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

J. Timmermans
Faculty of Technology, Policy, and Management, Delft University of Technology

Abstract

Employees are often referred to as the main cause of cyber security incidents in organizations. These incidents can lead to huge company risks and enormous losses. Therefore insight in how organizations can improve employees' information security behavior is important, realizing that technical measures alone cannot reduce all security risks. This paper examines the relation between organizational information security climate factors and employees information security behavior. The organizational climate concerns the tangible factors which relate to the atmosphere and work practices in the organization, like management support and openness on information security incidents. After a literature review and semi-structured interviews with information security experts, organizational factors are identified which influence information security behavior. A conceptual model is developed and quantitatively tested, with data collected via a survey under 289 employees. Structural equation modeling is used to analyze these data. The organizational factors education and communication, managerial commitment, employee involvement, work impediment and openness on information security, are confirmed to have a significant relation with the information security behavior of employees. Organizations can use these insights to strengthen their information security climate in order to improve employees' information security behavior.

Keywords: Information security, Organizational climate, Employee behavior, HAIS-Q, SEM

1. Introduction

Organizations are frequently facing cyber security breaches, which are increasing in number, complexity and severity. 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 [1]. Technical measures to reduce security risks are in themselves not always sufficient without effort of employees [2, 3]. For example, a phishing attack is sometimes not detected by a spam filter. An analysis from Verizon [4] 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 causing 18 to 35% of the data breaches in 2018 [5]. As stated by Cram, Proudfoot, and D'Arcy [6, p. 605] "security issues originating from employee actions remain a persistent problem for today's organizations".

Realizing the importance of human behavior 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 growing, but sometimes conflicting insights in what drives the behavior of employees. Organizations try to improve employee behavior by implementing information security policies, in which they define the standards, rules, boundaries and responsibilities of employees [2, 7]. Additionally, employees receive training to increase their information security knowledge and understanding of these policies. Research also suggests that in practice many variables, under which the organizational culture and climate, might influence employee behavior. Organizational factors, such as managerial commitment and peer behavior are suggested to have a very important influence on the behavior of employees in general [8, 9].
In the literature several various definitions of organizational climate can be found. In this article the following definition is used: "the organizational climate entails "the [by employees] shared perceptions of organizational policies, practices, and procedures, both formal and informal" [10, p. 22].

The relation of organizational factors on employees' information security (IS) behavior has been studied by several scholars, a few of them focusing on organizational IS climate. The organizational IS climate is not researched extensively, and often underlaying elements of climate, such as employee involvement and openness on information security issues, are not further specified in quantitative research. Research has a limited dept and is often descriptive, philosophical or theoretical, and results cannot easily be translated to practice [11].

To gain insight in factors and mechanisms related to employee IS behavior, a combination of qualitative and quantitative methods is used.
First a review of organizational climate, safety climate and information security literature is performed, to identify possible factors and underlying mechanisms that influence employee information security behavior. To capture insights from practice, semi-structured interviews with 8 information security experts were conducted. These combined findings from literature and practice form the basis of the conceptual model of this research and its underlying hypotheses. Subsequently a quantitative study is performed on 289 survey responses. 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.
Organizations can use the insights as input for their information security approach and activities to improve employee security behavior, possible contributing to a stronger information security climate in organizations.

In the following section of this paper the outcome of the literature review is described. This is followed by a section with the insights from the semi-structured interviews and the presentation of the conceptual model. Thereafter the research methodology, data collection and model estimation procedures are explained. Finally, the estimated model is presented and discussed, together with the limitations of the study and suggestions for future work.

2. Related work

The organizational climate has proven to have a close relation to employee behavior in general. Therefore, 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. Next to this, theories used to explain employees' information security behavior are explored and methods to measure this behavior are reviewed. Based on these insights, the most suitable theoretical basis and measurement model for further analysis are chosen. Additionally, literature of the research on organizational factors and employee information security behavior is reviewed, resulting in an overview of organizational processes and factors, including their expected influencing effect on employee behavior.

All elements of the literature review are combined to acquire an overview of what influences the IS behavior of employees in an organizational context. These outcomes are used as basis for the semi-structured interviews with information security experts.

2.1. Organizational and safety climate

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 and procedures and how employees experiences management initiatives in their daily work, bringing insights in how managers can influence behavior [12]. A strong relationship between the organizational climate and employees' job attitude and behavior is confirmed in many studies [13, 14].

