Zo ja, op welke wijze?
  Zo ja, hoe vindt terugkoppeling plaats?
  Worden er consequenties verbonden aan onveilig IS gedrag?
  Wat is volgens u het effect van sancties (of rewards)
  Zo nee, wat is de reden om niet te monitoren?
• Houden de medewerkers zich aan de IS richtlijnen?
  Zo nee, wat zijn de belangrijkste redenen waarom men zich niet houdt aan de IS richtlijnen?
• Vormen de de IS richtlijnen ervaren als een beperking voor de uitvoering van de werkzaamheden?
• Worden medewerkers betrokken bij het opstellen en/of aanpassen van IS richtlijnen en maatregelen?
  Zo ja, op welke manier worden medewerkers betrokken? Wat is het effect?
  Zo nee, waar is de reden om medewerkers niet te betrekken
• Wat voor andere activiteiten worden er ondernomen om het IS gedrag van medewerkers te verbeteren?
• Maakt IS gedrag, en de mate waarin medewerkers voldoen aan de richtlijnen, onderdeel uit van de bedrijfstargets?
  Zo ja, op welke manier?
• Denkt u dat het organisatieclimaat van invloed is op de wijze waarop IS richtlijnen worden nageleefd?
  (Open vraag naar mogelijke organisatieclimaat factored, evt. gevolgd door specifiek te vragen naar onderstaande lijst) Daarbij moet u denken aan elementen zoals
  Taak orientatie
  Hierarchy – hoe benaderbaar is het management
  Openheid om te spreken over IS in de organisatie
  Interactie met collega's
• Denkt u dat de sector waarin uw bedrijf zit een invloed heeft op het IS gedrag van de medewerkers?
  Bijvoorbeeld door de gevoeligheid van de informatie, wel/niet internationale karakter etc.
• Als u kijkt naar een aantal verschillende gedragingen, wat is dan volgens u de top 3 waarop het gedrag
  van de werknemers de meeste invloed heeft op IS incidents?
  Password management
  Internet use
  Social media use
  Mobile devices
  Information handling
  Incident reporting
• Wat denkt u dat de belangrijkste factoren zijn waarmee een organisatie invloed heeft op het gedrag van
  medewerkers (eerst als open vraag, evt. lijst voorleggen, mist u nog elementen op deze lijst)?
  Management support
  Peer behavior
  Rule orientation
  Goal / task orientation
  Sensitivity of information, industry
  User participation/involvement (business security alignment)
  Power-distance / hierarchy
  ISP provisioning / SETA programs
## Overview of identified factors

<table>
<thead>
<tr>
<th>Factor</th>
<th>Source*</th>
<th>Incl.</th>
<th>Rationale</th>
<th>Expected effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Top)management commitment and behavior [+]</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Yes</td>
</tr>
<tr>
<td>Management support</td>
<td>x</td>
<td>x</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Management priority [+](business vs IS)</td>
<td>x</td>
<td>x</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Transformational leadership</td>
<td>x</td>
<td>No</td>
<td></td>
<td>Partly covered in mgmt commitment &amp; behavior</td>
</tr>
<tr>
<td>ISP provisioning</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Yes</td>
</tr>
<tr>
<td>Security education [+]</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Yes</td>
</tr>
<tr>
<td>Aspect</td>
<td>+</td>
<td>±</td>
<td>-</td>
<td>Yes/No</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----</td>
<td>----</td>
<td>----</td>
<td>--------</td>
</tr>
<tr>
<td>Openness on information security [+]</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Yes</td>
</tr>
<tr>
<td>Employee involvement [+]</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>Yes</td>
</tr>
<tr>
<td>Risk severity employee (sanctions)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>No</td>
</tr>
<tr>
<td>Risk vulnerability employee (monitoring)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>No</td>
</tr>
<tr>
<td>Work impediment [-]</td>
<td>x</td>
<td>x</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Work pressure</td>
<td>x</td>
<td></td>
<td></td>
<td>No</td>
</tr>
<tr>
<td>Employee well-being</td>
<td></td>
<td></td>
<td>x</td>
<td>No</td>
</tr>
<tr>
<td>Job satisfaction</td>
<td></td>
<td></td>
<td>x</td>
<td>No</td>
</tr>
<tr>
<td>Factor</td>
<td>erw2</td>
<td>erw1</td>
<td>erw0</td>
<td>erw</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>Impact of rewards</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Perceived behavioral control</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self-efficacy</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response efficacy</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locus of control</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational environment</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rule orientation</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Goal orientation</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subjective norms</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer behavior</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee commitment</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* C: organizational and safety climate literature, IS: information security literature, E: expert interviews
Reliability of the HAIS-Q focus areas for knowledge, attitude and behavior. All Cronbach's alpha values are below the threshold of .70.

