TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Olga Šenberg 204806IVCM

THE ROLE OF INDIVIDUAL AND ORGANIZATIONAL FACTORS ON THE EMPLOYEES' INFORMATION SECURITY AWARENESS AND VULNERABILITY MANAGEMENT EFFICIENCY

Master Thesis

Supervisor
Kaie Maennel

Tallinn 2022

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Olga Šenberg .....
(signature)

Date: May 16, 2022

Abstract

One of the fundamental factors for successful information security management is the effective enforcement of security policies and the proper integration of "people", "processes" and "technology". When it comes to the question of "people", it is important to consider the potential impact of individual differences on vulnerability management efficiency and employees' security perception.

The main research question is to study individual differences and determine if there is any correlation between individuals' Information Security Awareness (ISA), individual difference variables, and vulnerability management efficiency. Understanding the variability between individuals is essential to preventing and reducing information security incidents as a result of human factors. According to a joint study by scientists from Harvard, Stanford, and the Carnegie Endowment, 85% of job success depends on the soft skills of employees [1]. Soft skills indicate an individual's ability to work and communicate with others, build relationships, solve problems, and grow within a company. But if hard skills can be learned by completing a certain number of courses and educational programs, then soft skills are more likely not about education, and it can be difficult to track the acquisition of such competencies.

This master thesis uses a combined research method – interviews with several stakeholders and a survey to analyze the connections between individuals' information security perception, vulnerability elimination speed, and personality differences. The study is conducted in one financial institution that mainly operates in the Baltic and Nordic regions.

The theoretical foundation is based on behavioral theories that are used to explain human behavior by analyzing the factors and consequences present in the individual's environment. The most successful information security programs and initiatives are based on an understanding of social behaviors and the context in which they occur. Therefore, interventions to improve behavior can be best designed with an understanding of relevant theories and using practical measurement tools. Individual knowledge, attitude, and behavior relating to information security were measured via HAIS-Q, which was complemented with 6 additional statements. Personality traits have been assessed using a ten-item Big Five

inventory tool. The data were analyzed using linear regression, and a comparison of means.

This study contributes to the sense that there have been no earlier studies looking into the relationship between vulnerability management efficiency and individuals' ISA and neither there is a study in the Baltic and Nordic regions. Personality differences have been used to explain the various behavioral outcome, however, personality traits have not been assessed in the context of vulnerability management efficiency.

The most interesting outcome of this thesis was the level of information security among selected groups assessed as good. This shows that the company has a strong security culture and information security training seems convenient to all types of personalities. It was found that openness explained variance in individuals' ISA, while the relationship between vulnerability management efficiency and individuals' differences has not been identified. Further research could further extend current findings by applying more comprehensive measurements for personality traits and considering more individual and organizational factors.

The thesis is written in English and contains 89 pages of text, 6 chapters, 8 figures, and 32 tables.

Acknowledgements

My sincerest gratitude goes to my supervisor Dr Kaie Maennel for her guidance, support, and encouragement during the process of creating this thesis.

I would also like to thank Hanna Katargina who was supporting me in the vulnerability management topic and situation insights within the company considered in this study.

Finally, I wish to thank my family for their utmost patience and care during the two years I have been on the way to my goal.

I hope that other students find this research useful in their studies, just as I have been inspired by the academic work of other students and researchers.

Thank you!

List of abbreviations and terms

BFI	Big Five Inventory
BFM	Big Five Factor Model
HAIS	Human aspects of information security
HAIS-Q	Human aspects of information security questionnaire
IS	Internet Security
ISACA	Information Systems Audit and Control Association
ISP	Information Security Policy
ISS	Internet Security Systems
IT	Information technology
KAB	Knowledge Attitude Behavior
NIST	National Institute of Standards and Technology
TIPI	Ten-Item Personality Inventory

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Motivation

The timely security patching has an important role in providing a secure enterprise IT environment. Vulnerability management in large enterprises is seen as an essential and non-optional task for responsible IT teams. Enterprises integrate advanced technologies to automate updates and detect vulnerabilities in time. However, according to Cyber Security Breaches Survey 2021, 69 percent of large businesses reported having up-to-date malware protection. One-third of large companies participated in the given survey and acknowledged having laptops with unsupported versions of Windows [2]. In qualitative interviews, the reason for having older versions of Windows was explained as the consequence of challenges that organizations have faced due to the Covid-19 pandemic. Many employees were forced to move home to work, thus, many laptops, tablets, and computers were issued for working at home. As result, upgrading software and hardware have become more difficult. The pandemic also had stretched resources and led to conflict between prioritizing IT service continuity, maintenance work, and cyber security aspects such as patching software. Thus the security of enterprise is not limited only to technical solutions; this is also very much a human issue. Because people are involved in the implementation of all decisions and their application in practice, people tend to make mistakes. Human behavior is largely determined by culture, everyday social, and work networks. This study aims to examine individuals and organizational factors that can contribute to enterprise security. Successful problem solving requires both an understanding of the problem and a willingness to solve it.

The motivation of this study is to make available to enterprises information about the potential connections between Information Security Awareness and Vulnerability management efficiency. This may be useful in improving the performance of detected vulnerability elimination. The predicted relationship between human factors and information security awareness will help enterprises understand the extent to which human factors affect information security at large and provide an accurate idea of what the enterprise should implement to achieve better performance.

1.2 Objective

The main objective of the present study is to investigate the relationship between the level of information security awareness, individual characteristics, and the effectiveness of vulnerability management. The previous research works already showed that ISA can be predicted by gender, age, job stress and education[3],[4],[5].In this study, the evaluation of the relationship between the level of ISA and human and organizational factors is done based on the inputs from employees of one international financial institution. Thus, this is one case study, and research is limited to the one particular financial service provider that mainly operates in Baltic and Nordic countries.

The author believes that due to the nature of the company the information security awareness should be at a good level. The author's assumption is also based on the previous research works. For example, ISA has been assessed in one Australian bank and compared with results of the identical survey conducted for the Australian general workforce[6]. Pattinson found that the level of ISA for bank employees was around twenty percent better than results for the general workforce. There was also done research for an outsourcing company in Indonesia that is engaged in banking Information Technology (IT) services [7]. This research outcome showed good results as well. Thus, the author can compare archived results with conclusions done in previous research works. This could be considered as the contribution to the construct validity of the existing ISA measurement tools.

Our findings could have important also implications for enterprises, as an outcome of this study can help them to assist in the identification of information security strengths and weaknesses, where more education and training are required. This may be useful in improving the performance on detected vulnerability elimination within the organization and can give a hint to managers about what kind of people with what personality traits fit better in one or another position.

1.3 Research questions

The thesis aims to provide answers to the following research questions (RQ):
RQ1: What is the overall ISA level in the examined company?
RQ2: Are the employees who are more involved in risk management procedures more aware of information security than the employees from business units and IT-related employees?
RQ3: Are there some correlations between the level of ISA and vulnerability management efficiency?

RQ4: What factors can contribute to the efficiency of vulnerability management?

Given the results of previous studies, it can be assumed that two personality traits (conscientiousness and agreeableness) can influence the effectiveness of vulnerability management. For example, Shropshire, who conducted a study among undergraduate students, found that conscientiousness and agreeableness are positively associated with the intention to take IS measures [8]. Uffen reported that conscientiousness is positively related to an individual's technical and organizational performance in information security [9]. In the context of this study, it can be assumed that employees with high conscientiousness scores are more effective in terms of managing vulnerabilities. Thus, the hypothesis is formulated as:
H1: Employees with high Conscientiousness scores are more likely to deal with vulnerabilities more effectively.
H2: Employees with high Agreeableness scores are more likely to deal with vulnerabilities more effectively.

RQ5: What factors are associated with ISA?

This study has collected and examined eight independent variables (age, gender, tenure, openness, conscientiousness, agreeableness, extroversion, and emotional stability) to analyze these relationships to information security awareness and vulnerability management efficiency.

Age and Gender

Personal characteristics such as age and gender are common and important demographic variables that are used in social science research. The age variables have been examined in various researches and from different aspects. For example, Nicholson in his research found that older individuals are generally more cautious and less prone to risk-taking [10]. Results of a study regarding InfoSec showed that age has been associated with risky behaviors [11], [12], [13]. Whitty has examined the effects of age on password-sharing and found that older people were more likely to share passwords [14]. However, there are studies with contradictable results in the scientistic literature. For instance, Gratian found that age demographics did not have a statistically significant unique effect on the intention of security behavior [15]. McCormac came to the same conclusion in his scientific work [4]. However, recent research works, conducted by Fatokun [16], Shappie, Dawson, and Debb [17] have shown that there is a statistically significant relationship between age and cybersecurity behavior, and that age is an important predictor of cybersecurity behavior.