Specific research on the influence of the safety climate on employees' behavior reveals more detailed information. Griffin and Neal [15] 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. This growing evidence of safety climate as a predictor for safety behavior is also mentioned by Kines et al. [16], who developed and validated a safety climate questionnaire. The safety climate/culture model from Cooper [17] has proven to be of practical support for organizations to improve their safety environment and optimize accident prevention [13, 17, 18, 19]. Based on the review of organizational and safety research, several characteristics of the climate of organizations are identified to influence safety 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, e.g. priority, empowerment and commitment
- Training and communication, e.g. training programs, procedures, rules and trust
- Risk and work pressure related factors, e.g. work pressure, rewarding safe conduct
- Social environment and employee related factors, e.g. employee involvement en well-being

2.2. Measuring employee behavior

Within the field of information security, many theories are used to explain the behavior of employees. Lebek, Uffen, et al. [20] identified 54 different theories, from which the main theories are the Theory of Planned behavior, the General Deterrence Theory, the Protection Motivation Theory and the Technology Acceptance Model. All these theories are adopting different factors to explain the behavioral intention or actual behavior of employees. This is resulting in many different factors which could influence security awareness and behavior. Another model to explain the information security behavior of employees is the knowledge, attitude and behavior (KAB) model [21, 22]. The KAB-model, which originates from the social psychology, is extensively used in healthcare studies to analyze the link between knowledge and behavior [23]. 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 [23, 24, 25, 26]. Therefore, this model is suitable to investigate how environmental factors can

influence the knowledge, attitude and behavior of employees.

Several scholars have found inconsistent results on factors that could influence employees' IS behavior [20, 27, 28]. In line with these suggestions, Cram et al. [6] 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 is suggested to play a role. Thereby they suggest, like many other scholars, to measure security behavior on a more detailed level [6, 20, 27]. 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" [2, p. 536]. The many different interpretations of those questions are suggested as possible cause of conflicting results [27].
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. [27] developed the human aspects of information security questionnaire (HAIS-Q), based on the KAB-model, to measure security behavior on a more detailed level. This questionnaire is judged to be most suitable for this study and contains questions on 7 specific focus areas: password management, email use, internet use, social media use, mobile devices, information handling, and incident reporting. Each of these focus areas contain knowledge, attitude and behavior statements which can be answered on a 5-point Likert scale, which ranges from strongly disagree to strongly agree. The combination of these responses can be used to measure the overall IS knowledge, attitude and behavior of the respondents.

2.3. Organizational climate and employee information security behavior

An extensive review of information security research, including journal articles, conference papers and books, is performed to identify the relation of organizational factors and processes on the information security behavior of employees. This results in a broad insight, although results of studies are not always comparable, due to different study designs and theories used and various interpretations of behavior. Taken this limitation into account, some interesting insights were acquired.

Management
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 [29, 30, 31, 32].The influence of management participation and transformational leader ship is however ambiguous [20, 33, 34, 35, 36].

Knowledge and awareness improvement measures
In most studies information security provisioning has a direct positive effect on IS behavior or indirect via subjective norms [37, 38, 39]. No supporting evidence was reported on the relation between ISP quality and IS behavior [36, 40]. In (almost) all analyzed studies internal communication and training have a positive relation with awareness, self-efficacy and intended security behavior [29, 41, 42, 43, 44].

Work impediment and employee involvement
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 [2, 45, 46]. 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.

Summarized, management plays an important role, although research is contradicting. This in contrary to training and communication, which generally shows a positive effect on the behavior of employees. Work impediment has significant negative impact, whilst the involvement of employees has a positive effect on their intentional behavior.

3. Expert interviews

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 literature review can be enriched with missing factors or mechanisms from practice. Furthermore, the input from the interviews is used to determine which of the identified organizational security climate related factors should be included in the research model.

3.1. Interview methodology

In total 8 Dutch information security consultants and company experts were interviewed to get a broad picture based on an inside and outside view. 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.

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.

Table 1: Overview interviewed experts

Expert	Position	Company focus	Industry
1	CISO	International	Financial
2	GISO	National	Insurance
3	Senior awareness officer	International	Commercial
4	CISO	International	Consultancy
5	CISO	National	Public
6	Senior awareness officer	International	Consultancy
7	IS consultant	International	Consultancy
8	IS consultant	International	Consultancy

Interview results

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 [47]. The qualitative data analysis software tool MAXQDA[1] is used to assign codes to citations and to bundle the classified information from all interviews. During the coding process all interview data was handled anonymously 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 [48]. Also, some individual quotes are selected for clarification and to ground the choice for new coding categories.

The interviews with the 8 information security experts provided valuable information and insights from practice. Although most of the findings from literature were confirmed, also factors were identified in which literature was not linked with the experiences from the experts. Additionally, nuance was added to 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. Embedding information security in all business activities and taking shared responsibility, and not only something the IT department must care about, also contributes to compliant behavior. Providing regular training, enriched with practical and actual topics contributes to better understanding.

The factors and processes that influence employees' IS behavior as identified via the interviews with experts in practice, summarized in table 2, form an essential contribution to the choices made for the construction of a conceptual model.