Table D.1: Reliability of knowledge, attitude and behavior specific focus areas of HAIS-Q

<table>
<thead>
<tr>
<th>Focus area</th>
<th>Knowledge</th>
<th>Attitude</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password management</td>
<td>.406</td>
<td>.513</td>
<td>.449</td>
</tr>
<tr>
<td>Email use</td>
<td>.484</td>
<td>.379</td>
<td>.476</td>
</tr>
<tr>
<td>Internet use</td>
<td>.606</td>
<td>.567</td>
<td>.650</td>
</tr>
<tr>
<td>Social media use</td>
<td>.468</td>
<td>.696</td>
<td>.318</td>
</tr>
<tr>
<td>Mobile devices</td>
<td>.591</td>
<td>.686</td>
<td>.629</td>
</tr>
<tr>
<td>Information handling</td>
<td>.428</td>
<td>.533</td>
<td>.586</td>
</tr>
<tr>
<td>Incident reporting</td>
<td>.457</td>
<td>.562</td>
<td>.719</td>
</tr>
</tbody>
</table>
Qualification questionnaire

• What is your gender?
  Female
  Male

• What is your age?
  17 or younger
  18-19
  20-29
  30-39
  40-49
  50-59
  60-older

• What is the highest level of school that you have completed?
  Primary school
  Some high school, but no diploma
  High school diploma (or GED)
  Some college, but no degree
  2-year college degree
  4-year college degree
  Graduate-level degree
  None of the above

• Which of the following best describes your current job level?
  Owner/Executive/C-Level
  Senior Management
  Middle Management
  Intermediate
  Entry Level
  Other
  Not applicable

• What is the size of the organization where you are employed?
  1-10
  11-50
  51-200
201-500
500-1,000
1,001-5,000
5,001-10,000
10,000+
Not applicable

- Does your employer impose any information security requirements? For example policies and instructions on installing and updating software, sharing of information or the use of passwords.
  Yes
  No
  I don’t know
  Not applicable

- How many hours per week do you use a computer at work?
  I don’t use a computer at work / Not applicable
  1-5
  6-10
  11-15
  16-20
  21-25
  More than 25

- In which sector do you work?
  public sector (e.g., government, social security, agency, military, public school, public hospital)
  nonprofit sector (e.g., foundation, volunteer organization, philanthropic organization, charity)
  private sector (e.g., industry company, service firm)
  I am currently not employed
Overview of questionnaire statements

In addition to the from the HAIS-Q statements shown in appendix A the following statements are used in
the questionnaire to measure the organizational climate factors. The measure the factors mainly statements
from literature are used. Small adaptations were made to the statements to make them suitable for this study.