The role of gender differences in information security behavior and awareness has been explored in a limited number of studies. Alothaibi conducted a study to examine the impact of gender differences on information security management and online security for Internet users. The results showed that men are likely to be better at information security and more secure on the Internet than women [18]. Broos [19], He, and Freeman [20] found that men have better IT skills and knowledge, and their decisions to use technology are more influenced by their perceived utility. Gratian found that women had weaker password generation behavior than men. In addition, women were found to report weaker proactive awareness intentions than men [15]. The above studies and findings show that gender differences can influence information security behavior and management. Thus, based on the results of related research works, we propose the following hypotheses:

H3: Human age is negatively correlated with ISA

H4: Men are more information security aware than women

Openness, Conscientiousness, Agreeableness, Extroversion and Neuroticism

In modern literature, it has long been established that in a social and organizational context, the Big Five Factor Model (BFM) is suitable for studying personality and human behavior. For example, Nicholson found that risky behavior is a characteristic of extraversion [10]. The study was conducted in various organizational and social contexts. The results of the study showed the relationship between risk-taking, high extraversion and agreeableness. Low neuroticism and low conscience have also been found to insulate people from feelings of guilt or anxiety associated with the negative consequences of taking risks. In addition, low conscientiousness makes it easier to overcome the cognitive barriers of the need for control [10], [21].

Some researchers are unanimous in their opinion that personality traits are especially important to study in relation to information security [9]. The findings have implications for employee information security behavior in terms of whether employees' personality traits explain predict their behavior in the field of information security in various organizational results. For example, Pattinson noticed that people who score high on extraversion and openness are more prone to security in the context of phishing emails [22]. Phishing email responses indicate that respondents are likely to share sensitive information, which in turn is indicative of cybersecurity risk behavior [23]. Uffen and Halevi reported that conscientiousness and extraversion are positively associated with information security management, but openness is not positively associated with the intention to use security controls [24],[25]. Welk noticed that people with lower levels of extraversion and anxiety,

which is indicative of emotional stability, were better at detecting phishing e-mails [26],[27]. Pattinson's findings showed that people who score low on extraversion and score high on agreeableness, conscientiousness, and openness are less likely to engage in risky information security behavior. Regarding emotional stability, the study found that it was not statistically significantly associated with the behavior of the information security service [22]. Whereas, Russell found that as neuroticism increases, cybersecurity behavior decreases [28]. Russell suggested that high levels of anxiety and stress in neurotics may limit the mental resources needed to maintain security in cyberspace [28]. Therefore, we expect to check the following hypothesis:

H5: Conscientiousness is positively associated with ISA
H6: Agreeableness is positively associated with ISA
H7: Openness is positively associated with ISA
H8: Neuroticism is negatively associated with ISA
H9: Extraversion is positively associated with ISA

The review of the literature related to InfoSec and personality traits revealed some conflicting results. This area of research is still developing and thus presents the opportunity to investigate further the relationship on the example of one financial institution.

1.4 Research approach

This thesis is carried out to find the answers to the questions stated in Section 1.3. The thesis applies both qualitative and quantitative methods to reach the presented aim. The author decided firstly to conduct interviews in order to gain a deeper understanding of how confident employees feel in cybersecurity-related topics and what factors can influence the process of eliminating vulnerabilities. The sample of people responsible for fixing vulnerabilities is about a hundred people. Since vulnerability management depends on several factors, it was decided to limit the sample to service owners who are directly responsible for tasks prioritization and verification of these performances. The research sample is not limited to just mentioned group of people - it includes more groups in order to get an overall view of ISA within the organization and compare groups with each other. In addition, the interviews are planned to be conducted with two-three people from several groups. Some conclusions can be drawn from the interviews as to whether chosen assessment method is relevant for application to the entire population. The author also aims to use interviews to figure out what personality traits are more typical for the employees in each group and particularly in the group, that deals with vulnerability elimination.

The quantitative research method is planned to be used to examine the level of ISA and

analyze distinctive personality traits. For this purpose author decides to use a survey distributing among 3 different groups:

- **Group 1** - employees from business units;
- **Group 2** - IT risk management procedures related to employees (risk managers, information security, and vulnerability management teams);
- **Group 3** - IT-related employees (engineers).

1.5 The contribution of the author and novelty

Individual differences and their correlation to information security awareness have been examined from different aspects. For example, it was found that agreeableness, conscientiousness, and emotional stability significantly explained variance in an individual's ISA, while gender and age did not [4]. However, the novelty of this study is the assessment of ISA and individual differences and their possible relationship to vulnerability management efficiency.

The purpose of this thesis is to examine the level of information security awareness in one targeted company and analyze the potential factors that can contribute to the efficiency of vulnerability management. The specific contribution of the author is following:

- Personality differences examination in the context of vulnerability management efficiency;
- Examination of the relationship between ISA level and vulnerability management efficiency;
- HAIS-Q complementation with 6 additional questions in order to highlight and examine the aspect that is actual nowadays.

Based on our best knowledge there is no such study conducted for the Baltic and Nordic regions.

1.6 Contents of the thesis

The first chapter is an introduction part that states the motivation, objectives, goals, research questions, and approach of the present work.

The second chapter is devoted to introducing background and definitions for information security, personality, and known measurement tools used to assess individuals' personalities

and information security awareness.

In the third chapter, the author describes the methodology used to conduct this study. This chapter also covers the construct of the survey and semi-structured interview.

The following fourth chapter is dedicated to the presentation of gathered data and its analysis. This includes the survey validity check and correlation tests.

The fifth chapter presents answers to the research questions. This chapter also provides the description of limitations that should be considered while reading this work. The thesis is closed with a conclusion part in the sixth chapter.

Every chapter is complemented with additional goals dedicated to a given section and provides input to the general aims of the given thesis.

2. Theoretical background and literature review

The chapter starts with giving a background of thesis-related topics and finishes by bringing together related academic literature specific to the research questions.

2.1 Information Security

The term "information security" has a variety of definitions and is sometimes abbreviated to the term InfoSec. The Information Systems Audit and Control Association (ISACA) defines information security as "Ensures that, within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and non-access when required (availability). Information security deals with all formats of information—paper documents, digital assets, intellectual property in people's minds, and verbal and visual communications" [29].

Previously, information security was considered mainly from a technological aspect [30]. However, technology solely is unable to provide a reliable solution to the information security needs of the company. In order to archive efficiency in information security, a balanced approach of technical, organizational, and human factors should be considered [31]. Technical factors include planning and deployment of new technologies and the purchase of hardware and software. Organizational factors are, for instance, the company's security policies, employees' awareness program, and implementation of best practices. All these activities are basic measurements for information security [32]. Human factors, such as talent hunting, hiring of specialized personnel, employee training, and motivation are the most critical element in information security [33]. From one side, employees can be seen as weakness side, as they may be involved in malicious activities and violate the security policy [34]. On the other hand, employees who keep their knowledge updated regularly, contribute to maintaining high quality for the company in terms of service, security, and regulatory compliance. Therefore, it is necessary to consider the human aspects in detail to reduce human shortcomings and ensure efficiency for better information security management. People have an important role in all organization's processes. One of the critical organizational processes, which is stressed in this study, is vulnerability management.

2.1.1 Vulnerability Management

Vulnerability management is integral to information security and important to companies due to the rising threat of cybersecurity attacks [35]. This is a term generally defined as the process that includes proactive asset discovery, continuous monitoring, mitigation, remediation, and defense tactics to protect an organization's IT and business assets. According to the ISO 27001 standard for ISO Information Security Management Systems, a vulnerability is "a weakness of an asset or control that could potentially be exploited by one or more threats", where threat is defined as "potential cause of an unwanted incident, which may result in harm to a system or organization" [36].

Vulnerability in computer systems can be defined as a defect or bug that allows an external entity to directly or indirectly influence the availability, reliability, confidentiality, or integrity of a system, application, or data. New vulnerabilities are discovered each day, creating a challenge for organizations to timely identify those affecting the organization, determining the possible impact on its assets, prioritizing and carrying out the mitigation activities required to protect the organization against exploitation. A security vulnerability that is so new that only a knowledgeable hacker knows about it and the software vendor is not fully aware of yet and has not even had a day to fix it is called a zero-day vulnerability. However, if a security patch to a vulnerable service already exists, that's a different story. Unfortunately, many organizations often do not have a detailed overview of all their vulnerabilities, as they do not perform vulnerability scans frequently enough. Timely detection and remediation of vulnerability are crucial to any security strategy [35].

The reality is that security vulnerabilities are in almost every system and in every code - each organization have to search for them and remediate in timely manner. The effective vulnerability management, like all else in security, is more than just the technology used in this space. It is a social science that combines people, processes, and technology. Thus, it is no wonder that many researchers aim to determinate what factors can be used to make people more aware of threats and take security warnings seriously [37].

2.2 Human aspects in information security

Information security is not just about technology, it is mostly about people using the technology. Since a person is a consumer of information and an important part of its processing the risk associated with a decision error has always existed, exists, and will exist in the future. Errors that are a manifestation of the human factor, in most cases, are not intentional. As a rule, a person performs erroneous actions and regards them as correct

or most appropriate. Errors can also occur due to ordinary carelessness or negligence.