4. Research model and 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.

[1] A software package for qualitative research, see maxqda.com

Table 2: Overview of influential factors and processes identified in practice

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

4.1. Research model

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. The knowledge-attitude-behavior model with the relations as suggested by Chaffee and Roser [24] 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 (HAISQ) [27]. This questionnaire, which is validated in multiple studies with in total 1681 participants, allows for the measurement of behavior on specific focus areas [27, 43, 49, 50, 51]. The combination of the measurement of specific IS behavior and the limited amount of predictors in the underlying model, makes the HAIS-Q a suitable instrument for this research.

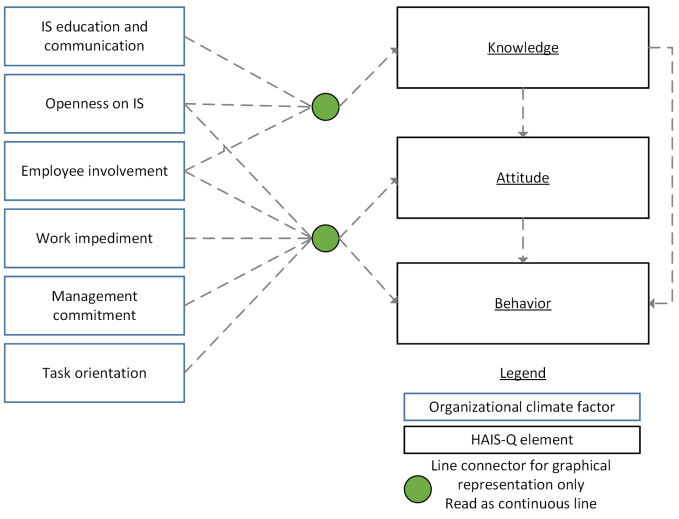

Figure 1: Research model

4.2. Hypothesis

As mentioned in literature and during expert interviews, many factors which can influence employee IS behavior.

However, due to restrictions in resources and parsimony, only a selected number of variables is included in further analysis. The selection of these factors is mainly 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.

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 a higher awareness and attitude, which in turn, will encourage compliant information security behavior [2, 33, 52]. 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.

H1: Information security education and communication is, via improved knowledge, positively related to employees' behavior

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 [16, 53].

H2: Openness on information security is, via improved knowledge and attitude, positively related to employees' behavior

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 [3, 54]. A positive relation with attitude and behavior is also mentioned in both safety climate research [18, 53] and information security research [39]. Experts express 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.

H3: Employee involvement is, via improved knowledge and attitude, positively related to employees' behavior

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 [2, 46, 55]. Experts named the impediment of IS measures on the daily work as one of the main reasons for non-complaint behavior.

H4: Work impediment is negatively related to employees' attitude and 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 [29, 32]. Also safety climate research confirms the important role of management in the employees' behavior [16, 53].

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.

H5: Perceived management commitment is positively related to employees' attitude and behavior

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 [2, 56].

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.

H6: Task orientation is positively relates to employees' attitude and behavior

5. Methodology

In this section 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 IS climate is described, followed by the explanation of the data collection approach. Next, the methodology for analyzing the collected data is discussed.

5.1. Data collection

Measuring employee 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 [20]. Additionally, many companies are reluctant to share IS related information, due to its sensitive nature [57]. A strong relation between behavioral intention and the actual behavior is reported in the literature [20]. Therefore, the self-reported behavioral intention via a questionnaire is used.

Measuring organizational IS 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 [58, 59, 60]. 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. [2] to measure work impediment. The questionnaire is distributed via Survey monkey, 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 process many responses. To reduce social desirability bias, all questionnaire responses are processed anonymously.

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. [27]. 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.

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.

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 explanation of definitions in introduction was improved by proving examples, some statements were too ambiguous and therefore replaced. Additionally, cosmetic changes to the layout were processed to improve the user experience.

Population

The target population for the survey are employees which have to deal with in information security in their work. Working on information security climate is often seen as stage of a IS maturity which comes after setting information security requirements [61]. When a company has no information security guidelines, requirements, rules or procedures whatsoever, then the company is too 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. [52] and Hofstede [62], the quantitative part of the research is targeted to US employees only. These considerations result in respondent requirements working in a company with more than 50 employees and where the employer poses any form of information security requirements. Additionally, the respondent must use a computer at work for at least 10 hours per week, and has to be working in the US.

The respondents are recruited via the crowd-sourcing platform Amazon Mechanical Turk (AMT). 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 [63, 64]. To make sure that the workers from AMT meet the before-mentioned requirements and to safeguard the response quality, 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 310 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 a dataset with 289 usable responses.

5.2. Data analysis

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 [63, 64]. 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 modeling choices and assumptions are made.