<table>
<thead>
<tr>
<th>Label</th>
<th>Statement</th>
<th>Derived from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open4</td>
<td>In my organization we seldom talk about information security errors</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Open5</td>
<td>In my organization we always discuss information security issues when such issues come up</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Open6</td>
<td>In my organization we can talk freely and openly about information security risks</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Open1</td>
<td>In my organization open communication about information security is encouraged*</td>
<td>Hofmann and Morgeson (1999)</td>
</tr>
<tr>
<td>Open2</td>
<td>I feel comfortable discussing information security issues with colleagues*</td>
<td>Hofmann and Morgeson (1999)</td>
</tr>
<tr>
<td>Open3</td>
<td>I try to avoid talking about information security issues with colleagues*</td>
<td>Hofmann and Morgeson (1999)</td>
</tr>
<tr>
<td>Open7</td>
<td>I try to avoid talking about information security issues with colleagues*</td>
<td>Hofmann and Morgeson (1999)</td>
</tr>
<tr>
<td>Task1</td>
<td>Management encourages employees here to work in accordance with information security rules - even when the work schedule is tight*</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Task2</td>
<td>Management places information security before production*</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Task3</td>
<td>Management accepts employees here taking risks when the work schedule is tight*</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Task4</td>
<td>Management suggests to skip information security rules and procedures when the work schedule is tight*</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Task5</td>
<td>Management places production before information security*</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Educ1</td>
<td>My organization provides training to help employees improve their awareness of information security issues</td>
<td>D’Arcy et al. (2009)</td>
</tr>
<tr>
<td>Educ2</td>
<td>My organization educates employees on their information security responsibilities</td>
<td>D’Arcy et al. (2009)</td>
</tr>
<tr>
<td>Educ3</td>
<td>Business communications (e.g. notices, posters, newsletters) are used to promote security awareness multiple times per year</td>
<td>Herath and Rao (2009b)</td>
</tr>
<tr>
<td>Educ4</td>
<td>The information security requirements (e.g. policies) of my company are clear, understandable and readily available</td>
<td>Chan et al. (2005); Herath and Rao (2009b)</td>
</tr>
<tr>
<td>Invo1</td>
<td>In my organization employees’ suggestions regarding information security are never considered</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Invo2</td>
<td>In my organization employees are never asked for their opinions before making decisions regarding information security</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Invo3</td>
<td>In my organization employees are involved in decisions regarding information security</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Invo4</td>
<td>Information security suggestions of employees from all function levels are taken seriously</td>
<td>Kines et al. (2011)</td>
</tr>
<tr>
<td>Mngt1</td>
<td>Senior management considers information management an important organizational priority</td>
<td>Knapp et al. (2006)</td>
</tr>
<tr>
<td>Mngt2</td>
<td>Senior management is interested in information security issues</td>
<td>Knapp et al. (2006)</td>
</tr>
<tr>
<td>Mngt3</td>
<td>Senior management’s words and actions demonstrate that information management is a priority</td>
<td>Knapp et al. (2006)</td>
</tr>
<tr>
<td>Mngt4</td>
<td>Visible support for information management goals by senior management is obvious</td>
<td>Knapp et al. (2006)</td>
</tr>
<tr>
<td>Mngt5</td>
<td>Senior management actively champions information security goals</td>
<td>D’Arcy and Greene (2014)</td>
</tr>
<tr>
<td>Mngt6</td>
<td>Top managers adhere to information security policies themselves</td>
<td>D’Arcy and Greene (2014)</td>
</tr>
<tr>
<td>Workimp1</td>
<td>Complying with the company’ information security requirements holds me back from doing my actual work</td>
<td>Bulgurcu et al. (2010)</td>
</tr>
<tr>
<td>Workimp2</td>
<td>Complying with the company’ information security requirements slows down my response time to my colleagues, customers, managers etc.</td>
<td>Bulgurcu et al. (2010)</td>
</tr>
<tr>
<td>Workimp3</td>
<td>Complying with the company’ information security requirements hinders my productivity at work</td>
<td>Bulgurcu et al. (2010)</td>
</tr>
<tr>
<td>Workimp4</td>
<td>My efficiency at work is not affected by complying with the company’ information security requirements</td>
<td>Bulgurcu et al. (2010)</td>
</tr>
</tbody>
</table>

All statements can be answered on a 5-point Likert scale from strongly disagree to strongly agree

* Dropped from the final model based on the results of the factor analysis
Attention and consistency checks

An overview of the number of failed attention and consistency checks, including the statements is shown in table G.1. Note that some respondents failed multiple checks, therefore the combined failed responses is lower than the sum of the separate failed responses.