The human factor is a concept that covers a set of various manifestations of human actions, his social or creative activity, and all possible consequences of activity, both at the personal level and at the level of labor and any other teams. The human factor is the subject of study in many public Sciences (sociology, social psychology, anthropology, etc.), which led to the creation of interdisciplinary theories reflecting its essential characteristics. For the first time, the concept of the "human factor" was introduced by Frederick Winslow Taylor, who set himself the task of creating a system for increasing labor productivity through its intensification. He concluded that the main reason for low productivity lies in the imperfect system of incentives for workers [38].

With the advent of computers and information systems, the human factor is becoming increasingly important. Due to the rapid growth of advances in telecommunications, computing, and software at the end of the 20th century, there followed a sharp increase in the complexity of information systems and, as a result, the requirements for the skills of their users. The range of threats to users of information systems has stepped far beyond the boundaries of specialized computing centers. Under such conditions, the human brain, as well as its physiological state, did not undergo any significant changes. The person did not become stronger or more enduring, did not begin to think and make decisions faster. However, the load on the human brain in the age of high technology has increased many times over. And, consequently, the probability of an error caused by a human factor has increased.

The reasons that contribute to human erroneous actions can be grouped into several groups: information support deficiencies or their absence (special handlers for such situations in software, visual materials, and instructions). This problem is especially pronounced in extreme situations and in conditions of lack of time to make a decision; errors caused by the influence of external factors (distraction of attention from the problem that has arisen); errors caused by the physical and psychological state and properties of a person. For example, sudden stress with the general monotony of work, emotional tension and impulsiveness, or vice versa, suppression of the reaction to the problem; limited resources to support and implement the decision; lack of consideration of the human factor in the list of possible causes of the incident [39], [40].

2.3 Information Security Awareness (ISA)

Information security awareness is one of several key principles of information security and it is one of the central terms in the field of human aspects of information security

[41]. By reviewing ISA-related literature, it became evident that there exists no one universal definition. Nevertheless, ISA could be defined through three aspects. The first is based on the cognitive perspective and is defined as an employee's state of mind, which is characterized by understanding the importance of information system security and its objectives, risks, and threats [42],[43],[44]. The second aspect refers to actual ISS behavior, focusing on the extent to which employees "acting or responding according to an organization's ISS rules" [45] and "being committed to their security mission" [42],[46],[47]. The third aspect covers process perspective. The ISA is also described as the actual process to raise awareness. Kritzinger and Smith (2008) [48] state that ISA "is about ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with." The U.S. National Institute of Standards and Technology (NIST) definition of ISA is also largely based on the process perspective since they state that "the purpose of awareness presentations is simply to focus attention on security." Nevertheless, NIST definition also incorporates two mentioned aspects, stating that awareness is "intended to allow individuals to recognize IT security concerns and respond accordingly "[49].

These definitions show that awareness and behavior are closely related to each other, and could be difficult to draw lines between them. In the current study, information security awareness (ISA) is defined as an employee's general knowledge about information security and his cognizance of the information security policies (ISP) of his organization.

2.3.1 Information Security Awareness Measurement

A thorough review of the literature has uncovered various frameworks used to measure information security awareness. This includes models such as the Theory of Planned Behaviour [50], the Protection Motivation Theory[51], the General Deterrence Theory [52] and the Knowledge–Attitude-Behaviour (KAB) model [53].

The theory of planned behavior was proposed by Ajzen and Fishbein and it argues that a combination of attitudes(beliefs about a behavior), subjective norms (beliefs about others' attitudes toward a behavior), and perceived behavioral control will shape an individual's intention towards carrying out a behavior[54](see Figure 1).

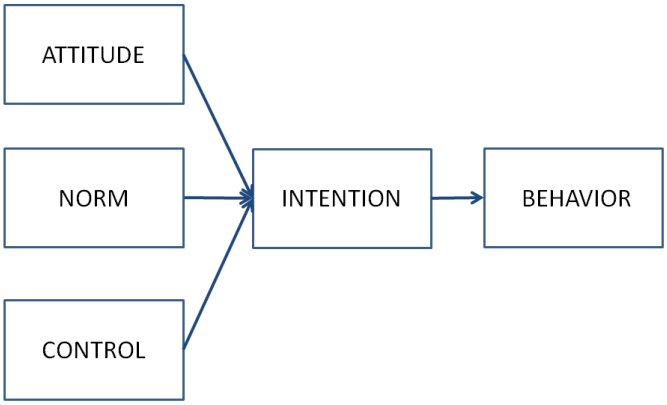

Figure 1. *Theory of Planned Behaviour (composed by the author based on [50]).*

This model is useful for making predictions and great for finding the relationship of attitudes to behavioral intentions. However, it doesn't address how to determine actions that result in changing behavior. The model does not include other behavioral factors like emotions (sadness, frustration), which can play an important role in influencing behavior.

Protection Motivation Theory, in contrast, focuses on one of the seven universal emotions experienced by everyone around the world - fear. This theory was originally developed to test how fear influenced individuals to change their health behavior and further adapted to be a more persuasive means of changing behaviors [51]. The protection motivation theory proposes that people protect themselves based on four factors: the perceived severity of a threatening event, the perceived probability of the occurrence, or vulnerability, the efficacy of the recommended preventive behavior, and the perceived self-efficacy (Figure 2).

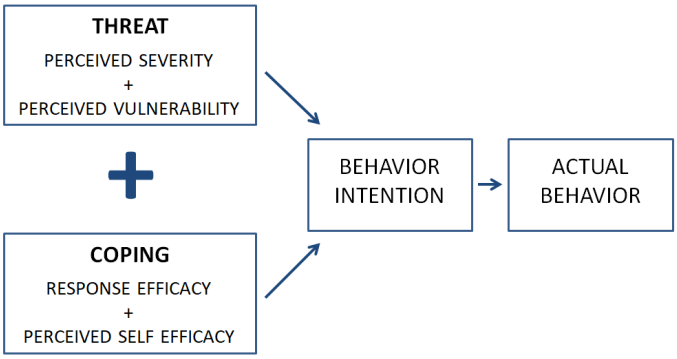

Figure 2. *The Protection Motivation Theory (composed by the author based on [51]).*

The protection motivation theory deals with how people cope with and make decisions in times of harmful or stressful events in life. The theory attempts to explain and predict what motivates people to change their behavior. The theory is used mainly as a model to explain decision-making and action about health. There are many important differences between the field of information security and the field such as health. These differ in regards to the comprehension of information and the consequences for action or inaction.

For example, topics like the health benefits of certain foods have been widely debated, which means people are faced with conflicting information and the scientific legitimacy of this information is not always clear. In contrast, in the field of information security, most companies have information security policies and guidelines, which indicate what is expected from employees [55].

General deterrence theory is correlated to Protection Motivation Theory, stating that the public can be discouraged from committing crimes by preying on their fears. But this focuses on another aspect - a fear of punishment [52]. Deterrence theory suggests that an individual commits a crime after evaluating the benefits and consequences of the deviant behavior. They involve in deviance after making sure that, the benefit of deviance is greater than conformity and the cost of deviance is lower compared to reward [**Cheng**].

Knowledge, Attitude, and Behavior (KAB) is an important theoretical model stating that knowledge and attitude influence behavior change [56](see Figure 3). From social learning theory, we learn that attitude is very important for the acceptance of the behavior. One consequence of this is that educators should work to instill positive attitudes in people in order to change their choice of action. People are more likely to take action if they believe that what they are about to do is of significant value [57].

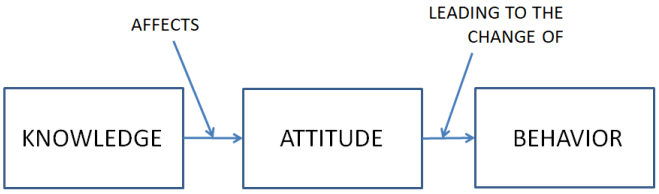

Figure 3. *Knowledge-Attitude-Behavior Theory (composed by the author based on [56])*

All these existing behavioral models have been used in an attempt to better understand aspects of ISA. However, according to Karjaleinen [58], many of these studies are focused primarily on theory-verification or validation. Whereas, the effectiveness of ISA programs has often been evaluated by measuring three-dimension originating from KAB model [59]. Additionally, previous studies show good results about the validity of the KAB model in practice. For example, Rosenbloom found that an active learning program in the schools in Israeli resulted in an increase in pupils' knowledge and improvement in behavior regarding road safety [60]. The research, performed in the information security area by Wyhyudiwan, showed that knowledge-based programs improved the knowledge, attitude, and behavior of people on such topics as password management and email usage

[61]. Also, Parson concluded that there are significant associations between an individual's knowledge, attitude, and behavior when using a work computer [55].

Although the importance of assessing the ISA of individuals has been acknowledged by researchers, research focusing on the ISA measurement is relatively limited. The majority of studies used one specific area of information security to measure ISA. For example, Stanton examined password-related behavior [62], Acquisti and Gross focused on behavior on social media [63]. In response to the need for a holistic method of measuring ISA, Parsons and her team developed a survey instrument HAIS-Q, that assesses seven focus areas. This research uses the Human Aspects of Information Security Awareness framework, as it has been peer-reviewed, refined, and comprehensively assessed the validity and reliability with diverse participant samples, using different methodologies, and is regarded as valid [55], [64],[65].