The behavior of employees is a result of a whole complex of interactions between different IS climate related factors and more generic factors (i.e. knowledge, attitude and behavior). The causal model 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.

Measurement model

A factor analysis is used to analyze the measurement model.

Table 3: Criteria for factor analysis, based on Hair et al. [63]

Criteria	Threshold
Measure of Sampling Adequacy	≥ 0.50
Bartlett's Test of Sphericity	<0.05
Communalities	>0.25
Factor loadings	>0.50
Cronbach's alpha	>0.70

This can be done via an exploratory factor analysis (EFA) and / or a confirmatory factor analysis (CFA) [65]. 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 suggests 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 [66] and Worthington and Whittaker [67] 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. 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 3 are used as thresholds for the EFA.

Causal model

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 [68], 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 by Jöreskog and Sörbom [69]. Thereby, the measurement error of associated summated scale is set to the variance multiplied by 1 minus the reliability (Cronbach's alpha).

6. Results

The survey was distributed via Amazon mechanical Turk to 723 selected workers. 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%.

Before analyzing the collected data with SEM it is important to gain insight in the representativeness of the sample for the population. Due to the selection of respondents on specific requirements (e.g. company size & computer hours), 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 a an accurate comparison between the sample and the population. For an indication of the representativeness of the sample a comparison is made with data of the U.S. Bureau of Labor Statistics on the 2017 employed U.S. population.
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. 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.

6.1. 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 [70], it is important for the interpretation of the results that statements load only on 1 factor. This is achieved via an exploratory and confirmatory factor analysis.

Exploratory factor analysis

The EFA is only performed on the organizational climate related factors, not on HAIS-Q factors The ML function is

Table 4: Validity and reliability analysis of 5 factor model

	CR	AVE	MSV	MaxR(H)	Mngt	Workim	Involv	Educ	Open
Mngt	0,912	0,635	0,531	0,928	0,797				
Workim	0,894	0,679	0,196	0,91	0,336***	0,824			
Involv	0,864	0,615	0,267	0,867	0,517***	0,442***	0,784		
Educ	0,84	0,569	0,531	0,852	0,728***	0,304***	0,426***	0,754	
Open	0,797	0,568	0,161	0,8	0,385***	0,171*	0,304***	0,401***	0,753

* p ¡ 0.050, ** p ¡ 0.010, *** p ¡ 0.001

Table 5: Model fit of CFA

Measure	Estimate	Threshold	Interpretation
CMIN	344,742		
DF	179		
CMIN/DF	1,926	Between 1 and 3	Excellent
CFI	0,952	>0.95	Excellent
SRMR	0,058	<0.08	Excellent
RMSEA	0,057	<0.06	Excellent
PClose	0,109	>0.05	Excellent

used for the EFA fitting procedure and for the rotation ProMax 4. The Bartlett's test shows that is possible to reduce the data. Also, the Kaiser-Meyer-OlkinMeasure of Sampling Adequacy test is higher than the threshold of ≥ 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. 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. All other factors have high loadings and a Cronbach's alpha > 0.70.

As the fitting of task is quite close to the cut-off values, this factor was included in a CFA model. However, 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.

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. Although the model fit of the 6 factor model is acceptable, 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. The values of table 4 shows that there are no validity concerns for this measurement model. Additionally, the model fit is also excellent as visible in table 5. Therefore, this 5 factor model is used for further analysis.

HAIS questionnaire

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.

The scores on knowledge, attitude and behavior can be measured by combining the statements of all focus areas. Thereby, 21 items are used to measure each construct. 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.

The HAIS questionnaire is already validated in multiple studies (see [27]). Therefore, no factor analysis is done on the HAIS-Q statements. The measurement reliability of the constructs is comparable with other studies.

Model-fit

The factors and their measurement error identified in the factor analysis are combined with the expected relations between the factors. These relations are based on the literature review and expert interviews.

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

Although the original model shows a good fit on some of measures, the model fit value of the rootmean 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.

To increase the model fit, some improvements were made. 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

Table 6: Model-fit of revised version SEM model

Measure	Estimate	Threshold	Interpretation
CMIN	25,211		
DF	13		
CMIN/DF	1,939	Between 1 and 3	Excellent
CFI	0,989	>0.95	Excellent
SRMR	0,035	<0.08	Excellent
RMSEA	0,057	<0.06	Excellent
PClose	0,326	>0.05	Excellent

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 [44, 52, 29, 16, 53, 3].

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. [46], 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. [2] 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 2. As shown in table 6, this revised model has an excellent model fit.

Signification relations

In figure 2 the path coefficients and portion explained variance of the revised model are shown. All relation in the figure are significant.

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 7 the standardized total of the direct and indirect effects are presented.