Table G.1: Attention and consistency checks included in the questionnaire

<table>
<thead>
<tr>
<th>Check</th>
<th>Statement</th>
<th>Approved responses</th>
<th>Incorrect responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attention check 1</td>
<td>Select disagree for this statement</td>
<td>disagree</td>
<td>3</td>
</tr>
<tr>
<td>Attention check 2</td>
<td>Usually, the color of grass is purple, red or blue.</td>
<td>strongly disagree, disagree</td>
<td>1</td>
</tr>
<tr>
<td>Attention check 3</td>
<td>For this statement, the correct answer is the opposite of agree.</td>
<td>disagree</td>
<td>3</td>
</tr>
<tr>
<td>Attention check 4</td>
<td>I have never used a computer for my work</td>
<td>strongly disagree, disagree</td>
<td>4</td>
</tr>
<tr>
<td>Attention check 5</td>
<td>A mouse is larger than a cat</td>
<td>strongly disagree, disagree</td>
<td>5</td>
</tr>
<tr>
<td>Consistency check 1</td>
<td>Repeat: I assess the safety of websites before entering information.</td>
<td>absolute deviation &lt;2</td>
<td>9</td>
</tr>
<tr>
<td>Consistency check 2</td>
<td>Repeat: I must not ignore poor security behavior by my colleagues.</td>
<td>absolute deviation &lt;2</td>
<td>11</td>
</tr>
<tr>
<td>All attention checks combined</td>
<td></td>
<td></td>
<td>16</td>
</tr>
<tr>
<td>All consistency checks combined</td>
<td></td>
<td></td>
<td>19</td>
</tr>
<tr>
<td>All checks combined</td>
<td></td>
<td></td>
<td>21</td>
</tr>
</tbody>
</table>
Exploitative Factor Analysis

**EFA with 6 factors**

Result of the exploitative factor analysis with the task items. A maximum likelihood extraction combined with a Promax rotation was used. All scores below .30 are not shown.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Factor 1</th>
<th>Factor 2</th>
<th>Factor 3</th>
<th>Factor 4</th>
<th>Factor 5</th>
<th>Factor 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educ1</td>
<td></td>
<td></td>
<td>0.765</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educ2</td>
<td></td>
<td></td>
<td>0.804</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educ3</td>
<td></td>
<td></td>
<td>0.749</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educ4</td>
<td></td>
<td></td>
<td>0.486</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invo1</td>
<td></td>
<td>0.662</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invo2</td>
<td></td>
<td>0.952</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invo3</td>
<td></td>
<td>0.832</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invo4</td>
<td></td>
<td>0.650</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt1</td>
<td>0.753</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt2</td>
<td>0.940</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt3</td>
<td>0.828</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt4</td>
<td>0.736</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt5</td>
<td>0.805</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt6</td>
<td>0.577</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open4</td>
<td></td>
<td></td>
<td></td>
<td>0.666</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open5</td>
<td></td>
<td></td>
<td></td>
<td>0.780</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open6</td>
<td></td>
<td></td>
<td></td>
<td>0.784</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.717</td>
<td></td>
</tr>
<tr>
<td>Task4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.583</td>
<td></td>
</tr>
<tr>
<td>Task5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.444</td>
<td></td>
</tr>
<tr>
<td>Workimp1</td>
<td>0.599</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workimp2</td>
<td>0.957</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workimp3</td>
<td>0.872</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workimp4</td>
<td>0.820</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**EFA with 5 factors**

Result of the exploitative factor analysis without the task items. A maximum likelihood extraction combined with a Promax rotation was used. All scores below .30 are not shown.