2.4 Human Aspect Information Security Questionnaire (HAIS-Q)

HAIS-Q is an online survey tool, which allows managers to examine the information security awareness among their staff from a non-technical perspective. This instrument was designed and developed as a modular tool to enable it to be tailored to specific research needs [6]. The tool consists of 63 statements answered on a 5-point Likert scale, ranging from 1="Strongly Disagree" to 5="Strongly Agree". As shown in Figure 4, the HAIS-Q comprises seven focus areas: Password management, Email use, Internet use, Social media use, Mobile devices, Information handling, and Incident reporting. These seven focus groups are priority areas in the ISA commonly covered in the company's information security procedures and instructions. Each focus area is further divided into three specific sub-areas that are based on Knowledge-Attitude-Behaviour (KAB) model, and contains statements relating to knowledge, attitude, and behavior. This current research uses Parsons [55] definition of these three components:
Knowledge - What a person "knows" about behaving in a safe manner;
Attitude - How a person "feels" about behaving in a safe manner;
Behavior - What a person actually "does" when using a digital device.

For example, within the incident reporting focus area, the specific statements include:
Knowledge: *"If I see someone acting suspiciously in my workplace, I should report it."*
Attitude: *"If I ignore someone acting suspiciously in my workplace, nothing bad can happen.*"*
Behavior: *"If I saw someone acting suspiciously in my workplace, I would do something about it."*

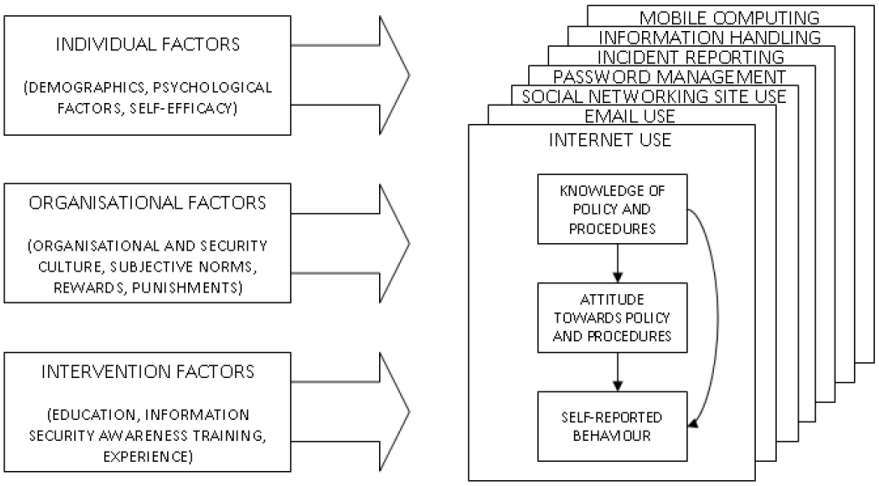

Figure 4. *The Human Aspects of Information Security Model [55].*

It is important to mention that the KAB statements stand for one part of an overall HAIS model that is being developed by Parson [55]. Figure 4 shows that the relationship between these three components is influenced by many other factors, that could be grouped as an individual, organizational, and intervention factors. For example, an individual's education and experience, security culture in the company, fears to be punished, and individual characteristics. Thus, the HAIS model embraces several behavioral theories and frameworks, such as the Protection Motivation Theory (reward, punishment), the deterrence theory (fear of punishment), the theory of planned behavior (company's policy, culture) and the KAB model.

2.5 Personality

Personality refers to a person's qualities and individual characteristics, as well as character traits of thinking, feeling, and behaving. According to an American psychologist, Gordon Allport, personality can be defined as the dynamic organization within the individual of those psychological systems that determine his characteristics behavior, and thought [66],[67]. While it may have been defined in many ways, most theories focus on psychological motivation and interaction with the surrounding environment. Thus, for example, Freud found that the personality can be structured into three parts – the id, ego, and superego- that are developing and changing during the different stages of an individual's life [68]. The concept of the id intersects with Eysenck proposed personality theory, also known as Eysenck's personality theory [69],[70]. According to this theory personality is based on biological factors. He argued that humans inherit a type of nervous system that predicts their ability to learn and adapt to the environment.

Eysenck [70] found that an individual's behavior could be represented by two dimensions:

Introversion / Extroversion (E) and Neuroticism / Stability (N). Later he added a third trait/dimension – Psychoticism/ Normality [71]. Meanwhile Cattell argued that a complete picture of someone's personality should be looked at through a much larger number of traits [72]. Cattell developed a personality test, called 16 Personality Factors Test (16PF). This test has 160 questions in total and measured sixteen traits. However, Cattell's list of traits has been examined by several psychologists and researchers and as result, this list was reduced to five traits. This framework became known as the "Big Five" [73], [74],[75].

This framework has been examined and validated across different populations and cultures. Since it is the most widely accepted personality theory held by psychologists today, the author decided to use it for the current study.

2.5.1 Big Five inventory (BFI)

The Big-Five framework is a model of personality traits with five broad factors. Each factor is bipolar (for example, Extroversion <-> Introversion) and reflects several more specific facets, such as sociability, excitability, and assertiveness. The Big Five proposes that all people, regardless of gender, age, or culture, share the same basic personality traits, but differ in their degree of expression. The framework suggests that most individual differences in human personality can be classified into five broad domains. These five domains are usually described as openness, conscientiousness, extroversion, agreeableness, and neuroticism, Sometimes it is abbreviated to the acronym OCEAN.

While there is a significant part of literature that supports this five-factor model of personality, the researches' opinion about exact labels can differ. However, these five traits are usually described as follows:

Table 1. *Descriptions of Big Five Personality Traits [76].*

Big Five trait	**Description**
Openness to experience (O)	People are characterized by such attributes as open-mindedness, active imagination, preference for variety, and independence of judgment.
Conscientiousness (C)	People high on this scale tend to distinguish themselves for their trustworthiness and their sense of purposefulness and responsibility. They tend to be strong-willed, task-focused, and achievement-oriented.

Continues...

Table 1 – *Continues...*

Big Five trait	**Description**
Extroversion (E)	People scoring high on the extroversion scale tend to be sociable and assertive, and they prefer to work with other people.
Agreeableness (A)	People high on this scale tend to be tolerant, trusting, accepting, and they value and respect other people's beliefs and conventions.
Neuroticism (N)	It is the opposite of emotional stability. People high on the N scale tend to experience such negative feelings as emotional instability, embarrassment, guilt, pessimism, and low self-esteem.

There have been developed several rating instruments to measure the Big-Five dimensions. The most comprehensive instrument is 240-item NEO Personality Inventory, developed by Costa and McCrae [77]. This tool measures the Big-Five domains and six specific facets within each dimension. The NEO-PI-R is too lengthy and takes about 45 min to complete, therefore several shorter tools are created and commonly used. For example, well-established and widely used instruments are Goldberg's instrument comprised of 100 trait descriptive adjectives (TDA)[78], the 60-item NEO Five-Factor Inventory (NEO-FFI) [77] and the 44-item Big-Five Inventory (BFI) [79]. Recognizing the need for an even briefer measure of the Big Five, Saucier (1994) developed a 40-item instrument derived from Goldberg's (1992) 100-item set [80]. Due to the cost and time associated with BFI measurement, very brief measures, such as 5-item and 10-item inventories were also developed and evaluated [81].

Given the large selection of tools, researchers suggest choosing the tool depending on the scope and need of the study. The long tool tends to have a comprehensive measure of psychometric properties, whereas the brief tool can be considered when time is limited [77],[81].

2.6 Related works

In academic literature, several studies applying human behavior theories did research on inter-relatedness of people and their environments, their interactions with and adaptations to each other, explain the contextual nature of human behavior. This section presents overview of conducted works related to information security awareness, personality and vulnerability management.

Information security awareness of employees is one of the most important aspect for achieving information security goals in each organization. Therefore, many researchers are interested to reveal factors that affect employees' ISA level. The ISA level has examined in context of employees' gender, age, personality, and risk-taking propensity [4]. The study found a significant positive between age and level of information security awareness, but in relation to gender, the difference is not significant. It was also revealed that open individuals who are more likely to take fewer risks have a higher level of information security awareness. These findings partially align with previous Pattinson' research results [22]. They showed that agreeableness, conscientiousness and ability to control impulsivity are significant predictors in self-reported InfoSec behaviour. Whereaes, McBride argued that simply being an agreeable individual does not necessarily mean that individual is less likely to violate a cybersecurity policy [82]. The research stated that agreeable individuals who feel that sanctions are unlikely to be applied are more likely to violate cyber security policies, even if they know that penalties are likely to be enforced [82].