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 the HAIS-Q subsection, a higher score on these items stands for more IS knowledge, a better attitude towards IS and a more secure IS behavior.

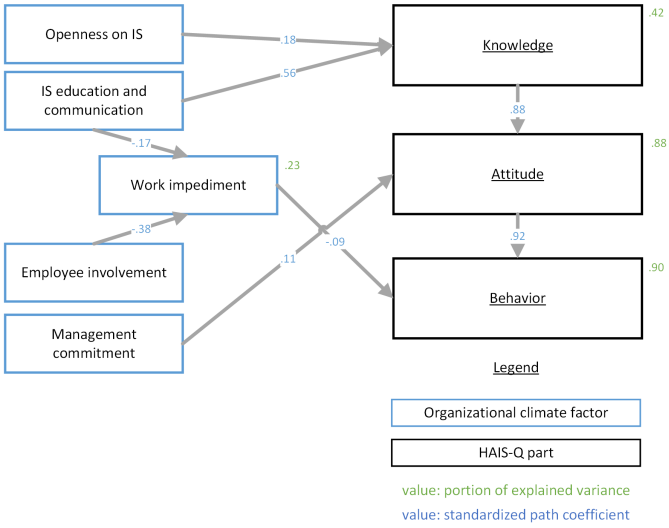

Figure 2: Estimated revised model with standardized effects

Within figure 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 1, turns out to be not significant when added to the revised model (see figure 2). This in contrary to the findings reported by Parsons, McCormac, Butavicius, et al. [43] 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, They 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 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. [43], 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

Table 7: Total effect from factors in the model on attitude, behavior, knowledge and work impediment

To	Total effect from: Mngt	Educ	Invo	Open	Knowledge	Workimp	Attitude
Knowledge	0	0,555	0	0,182	0	0	0
Workimp	0	-0,165	-0,375	0	0	0	0
Attitude	0,105	0,49	0	0,161	0,883	0	0
Behavior	0,097	0,466	0,033	0,148	0,813	-0,088	0,921

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.

The relations with the organizational climate factors are discussed in the next section.

7. Conclusion and discussion

This section provides the conclusion of the research on the influence of organizational climate factors on the behavior of employees. Based on the SEM-based analysis of the final model, the hypotheses, are discussed. Finally, the limitations of this study are discussed and recommendations are provided.

7.1. Main findings

In this subsection 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 a 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.

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.

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. 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 study by Boss et al. [71] 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 [42]. In a study by Cuganesan et al. [38] 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 [42] 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 [44], education and communication had, via ISA and attitude, a significant effect on the intention. Similarly, Herath and Rao [45] 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 (-0.17) 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. [2] to have a significant negative relation (-0.24) with work impediment. Additionally, the safety climate studies from Neal et al. [53] and Neal and Griffin [72] confirm the effect of education on work impediment.

In summary, the findings fromthe expert interviews, the safety climate literature and the study by Bulgurcu et al. [2] are in line with the findings of this study.

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 (0.18). 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 [53, 64]. 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 [16, 53].

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.

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 [3] 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 [3] 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.

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. [2] and Vance et al. [46], employees perceives measures to comply with the information security policy often as a barrier to productivity. In the studies by Bulgurcu et al. [2], Guo et al. [73], Herath and Rao [45] and Vance et al. [46] work impediment has a significant negative relation with the intention towards secure IS behavior. An exemption is the study by Ifinedo [74] 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 [54]. 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.

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.[38] 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 Hu et al. [33], 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 [32, 29, 35]. Additionally, the importance of management commitment for employee's behavior, is mentioned in the safety climate literature [16, 53].

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 6th 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

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, more research is required to provide more solid evidence for the influence of the organizational information security climate

7.2. 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 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. 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 [20], 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 matureness 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.

7.3. 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.

Further research

For further research it would be interesting to include the measurement of real IS behavior instead of self-reported behavior to increase the reliability of the results. 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. [52], 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.

Organizations

Organizations can use the following recommendations to improve and strengthen their IS climate and thereby the employees IS 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 IS 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.

References

[1] S. M. Tisdale, Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective, Issues in Information Systems 16 (3).

[2] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, MIS Quarterly: Management Information Systems 34 (3) (2010) 523–548. doi:10.2307/25750690.

[3] J. L. Spears, H. Barki, User participation in information systems security risk management, MIS Quarterly: Management Information Systems 34 (3) (2010) 503–522.

[4] Verizon, Data breach investigations report 2017 (2017).
URL `http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/`

[5] Ponemon Institute LLC, Cost of data breach study 2018: Global overview (2018).
URL `https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf`

[6] W. A. Cram, J. G. Proudfoot, J. D'Arcy, Organizational information security policies: a review and research framework, European Journal of Information Systems 26 (6) (2017) 605–641. doi:10.1057/s41303-017-0059-9.