Table H.2: EFA with 5 factors

<table>
<thead>
<tr>
<th>Statement</th>
<th>Factor 1</th>
<th>Factor 2</th>
<th>Factor 3</th>
<th>Factor 4</th>
<th>Factor 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Educ1</td>
<td>0.782</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educ2</td>
<td>0.810</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educ3</td>
<td>0.748</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educ4</td>
<td>0.506</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invo1</td>
<td></td>
<td>0.655</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invo2</td>
<td></td>
<td>0.949</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invo3</td>
<td></td>
<td>0.833</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Invo4</td>
<td></td>
<td>0.625</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt1</td>
<td>0.791</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt2</td>
<td>0.933</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt3</td>
<td>0.863</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt4</td>
<td>0.665</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt5</td>
<td>0.786</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mngt6</td>
<td>0.655</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open4</td>
<td></td>
<td></td>
<td></td>
<td>0.671</td>
<td></td>
</tr>
<tr>
<td>Open5</td>
<td></td>
<td></td>
<td></td>
<td>0.771</td>
<td></td>
</tr>
<tr>
<td>Open6</td>
<td></td>
<td></td>
<td></td>
<td>0.801</td>
<td></td>
</tr>
<tr>
<td>Workimp1</td>
<td>0.681</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workimp2</td>
<td>0.917</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workimp3</td>
<td>0.892</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workimp4</td>
<td>0.805</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Table H.3: Reliability of all organizational climate factor based on Cronbach's alpha

<table>
<thead>
<tr>
<th>Factor</th>
<th>Cronbach's alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>Education and communication</td>
<td>0.825</td>
</tr>
<tr>
<td>Involvement</td>
<td>0.860</td>
</tr>
<tr>
<td>Management commitment</td>
<td>0.907</td>
</tr>
<tr>
<td>Openness on IS</td>
<td>0.795</td>
</tr>
<tr>
<td>Workimpediment</td>
<td>0.889</td>
</tr>
<tr>
<td>Task orientation</td>
<td>0.676</td>
</tr>
</tbody>
</table>
Figure I.1 shown the model as estimated in AMOS. In this model, like in the study by Molin (2005), the summated scales are used. Thereby, the procedure as outlined by Jöreskog and Sörbom (2001) is followed. The random error of associated summated scale is set to the variance multiplied by 1 minus the reliability (Cronbach's alpha). The calculated error variances is shown in table I.1. These are used for the specification of the model, as shown in figure I.2.

![Figure I.1: Model as estimated in AMOS](image)

### Table I.1: Calculated error variance of summated scales

<table>
<thead>
<tr>
<th>Factor</th>
<th>Number of statements</th>
<th>Variance</th>
<th>Cronbach's alpha</th>
<th>Error variance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sopen</td>
<td>3</td>
<td>6,239</td>
<td>0,795</td>
<td>1,279</td>
</tr>
<tr>
<td>Seduc</td>
<td>4</td>
<td>6,841</td>
<td>0,825</td>
<td>1,197</td>
</tr>
<tr>
<td>Sworkimp</td>
<td>4</td>
<td>11,270</td>
<td>0,889</td>
<td>1,251</td>
</tr>
<tr>
<td>Sinvo</td>
<td>4</td>
<td>11,333</td>
<td>0,860</td>
<td>1,587</td>
</tr>
<tr>
<td>Smngt</td>
<td>6</td>
<td>14,254</td>
<td>0,907</td>
<td>1,326</td>
</tr>
<tr>
<td>Satitude</td>
<td>21</td>
<td>59,628</td>
<td>0,881</td>
<td>7,096</td>
</tr>
<tr>
<td>Sbehavior</td>
<td>21</td>
<td>62,858</td>
<td>0,862</td>
<td>8,674</td>
</tr>
<tr>
<td>Sknowledge</td>
<td>21</td>
<td>80,426</td>
<td>0,821</td>
<td>14,396</td>
</tr>
</tbody>
</table>
Figure I.2: Model as specified in AMOS