Level of Information Security Awareness was also explored in the context of moral disengagement and counterproductive work behaviors [83]. The research found that moral disconnection does not automatically lead to problematic behavior and that ISA knowledge and attitude can mitigate negative consequences. However, the roll of stress is positively associated with non-compliance with ISP requirements. Simon Trang and Ilja Nastjuk determined that in a situation of limited time, a person's goal is to reduce the amount of information processed, and as result shape ISP compliance behaviour. They also found that punishment can buffer the effect of perceived stress on ISP non-compliance [84].

The relationship between culture and Information Security Awareness has been examined by Ashleigh Wiley, Agata McCormac, Dragana Calic [85]. Study findings showed that security culture mediates the relationship between organizational culture and ISA strongly affected by security culture. Meaning a strong security culture may be a better predictor of employee ISA. According to Tanja Grassegger, Dietmar Nedbal, the important factors that influence ISA are leadership and risk-taking behavior [86]. This was further supported by Hadlington, who found that those people who were categorized as more external, having limited perceived control over their work environment, were more likely to have weaker information security awareness [83].

Jordan Shropshirea, Merrill Warkentinb, Shwadhin Sharmab in their research work were trying to predict the initial adoption of information security behavior and figure out, if there some dependencies on personality factors in determining the likelihood that an individual will or will not follow through and act on the intent to engage in protective behaviours [87]. According to the research result, people who are conscience and agreeableness

showed to lead to increased usage behavior among those who reported intent to adopt this security software. Mark Harris and Steven Furnell looked at security compliance behavior from a shamed perspective. It turned out that the effectiveness of shame as a tool of encouraging security compliance is depend on whether employee cares about co-workers and employment [88].

There have been done several researches to determine the impact of training to employees' level of security awareness. Marlies Sas examined how training sessions effect on employees' level of physical security awareness and found short-term positive effect of training's on physical security awareness level [59]. Mitchell Kajzer made an exploratory investigation of message-person congruence in information security awareness campaigns [89]. He examined whether certain information security awareness message themes are more or less effective for different types of individuals based on their personality traits. Study results shows that personality plays a role in security awareness message effectiveness. However, Malcolm Pattinson came to the opposite conclusion while examined information security awareness at an Australian bank. This comparative study showed that training and frequency of trainings have no significant effect on employee's level of ISA [90].

3. Methodology

This chapter presents the research method and design, and describes the criteria for the selection of participants and data collection. This also provides considerations about data privacy and ethics.

3.1 Research method

This study is conducted using mixed methods research, that utilizes qualitative (interview) or quantitative (survey) approaches. Qualitative data helps researchers understand processes, provide detailed context information, and seek to explore human experience to understand the reason behind the behavior [91]. Quantitative research is used for deductive research, to gather descriptive information, or examine relationships among variables. Quantitative data provides measurable evidence and helps to facilitate the comparison of groups, and establish potential cause [91],[92]. The mixed methods research involves the collection of both qualitative and quantitative data to combine the strengths of each to answer research questions [92]. According to Yin [93] such an approach would allow addressing a more complicated question.

First we conduct a literature review on theories and previous researches related to the topic of this study. Next the author decided to perform research in two steps. A semi-structured or structured interview is planned to be used for the first part and a survey for the second part. Interviews do not restrict interviewer and interviewee allowing expressing more details and their own views. Interviews were used also to examine the validity of chosen methodology and get recommendation for survey improvements prior distributing it to the larger audience.

The benefit of using a hybrid approach is that once the interviews have been conducted, it is possible to make some initial conclusions about correlations and select appropriate research method for the whole population.

The author's initial consideration is to adopt the HAIS-Q [64] to measure an individual's ISA based on their knowledge, attitude and behavior, and the Big Five model [94] for measuring and understanding the personality. The author reviewed different instruments

and explained the choice in the second chapter.

3.2 Research design

The preparation work started with analysing data from vulnerability management system that is used in the company. The author consulted with vulnerability process manager to get overview of the existing vulnerability process and to request initial data for analysis.

Since one the goal is to examine level of information security awareness and its correlation to vulnerability efficiency, the author faced with a dilemma: what criteria should be used to divide people in Group 3 into sub-groups. The third group, that was considered from the beginning, consists from employees, who are responsible for some information asset and responsible for vulnerability elimination in case of such detection. In turn, these people should be divided into two groups by efficiency of detected vulnerability elimination. Based on the received insight information about process and initial data analysis, it was decided to take as a basis the number of vulnerability records eliminated within the defined time frame and the number of vulnerability records that missed target date.

The used vulnerability management tool operates with 5 main remediation statuses: approaching target, in-flight, no target, target met, target missed. As three first statuses do not reflect the final state, it was decided to use only statuses "target met" and "target missed". Only vulnerability records registered during 2021 year were taken into consideration. The author extracted the records that meet described conditions from the vulnerability management system. The extracted list was further grouped by task assignment group. To select the list of assignment groups, that in most cases eliminate vulnerabilities within defined time, the author summed up all records assigned to the exact group. This was considered as "Total". Next, this list had to be divided into two groups. The author called these respectively as "Top Target Met" and "Top Target Missed". Next conditions have been used:

- Top Target Met: ration of records with state "target met" assigned to exact assignment group towards "total" is 80% or higher.
- Top Target Missed: ration of records with state "target missed" assigned to exact assignment group towards "total" is 40% or higher.

When two groups where created, the author using available tools added next to each assignment group the names of service owner and assignment person. Due to the fact, that one person could be in the role "service owner" and "assigned person" for several services, the author reviewed composed two groups with purpose to ensure that the person

is a member of just one group. As result, people names, that were in both groups, were removed from these two sub-groups, but these were used in analysis of Group 3.

3.3 Interview preparation

In the preparation stage it was decided to use a semi-structured individual interview with 2-3 people from each group. The author used some personal contacts and consulted with the vulnerability process manager to find people, who is open and talkative. The main focus was on the third group of people, who is responsible for some service and as result part of vulnerability management process. The author has acknowledged that there can be several correlations which could influence the speed of vulnerability patch. For example, application owners can have dependencies on platform owners. Another widespread reason for not patching vulnerability in time is dependencies on vendor patching process. Thus, it was planned asking to share the interviewee's point of view about possible constructions that could influence the vulnerability management process.

To get feeling about differences among people in different groups, the author hold interviews with people from Group 1 and Group 2 as well. The purpose of having discussions with these two groups was to discover how confident they feel in information security topics and how would they, based on working experience, evaluate ISA in different groups.

The author took into consideration the potential impact of individual differences on ISA. For example, some previous studies have found that ISA is positively associated with such personality characteristics as agreeableness and conscientiousness. It has been suggested that individuals who are more agreeable experience security issues [95]. Thus, in order to perform some short pre-assessment, two statements that could help to rate interviewee's level on agreeableness were added.

The author prepared the following interview structure to have discussion with people from the three groups:

1. Introduce the purpose and the scope of the interview.
2. Explain what is planned to be examined in the study and how interview and survey results can contribute to the study purpose.
3. Ask the interviewee to describe their job role and main responsibilities.
4. Ask to rate two statements choosing on of the answer: strongly agree/agree/neutral/disagree/strongly disagree:
    - *I see myself as someone who tends to be lazy.*
    - *I see myself as someone who does a thorough job.*

5. Describe a suspicious situation and discuss this with interviewee to figure out if the person feel confident or unprepared to be able to spot something out of place.
6. Ask to rate the level of information security awareness in a range from 1 to 10, where 1 is low and 10 is high:
   - interviewee's level
   - ISA level in interviewee's team
   - average level in the whole organization
7. Ask to elaborate how they understand "efficient vulnerability management".
   Next questions were asked only from people in the Group 3:

8. Investigate what the interviewee think about current vulnerability management process and what can be improved or be done in different way.
9. Ask to describe the main obstacles that they have experienced with vulnerability remediation.
10. Investigate how they keep informed about vulnerabilities and threats that have discovered outside the company environment.
11. Ask to describe the routine of getting vulnerability alerts internally and from vendors.
12. Ask to introduce the basis for prioritization of vulnerability remediation within the team and organization.

Each individual interview has been conducted by following the structure described above. The author took notes on the responses during the interview. At the end of discussion the author presented the prepared survey and asked to answer this. Each interview lasted for about 30 minutes. In addition, the author asked while answering the survey to pay attention on its construction and possible shortcomings. The interviewee was asked for having one more short meeting for sharing feedback and correction notes. All received comments were considered in the final version of the survey.

3.4 Questionnaire preparation

To accurately measure employees's awareness of information security and their personality traits a survey was created. The questionnaire methodology contains 3 sections:

1. Background information/demographic questions (such as gender, age group, current role and work experience in years)
2. Information security statements
3. Personality assessment statements

The first section collects basic information related to respondents and their employment

basic information.