[7] P. B. Lowry, G. D. Moody, Proposing the control-reactance compliance model (crcm) to explain opposing motivations to comply with organisational information security policies, Information Systems Journal 25 (5) (2015) 433–463. doi:10.1111/isj.12043.

[8] L. W. Porter, G. B. McLaughlin, Leadership and the organizational context: Like the weather?, The Leadership Quarterly 17 (6) (2006) 559–576. doi:10.1016/j.leaqua.2006.10.002.

[9] B. Schneider, M. G. Ehrhart, W. H. Macey, Organizational climate and culture, Annual review of psychology 64 (1) (2013) 361–388. doi:10.1146/annurev-psych-113011-143809.

[10] A. E. Reichers, B. Schneider, Climate and culture: An evolution of constructs, in: B. Schneider (Ed.), Organizational climate and culture, Jossey - Bass Publishers, San Francisco - Oxford, 1990, Ch. 1, pp. 5–39.

[11] Karlsson Fredrik, Åström Joachim, Karlsson Martin, Information security culture – state-of-the-art review between 2000 and 2013, Information and Computer Security 23 (3) (2015) 246–285. doi:10.1108/ICS-05-2014-0033.

[12] D. R. Denison, What is the difference between organizational culture and organizational climate? a native's point of view on a decade of paradigm wars, Academy of Management Review 21 (3) (1996) 619–654. doi:10.5465/amr.1996.9702100310.

[13] M. G. Ehrhart, B. Schneider, W. H. Macey, Organizational climate and culture: an introduction to theory, research, and practice, Routledge/Taylor & Francis Group, New York, NY, US, 2014.

[14] M. Kuenzi, M. Schminke, Assembling fragments into a lens: A review, critique, and proposed research agenda for the organizational work climate literature, Journal of Management 35 (3) (2009) 634–717. doi:10.1177/0149206308330559.

[15] M. A. Griffin, A. Neal, Perceptions of safety at work: A framework for linking safety climate to safety performance, knowledge, and motivation, Journal of Occupational Health Psychology 5 (3) (2000) 347–358. doi:10.1037/1076-8998.5.3.347.

[16] P. Kines, J. Lappalainen, K. L. Mikkelsen, E. Olsen, A. Pousette, J. Tharaldsen, K. Tómasson, M. Törner, Nordic safety climate questionnaire (nosacq-50): A new tool for diagnosing occupational safety climate, International Journal of Industrial Ergonomics 41 (6) (2011) 634–646. doi:10.1016/j.ergon.2011.08.004.

[17] M. D. Cooper, Towards a model of safety culture, Safety Science 36 (2) (2000) 111–136. doi:10.1016/S0925-7535(00)00035-7.

[18] M. D. Cooper, Navigating the Safety Culture Construct: A Review of the Evidence, B-Safe Management Solutions Inc., 2016.

[19] R. Flin, C. Burns, K. Mearns, S. Yule, E. M. Robertson, Measuring safety climate in health care, BMJ Quality & Safety 15 (2) (2006) 109–115. doi:10.1136/qshc.2005.014761.

[20] B. Lebek, J. Uffen, M. Neumann, B. Hohler, M. H. Breitner, Information security awareness and behavior: A theory-based literature review, Management Research Review 37 (12) (2014) 1049–1092. doi:10.1108/MRR-04-2013-0085.

[21] B. Khan, K. S. Alghathbar, S. I. Nabi, M. K. Khan, Effectiveness of information security awareness methods based on psychological theories, African Journal of Business Management 5 (26) (2011) 10862–10868. doi:10.5897/AJBM11.067.

[22] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, C. Jerram, A study of information security awareness in australian government organisations, Information Management and Computer Security 22 (4) (2014) 334–345. doi:10.1108/IMCS-10-2013-0078.

[23] T. Baranowski, K. W. Cullen, T. Nicklas, D. Thompson, J. Baranowski, Are current health behavioral change models helpful in guiding prevention of weight gain efforts?, Obesity Research 11 (S10) (2003) 23S–43S. doi:10.1038/oby.2003.222.

[24] S. H. Chaffee, C. Roser, Involvement and the consistency of knowledge, attitudes, and behaviors, Communication Research 13 (3) (1986) 373–399. doi:10.1177/009365086013003006.

[25] L. R. Fabrigar, R. E. Petty, S. M. Smith, S. L. Crites Jr., Understanding knowledge effects on attitude-behavior consistency: The role of relevance, complexity, and amount of knowledge, Journal of Personality and Social Psychology 90 (4) (2006) 556–577. doi:10.1037/0022-3514.90.4.556.