The second section contains items to measure level on information security awareness among 7 focus areas. The questions were created based on HAIS-Q framework developed by Parsons [64]. Parsons' origin questionnaire consists of 63 questions. As the field of IT is changing a lot over the years, the author analysed what has been changes in IT from information security perspective during last 5 years. As result the second section was updated with 6 more questions. Namely, the author decided to add 3 questions under focus area Mobile or Portable device about working at home. The ground for this is the current situation with covid and in connection with which thousands of businesses around the world have been forced to introduce remote work for their employees. People feel at home safe and as result could tend to ignore rules for keeping conversations, sensitive documentations and data secure. Employee could feel that close family can be trusted, nevertheless there is no control over precisely who is listening in and who might inadvertently disclose something that's seen or heard. Thus, next three questions following the logic of KAB module were added:

Knowledge: *"I have to keep my laptop locked when I step away from it, even when work from home."*
Attitude: *"Nothing bad can happen, if my family members see documents, programs I use at my work laptop.*"*
Behavior: *"I use my working laptop only for work related tasks."*

The focus area Information handling was also updated with 3 more questions. The author found that the important element of information security such as information classification is not covered in the Parson's origin questionnaire. This is probably due to the fact that the leading information security standard ISO/IEC 27001 standard doesn't say much about information classification and how to implement this.[add reference] Thus the way of implementation is pretty much left up to each company. Nevertheless, the classification of information is certainly as fundamental part of securing companies' information, as this provides the basis for protection efforts and access control.

After reviewing company group security policies and training materials, the author decided to add the next 3 items:

Knowledge: *"All documents developed within or by order of the company have to be labelled in accordance with the classification of their content."*
Attitude: *"Information classification and document labeling makes easier for everyone to understand how to handle information."*

Behavior: *"I label document only when this contains confidential information.*"*

Thus, the structure of adjusted HAIS-Q is shown at Figure 5. The updated parts are marked as blue.

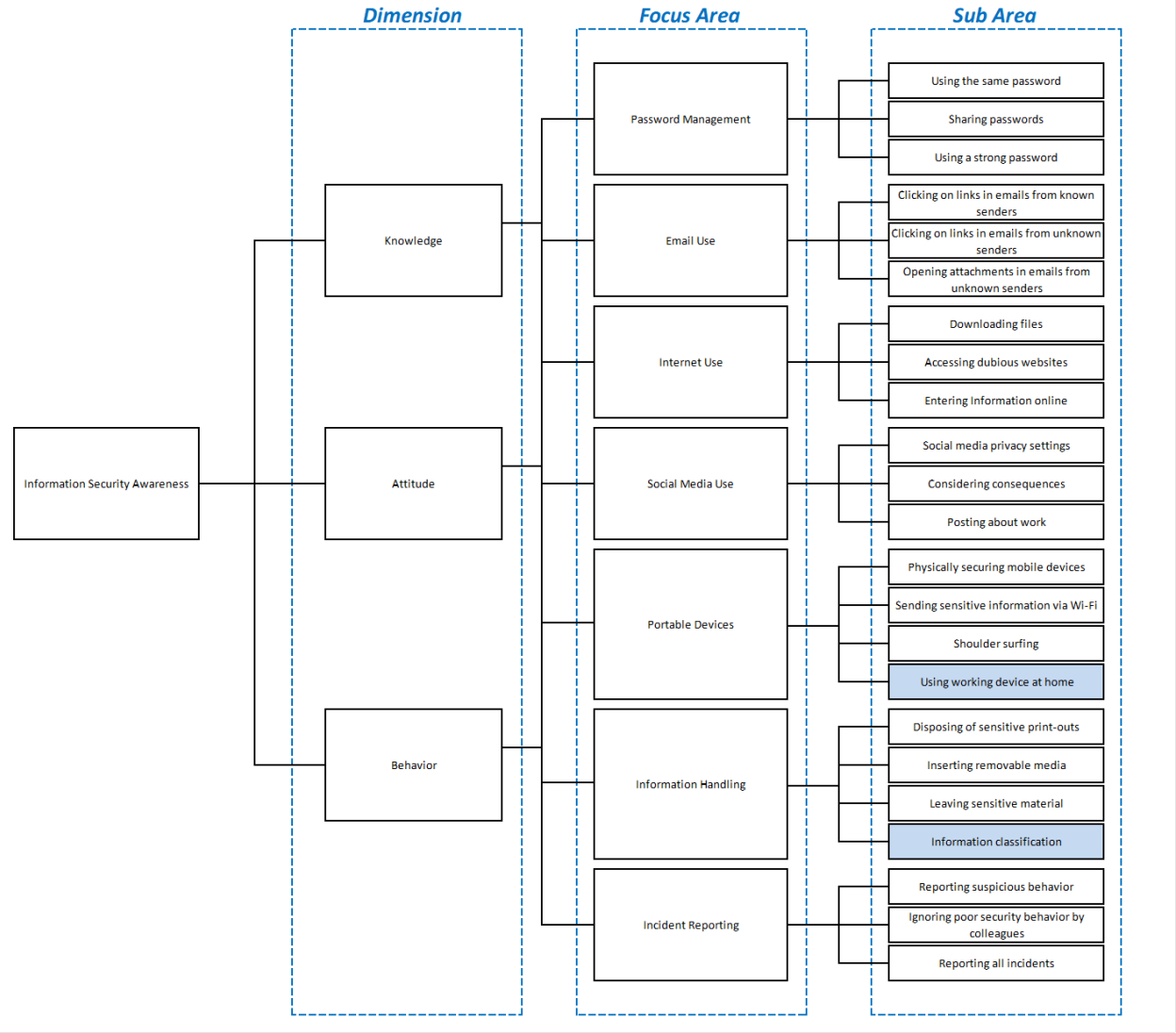

Figure 5. *Parsons HAIS-Q 2017, added by author (composed by the author).*

The third section of the questionnaire includes items to examine respondent's personal traits. For this purpose the author decided to use the Big Five Personality test, that is widely prevalent in personality research. There is a variety of measures have been developed to measure personality variables. The author decided to use 44-item test, that was drawn from previously validated studies [79],[94],[96],[97]. The Big Five Personality test is designed to measure these five personality factors or dimensions: Extroversion, Agreeableness, Conscientiousness, Neuroticism and Openness. The test consists of forty four items that is asked to asnwer using a five point scale where 1=Strongly disagree, 2= Disagree, 3=Neither agree nor disagree, 4=Agree and 5=Strongly agree.

The personality dimensions of the Big Five have been observed across cultures and in many different measurement systems. They are the fundamental building blocks for describing personality. Each of the Big Five aspects has significant validity and reliability, making them extremely valuable for a business that wants to evaluate potential new hires or make a hiring decision on current staff.

3.4.1 Questionnaire validation

We asked for feedback on our initial measurement items from people, with whom we hold interviews. Firstly we had interview and then asked to fulfill the questionnaire. After a while we have contacted this person again and asked for feedback.

The average time spent to answer all questions was 50 minutes, that most probably indicates that there was too much questions. The another reason could be that the questionnaire was on English language and some terms was hard to understand for people, who's native language is not English. The received feedback confirmed that the third part of questionnaire required too much time, as some terms have been checked additionally in the dictionary to clearly understand its meaning. For example, "I see myself as someone who has an assertive personality." and "I see myself as someone who starts qurrels with others."

In additional, as the questionnaire has been sent to employees during their working time and considering that people should prioritize the work tasks first, the questionnaire was answered by piecemeal.

Considering all received feedback, the questionnaire was adjusted accordingly. The author decided instead of using the origin version (44-item) of the Big Five inventory (BFI), implement the short ten-item long, which will significantly reduce the length of the questionnaire. This also reflect Mary Addo recommendations, that the survey should have to be reasonably short, since surveys that demand to much time and commitment tend to go unanswered [91]. The short questionnaire might be challenged by some author, although other researches showed that shorter versions (5-item and 10-item) are validated and reliable tools [81],[98]. Of the two short tools, the 10-item tool is preferable, as it allows researchers to assess for acquiescence response bias and check for errors. It takes no longer to complete than the 5-item instrument (about 1 min), thereby this is considered to be more desirable instrument, especially when research conditions dictate that a very short measure be used [81].

3.5 Data collection

After the questionnaire was composed and validated by 11 people from 4 groups, this was adjusted and then distributed among staff members between 23 March and 3 April. Since the goal is to measure ISA among different groups, the author created separate survey for each group. This approach helps to have anonymous responses and still get data that represent the group. Selected groups of employees received an email with a corresponding link to the questionnaire, which was developed in Netigate, as this platform is accessible for all employees in working environment. After seven days, a polite reminder was sent via email. The survey setup allowed only one answer per computer.

3.6 Ethical considerations and data privacy

Information is valuable asset and its protection is the main concern of any company. Revealing too much details about information security and possible weaknesses in the company can have reputation impact or be used for adversaries or scammers. That is why it is important to ensure that no confidential and compromised information are disclosed.

There are several ethical issues that author considered when planned the data collection from participants, such as a voluntary participation in the interview and survey, informed consent for potential participant, anonymity of collected data and confidentiality of interviewees.

The participation in the interview and survey is voluntary and all people invited to participate are free to choose to participate without any pressure or coercion. All participants are able to withdraw from the survey participation at any point without need to provide a reason for that. The author informed all potential participants that they are free to choose whether they want to participate, and they can withdraw from the study anytime without any negative repercussions in the email-invitation.

The author provided all potential participants with all relevant information about this study purpose. We also let them know that their data will be anonymized and will be kept confidential. The data collected during the interview is pseudonymized, personal information is separates from the study data. Only author knows who the participants are, but all identifying information is removed from the report to ensure the confidentiality of interviewees.

The author used a dedicated separate survey account, where data privacy is regulated by

the signed agreement between the company and survey service provider. Final interview and survey data were stored on the company computer and using company secure network. Only author had access to the computer, that using two-factor authentication method. The collected data form surveys and interview will be deleted after the thesis work has been defended.

4. Data analysis

In this chapter, the author has presented the gathered data and these analyses. This part is constructed in a way to find the answers to the raised questions:
RQ1:*What is the overall ISA level in the examined company?*
RQ2: *Are the employees who are more involved in risk management procedures more aware of information security than the employees from business units and IT-related employees?*
RQ3: *Are there some correlations between the level of ISA and vulnerability management efficiency?*
RQ4: *What factors can contribute to the efficiency of vulnerability management?*
RQ5: *What personality trails are more typical for the employees in each of the selected groups?*
RQ6: *What factors are associated with ISA?*

This chapter starts with interview results and continues with the analysis of survey data, including the demography of respondents and the assessment of the survey reliability. This part includes the assessment of ISA differences among selected groups and an analysis of possible factors, that could potentially affect the level of information security awareness and way of working.

Almost half of the statements included in the survey were reversed. Prior to the start of data analysis, the survey responses were converted to points to get the quantitative result using the Likert Scale. Positive questions have 5 points for "Strongly agree", 4 points for "Agree", 3 points for "Neither agree nor disagree", 2 points for "Disagree", and 1 point for "Strongly Disagree". The responses for the reversed statement were assigned to integers in the opposite direction. For example, "Strongly disagree" was rated as a 5, not as 1. Such it was possible to aggregate the scores achieved by the items belonging to the same focus area and analyze these through KAB components and relation with personality traits.

4.1 Results from interviews

In this part, the author has presented the main takeaways from the interviews. The interviews were used to get feelings about what people think about information security

awareness in the closest team and in the whole organization, discuss the importance of vulnerability management and get some impression about personality.

The fact, that these people were ready to have an interview, is already indicated that they enjoy new experiences, and feel empathy and concern for other people. It was also seen, that some people tried to prepare prior to the meeting by asking for more details about the purpose of the interview, others just followed the way it goes. In order to pre-assess the level of conscientiousness, that is associated with higher scores on the HAIS-Q [4],[6], the author asked the interviewee to rate two statements. These were later reviewed in the context of HAIS-Q points. The total of two statements was higher than 7 for all interviewees, while the results from the online survey were in the range of 6 to 9. This could potentially explain that responses were not straightforward, predictably due to personal interaction.

In order to understand how confident interviewees can spot something out of place, all participants responded identically - confident. It could show confident bias because humans tend to overestimate their abilities, however, this does not affect the results of this study. Whereas interviewees were asked to rate the level of information security awareness, the answers were various. The employees were asked about their personal ISA level, as well as the level in their team and the whole organization. It was asked to use 10 point scale, where 1 is low and 10 - high. The majority rated their level the same or higher than the level in their team, whereas everyone was unanimous in the opinion, that the level of ISA in the organization is lower than their own and in their team. The minimum given value was 3 and the maximum was 8 when discussing the overall level in the organization. To conclude, the average score for personal ISA level was 8.3, in the team, it was 7.4, and for the overall - 6.1 points.

It is quite common, that the same thing can have different meanings and interpretations for people. This was the case with a definition for "efficient vulnerability management". Some people were more focused on technical aspects, such as tools that are used for vulnerability detection, and their capabilities to analyze and select the method to eliminate vulnerabilities. Others described this as a process of implementation, testing, and reporting, as well as how the implemented process is followed in the organization. Few people were on the option that it is more than just a tool or process, it is employees' mindset and their level of awareness. There were shared some examples, such as, that by default everything should be closed and then could be open only based on clear need.

When interviewees were asked how the vulnerability management process can be improved or if there is something that can be done differently, then the main concerns were heard

about the vulnerability management tool and its' setup. Some people are looking forward to having more transparent procedures of processes and responsibilities.

The discussion with the interviewees also revealed some obstacles that could influence the speed of vulnerability elimination. The main reasons are dependencies on other systems, legacy applications that are not working with some new application, software, versions of hardware, and dependencies on vendors and other internal teams. In case when there are many vulnerabilities detected for one team within a short time period, there are usually prioritized the elimination of vulnerabilities, that can be hacked outside and that can have an impact on the company's customers.

The author received valuable feedback about the composition of the survey, which was considered in the final version of the survey setup. For example, the length of the survey seemed to be too long and a lot of statements in the Big Five assessment part required explanations. The newly added statements in HAIS-Q received positive feedback, especially the part about information classification.

4.2 Survey statistical data

Before data analysis, survey responses were examined to evaluate data quality. First, the researcher validated each returned survey response to ensure that all questions are answered. Next, responses were reviewed with the purpose to identify responses provided without due care. For this purpose, the recommendations of Meade and Craig [99] have been followed. For example, participants, who responded with the same response option (e.g. "Agree") to all questions, were excluded. On this basis, 27 responses were excluded, which resulted in a final sample of 111 company employees. Table 2 provides an overview of the demographic characteristics of the participants. It is classified by gender, age, and work experience. The gender split was a 40,5% females (n= 45) and 56,8% males (n=63), 3 respondents preferred not to answer. Based on the age, the age between 31 and 40 years are the majority of respondents, it has 38.8%, followed by 41 - 50 years has 30.6%. Most respondents had been working at the company for over 6 years (62,8%). More than 37 percent of participants have been working in their current position for the last 1 to 3 years.

Table 2. *Demography of respondents.*

Variable	**Category**	**Group 1**	**Group 2**	**Group 3**	**Total**
Responses	n	27	31	53	111
Gender Identity	Male	7	15	41	63
	Female	20	15	10	45

Continues...

Table 2 – *Continues...*

Variable	Category	Group 1	Group 2	Group 3	Total
	No answer	0	1	2	3
Age Group	20 and younger	0	0	0	0
	21 - 30	8	3	3	14
	31 - 40	6	13	24	43
	41 - 50	10	8	16	34
	51 - 60	3	6	9	18
	61 or older	0	1	1	2
Work experience at current employer	less than 1 year	4	4	6	14
	1 - 3 years	4	1	8	13
	4 - 6 years	3	4	7	14
	over 6 years	16	22	32	70
Work experience at current position	less than 1 year	9	8	8	25
	1 - 3 years	7	15	20	42
	4 - 6 years	6	4	8	18
	over 6 years	5	4	17	26

4.3 Reliability of the survey

The survey used by the author in this work consists of three assessment parts: 1) background information of respondent; 2) HAIS-Q; 3) personality traits. The second and third parts of the survey have largely been based on existing surveys which had been validated for their reliability. However, the author decided to update HAIS-Q with six additional statements to reflect such information security aspects as working at home and information classification. This means that the reliability of the modified survey tool needs to be re-assessed.

4.3.1 HAIS-Q

The second assessment part HAIS-Q consisted of 69 questions, which were divided into three sub-areas (Knowledge, Attitude, and Behaviour). The questions have positive and negative values to ensure the respondent understands the purpose and meaning of the questions.

The author has chosen Cronbach's alpha for reliability measurement because it is easy to use, as it only requires one test administration. Alpha was developed by Lee Cronbach in 1951 to provide a measure of the internal consistency of a test or scale. Cronbach's

alpha is computed by correlating the score for each scale item with the total score for each observation and then comparing that to the variance for all individual item scores [100]. Cronbach's alpha results normally stay between 0 and 1, with higher values indicating that the survey or questionnaire is more reliable.

Cronbach's alpha can be written as a function of the number of test items and the average inter-correlation among the items:

$$\alpha = (\frac{k}{k-1})(1-\frac{\sum_{i=1}^{k}\sigma_{y_i}^2}{\sigma_x^2})$$

Figure 6. *Cronbach's alpha calculation formula*

In the current study, Cronbach's alpha for the HAIS-Q assessment part is 0.908. This value indicates that the combination of statements is reliable. The author has calculated Cronbach's alpha for the KAB survey components as well (see Table 3) Compared to the HAIS-Q survey performed by Parsons [64] the current study shows weaker correlations. Parsons reported Cronbach's alphas of 0.844, 0.884, and 0.918 for Knowledge, Attitude, and Behaviour, whereas scores obtained in the present study are 0.701, 0.828, and 0.770, respectively.

Table 3. *Cronbach's alpha for the KAB survey components*

Construct	**Cronbach's alpha**
Knowledge of policy and procedures	0.701
Attitude towards policy and procedures	0.828
Self-reported behaviour	0.770

The scores for the attitude and behavior constructs exceeded the recommended cut-off value of 0.7, which provides evidence of a high degree of reliability [101].