[26] M. Fishbein, I. Ajzen, Belief, Attitude, Intention and Behavior, Addison-Wesley, Reading, 1975.

[27] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, T. Zwaans, The human aspects of information security questionnaire (hais-q): Two further validation studies, Computers and Security 66 (2017) 40–51. doi:10.1016/j.cose.2017.01.004.

[28] M. Siponen, A. Vance, Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations, European Journal of Information Systems 23 (3) (2014) 289–305. doi:10.1057/ejis.2012.59.

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

[30] K. J. Knapp, T. E. Marshall, R. K. Rainer Jr., F. N. Ford, Information security: Management's effect on culture and policy, Information Management and Computer Security 14 (1) (2006) 24–36. doi:10.1108/09685220610648355.

[31] M. Warkentin, A. C. Johnston, J. Shropshire, The influence of the informal social learning environment on information privacy policy compliance efficacy and intention, European Journal of Information Systems 20 (3) (2011) 267–284. doi:10.1057/ejis.2010.72.

[32] A. AlKalbani, H. Deng, B. Kam, Organisational security culture and information security compliance for e-government development: The moderating effect of social pressure., in: Pacific Asia Conference on Information Systems, 2015.

[33] Q. Hu, T. Dinev, P. Hart, D. Cooke, Managing employee compliance with information security policies: The critical role of top management and organizational culture, Decision Sciences 43 (4) (2012) 615–660. doi:10.1111/j.1540-5915.2012.00361.x.

[34] W. Rocha Flores, M. Ekstedt, Shaping intention to resist social engineering through transformational leadership, information security culture and awareness, Computers and Security 59 (2016) 26–44. doi:10.1016/j.cose.2016.01.004.

[35] P. Puhakainen, M. Siponen, Improving employees' compliance through information systems security training: An action research study, MIS Quarterly: Management Information Systems 34 (4) (2010) 757–778. doi:10.1016/S1386-5056(98)00022-7,.

[36] P. Mayer, N. Gerber, R. McDermott, M. Volkamer, J. Vogt, Productivity vs security: Mitigating conflicting goals in organizations, Information and Computer Security 25 (2) (2017) 137–151. doi:10.1108/ICS-03-2017-0014.

[37] J. D'Arcy, A. Hovav, D. Galletta, User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach, Information Systems Research 20 (1) (2009) 79–98. doi:10.1287/isre.1070.0160.

[38] S. Cuganesan, C. Steele, A. Hart, How senior management and workplace norms influence information security attitudes and self-efficacy, Behaviour & Information Technology 37 (1) (2018) 50–65. doi:10.1080/0144929X.2017.1397193.

[39] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani,

T. Herawan, Information security conscious care behaviour formation in organizations, Computers and Security 53 (2015) 65–78. doi:10.1016/j.cose.2015.05.012.

[40] P. Ifinedo, Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition, Information and Management 51 (1) (2014) 69–79. doi:10.1016/j.im.2013.10.001.

[41] S. Bauer, E. W. Bernroider, The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring, Vol. 9190, Springer Verlag, 2015. doi:10.1007/978-3-319-20376-8_14.

[42] F. Haeussinger, J. Kranz, Information security awareness: Its antecedents and mediating effects on security compliant behavior, in: Thirty Fourth International Conference on Information Systems, 2013.

[43] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, C. Jerram, Determining employee awareness using the human aspects of information security questionnaire (hais-q), Computers and Security 42 (2014) 165–176. doi:10.1016/j.cose.2013.12.003.

[44] S. Bauer, E. Bernroider, From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization, Data Base for Advances in Information Systems 48 (3) (2017) 44–68. doi:10.1145/3130515.3130519.

[45] T. Herath, H. R. Rao, Protection motivation and deterrence: A framework for security policy compliance in organisations, European Journal of Information Systems 18 (2) (2009) 106–125. doi:10.1057/ejis.2009.6.

[46] A. Vance, M. Siponen, S. Pahnila, Motivating is security compliance: Insights from habit and protection motivation theory, Information and Management 49 (3-4) (2012) 190–198. doi:10.1016/j.im.2012.04.002.

[47] J. Saldaña, The coding manual for qualitative researchers, 3rd Edition, SAGE, 2015.

[48] C. Schmidt, The analysis of semi-structured interviews, A companion to qualitative research (2004) 253–258.

[49] A. McCormac, D. Calic, M. Butavicius, K. Parsons, T. Zwaans, M. Pattinson, A reliable measure of information security awareness and the identification of bias in responses, Australasian Journal of Information Systems 21. doi:10.3127/ajis.v21i0.1697.

[50] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, M. Pattinson, Individual differences and information security awareness, Computers in Human Behavior 69 (2017) 151–156. doi:10.1016/j.chb.2016.11.065.

[51] M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, D. Calic, Managing information security awareness at an australian bank: A comparative study, Information and Computer Security 25 (2) (2017) 181–189. doi:10.1108/ICS-03-2017-0017.

[52] L. Y. Connolly, M. Lang, J. Gathegi, D. J. Tygar, Organisational culture, procedural countermeasures, and employee security behaviour a qualitative study, Information and Computer Security 25 (2) (2017) 118–136. doi:10.1108/ICS-03-2017-0013.

[53] A. Neal, M. Griffin, P. Hart, The impact of organizational climate on safety climate and individual behavior, Safety Science 34 (1) (2000) 99–109. doi:10.1016/S0925-7535(00)00008-4.

[54] T. Sommestad, H. Karlzén, J. Hallberg, The theory of planned behavior and information security policy compliance, Journal of Computer Information Systems (2017) 1–10doi:10.1080/08874417.2017.1368421.

[55] T. Herath, H. R. Rao, Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, Decision Support Systems 47 (2) (2009) 154–165. doi:10.1016/j.dss.2009.02.005.

[56] E. Albrechtsen, A qualitative study of users' view on information security, Computers and Security 26 (4) (2007) 276–289. doi:10.1016/j.cose.2006.11.004.

[57] A. G. Kotulic, J. G. Clark, Why there aren't more information security research studies, Information and Management 41 (5) (2004) 597–607. doi:10.1016/j.im.2003.08.001.

[58] N. M. Bradburn, S. Sudman, E. Blair, W. Locander, C. Miles, E. Singer, C. Stocking, Improving interview method and questionnaire design: Response effects to threatening questions in survey research, Jossey-Bass San Francisco, 1979.

[59] A. J. Nederhof, Methods of coping with social desirability bias: A review, European Journal of Social Psychology 15 (3) (1985) 263–280. doi:10.1002/ejsp.2420150303.
URL https://onlinelibrary.wiley.com/doi/abs/10.1002/ejsp.2420150303

[60] D. L. Paulhus, Two-component models of socially desirable responding., Journal of personality and social psychology 46 (3) (1984) 598. doi:10.1037/0021-9010.84.5.754.

[61] International Organization for Standardization, ISO/IEC 21827:2008 information technology – security techniques – systems security engineering – capability maturity model (sse-cmm), Standard, Author, Geneva, CH (2008).

[62] G. H. Hofstede, Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations / Geert Hofstede, 2nd Edition, SAGE, Thousand Oaks, Calif. and London, 2001.

[63] J. Hair, W. Black, B. J. Babin, R. E. Anderson, Multivariate Data Analysis, 7th Edition, Pearson Prentice Hall, Upper Saddle River, NJ, 2010.

[64] R. B. Kline, Principles and practice of structural equation modeling, 3rd Edition, Methodology in the Social Sciences, The Guilford Press, New York and London, 2010.

[65] J. H. Kahn, Factor analysis in counseling psychology research, training, and practice: Principles, advances, and applications, The counseling psychologist 34 (5) (2006) 684–718.

[66] P. Cabrera-Nguyen, Author guidelines for reporting scale development and validation results in the journal of the society for social work and research, Journal of the Society for Social Work and Research 1 (2) (2010) 99–103.

[67] R. L. Worthington, T. A. Whittaker, Scale development research: A content analysis and recommendations for best practices, The Counseling Psychologist 34 (6) (2006) 806–838.

[68] E. Molin, Causal analysis of hydrogen acceptance, Transportation Research Record: Journal of the Transportation Research Board (1941) (2005) 115–121.

[69] K. G. Jöreskog, D. Sörbom, LISREL 8: users reference guide., Scientific Software International, Lincolnwood, IL, 2001.

[70] D. W. Gerbing, J. C. Anderson, An updated paradigm for scale development incorporating unidimensionality and its assessment, Journal of marketing research (1988) 186–192.

[71] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, R. W. Boss, If someone is watching, i'll do what i'm asked: Mandatoriness, control, and information security, European Journal of Information Systems 18 (2) (2009) 151–164. doi:10.1057/ejis.2009.8.

[72] A. Neal, M. A. Griffin, A study of the lagged relationships among safety climate, safety motivation, safety behavior, and accidents at the individual and group levels, Journal of Applied Psychology 91 (4) (2006) 946–953. doi:10.1037/0021-9010.91.4.946.

[73] K. H. Guo, Y. Yuan, N. P. Archer, C. E. Connelly, Understanding nonmalicious security violations in the workplace: A composite behavior model, Journal of Management Information Systems 28 (2) (2011) 203–236. doi:10.2753/MIS0742-1222280208.

[74] P. Ifinedo, Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory, Computers and Security 31 (1) (2012) 83–95. doi:10.1016/j.cose.2011.10.007.