4.3.2 Big-Five inventory

A brief measure of the Big-Five personality dimensions has been criticized by some researchers, however, the 10-item measure has been evaluated and confirmed its validity. The instruments reached adequate levels in terms of (a) convergence with widely used Big-Five measures in the self, observer, and peer reports,(b) test-retest reliability, (c) patterns of predicted external correlates, and (d) convergence between self and observer

ratings [81]. A 10-item measure of the Big-Five dimensions is recommended for situations where very short measures are needed, although personality traits are not the primary topic of interest. This is exactly the case in this study.

4.4 The overall ISA level in the company

To examine the interconnectedness between the items used to create the three main constructs (knowledge, attitude, behavior), a Pearson product-moment correlation was conducted [102]. The author decided to use Pearson's correlation test to check the linear relation between two sets of data. That means that a change in one variable is associated with a proportional change in the other variable. For example, the Pearson correlation may be used to determine whether an increase in one focus area contributes to an increase in another focus area.

There was a significant positive relationship between several variables, that provides further support for the reliability of the HAIS-Q and provides justification for calculating ISA scores [55].

These correlations are shown in Tables 4, 5 and 6.

Table 4. *Pearson's Correlations for knowledge.*

Focus area	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1. Password management	–						
2. Email use	0.137	–					
3. Internet use	0.323***	0.266**	–				
4. Social Media use	0.189*	0.121	0.383***	–			
5. Mobile devices	0.237*	0.048	0.227*	0.338***	–		
6. Information handling	0.160	0.102	0.294**	0.230*	0.217*	–	
7. Incident reporting	0.189*	0.130	0.265**	0.199*	0.109	0.295**	–
* p < .05, ** p < .01, *** p < .001							

The Pearson's correlation for the knowledge dimension (Table 4) shows that the focus area of Internet use is more strongly related to Password management and Social Media use than to Email use. These three focus areas (Internet use, Password management, and Social Media) are closely connected and as result can be logically explained. In the majority of cases, Social media equates to the Internet, and the need to manage passwords is often associated with social media and Internet use. The strong relation in mentioned

areas means, that, for example, people who have good acknowledge of possible threats in the Internet area and know how to act in order to mitigate them, have also a good acknowledgment level in the Social media area. A strong relationship can be also noticed between Mobile devices and Social Media use focus areas.

In contrast with Pearson's correlation for knowledge, the correlation test for attitude shows that almost all focus areas are related to each other strongly enough. A lower relation has been noticed between Mobile devices and Email use, Incident reporting and Password management, and Email use and Incident reporting focus areas (see Table 5).

Table 5. *Pearson's Correlations for attitude.*

Focus area	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1. Password management	–						
2. Email use	0.307**	–					
3. Internet use	0.411***	0.421***	–				
4. Social Media use	0.338***	0.429***	0.390***	–			
5. Mobile devices	0.300**	0.213*	0.372***	0.501***	–		
6. Information handling	0.332***	0.378***	0.488***	0.446***	0.409***	–	
7. Incident reporting	0.222*	0.199*	0.384***	0.526***	0.425***	0.444***	–
* p < .05, ** p < .01, *** p < .001							

While in the Table 5 all focus areas are somewhat related to each other, it is interesting to see the correlation between Social media use and Email use as well as between Information handling and Incident reporting focus areas is shown as insignificant in the Table 6. That means that the behavior in these areas could be different. On the contrary, the relationship between Social Media use and Internet use is strong enough under all three constructs.

Table 6. *Pearson's Correlations for behavior.*

Focus area	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1. Password management	–						
2. Email use	0.138	–					
3. Internet use	0.291**	0.304**	–				
4. Social Media use	0.274**	0.163	0.450***	–			
5. Mobile devices	0.377***	0.284**	0.478***	0.381***	–		
6. Information handling	0.277**	0.214*	0.297**	0.359***	0.383***	–	
7. Incident reporting	0.294**	0.358***	0.272**	0.271**	0.349***	0.071	–

Continues...

Table 6 – *Continues...*

Focus area	**1**	**2**	**3**	**4**	**5**	**6**	**7**
* p < .05, ** p < .01, *** p < .001							

The HAIS-Q used in the survey as an instrument for measuring ISA assesses participants' present knowledge and attitude regarding cyber security topics, as well as their self-reported behavior patterns towards cyber security. The reason for measuring an individual's information security awareness using the knowledge-attitude-behavior module can be explained in the following way. Users can acknowledge the threats and even know how to act to mitigate the impact, but for some reason, they do not act correspondingly to their knowledge. The reason could be in their attitude or low motivation. There could be another case as well - the users can have enough motivation in securing themselves, but do not know how to act.

In order to get a wide overview of HAIS-Q results, the author composed the table with descriptive statistics. The table 7, demonstrates the means and standard deviations for each of the focus areas of the HAIS-Q of all 111 responses. Focus areas Mobile devices and Information handling differ from other areas by maximum possible value, as these include three statements more each.

Table 7. *Descriptive statistics for each focus area.*

Focus area	**Mean**	**SD**	**Min**	**Max**	**Max possible**
1. Password management	41.378	3.683	28	45	45
2. Email use	39.414	4.271	25	45	45
3. Internet use	38.973	4.546	26	45	45
4. Social Media use	38.730	4.094	27	45	45
5. Mobile devices	54.703	4.788	36	60	60
6. Information handling	53.523	4.624	36	60	60
7. Incident reporting	39.027	4.237	27	45	45

Respondents' scores were lowest for the Email use, Incident reporting, Internet, and Social Media use focus areas. A similar pattern, when these three areas had the lowest score, has noticed Mainar Swari Mahardika [103], who measured ISA among two groups at the Judicial Commission in the Republic of Indonesia. It was assumed that employees can use work computers for non-work-related purposes during working hours.

The highest scores were for the Password management and Mobile devices. The password management scores are inconsistent with the finding of Parsons [64], who has noticed improvements in this area in recent years. High scores for the Mobile devices focus area could be potentially related to the situation with a pandemic, as a significant number of workers started to work remotely on regular basis. In turn, the employer, to minimize the risks of the changed environmental conditions, prepared materials and ensured that employees are aware of the risks and well trained.

The ISA level in percentage terms through KAB dimensions is presented in the Table below:

Table 8. *ISA results of the whole sample.*

Focus area	**Knowledge**	**Attitude**	**Behaviour**	**Average**
1. Password management	93.0	90.3	92.5	92.0
2. Email use	81.6	92.6	88.6	87.6
3. Internet use	86.4	90.3	83.2	86.6
4. Social Media use	84.7	89.4	84.0	86.1
5. Mobile devices	91.3	92.0	90.3	91.2
6. Information handling	86.7	93.6	87.3	89.2
7. Incident reporting	85.6	89.4	85.1	86.7

Email use gets a low value on the knowledge dimension. According to received feedback from people who took part in the survey, there was confusion with statements about email use. For example, the statement "I am allowed to open email attachments from unknown senders." In most cases, the author believes that employees understand all consequences of opening an email attachment. The reflection was that most employees can expect email coming outside the company network, such as emails from customers and vendors, and it would be strange to say that they are not allowed to open any attachments from unknown senders.

Almost all focus areas, except Password management, have the highest value in the Attitude dimension. The attitude component is used to assess what participants think about guidelines that apply to each focus area. From Table 8 we can see that employees have a positive attitude towards guidelines. Knowledge and behavior are almost on the same level, which could mean that people behave according to their best knowledge.

To get the answer to the raised research question, that is stated as **"What is the overall ISA level in the examined company?"**, the Kruger's Scale of Information Security Awareness

Measurement [104],[105] was used, as it covers unique variance across several constructs and was the unique predictor of the number of long-term relationships [106]:

Table 9. *The Kruger's Scale of Information Security Awareness Measurement [104].*

Dimensions	**Weightings**
Knowledge	30
Attitude	20
Behaviour	50

Rules	**Weightings**
Adhere to policies	20
Keep password secret	20
Use e-mail/Internet with care	20
Careful with mobile equipment	10
Report security incidents	10
Actions carry consequences	20

The overall awareness level of the whole sample has been measured as 88%. This is a good level (80% - 100%) and indicates that no need for action. The total awareness level for each one of the three dimensions (knowledge, attitude, and behavior) has been measured as a good as well [104].

Before starting the comparison of ISA levels among different groups, the author decided to check whether there can be seen some trend between ISA levels and respondent's gender, age, and tenure. The average ISA scores were calculated for each category of the sample. The maximum possible points for the HAIS-Q part are 345.

Table 11. *ISA scores per each category.*

Variable	**Category**	**Total**	**ISA score**
Responses	n	111	305.8
Gender Identity	Male	63	305.0
	Female	45	306.2
	No answer	3	315.6
Age Group	20 and younger	0	-
	21 - 30	14	298.3
	31 - 40	43	308.2

Continues...

Table 11 – *Continues...*

Variable	**Category**	**Total**	**ISA score**
	41 - 50	34	303.2
	51 - 60	18	311.4
	61 or older	2	298
Work experience at current employer	less than 1 year	14	304.6
	1 - 3 years	13	308.8
	4 - 6 years	14	313.6
	over 6 years	70	303.9
Work experience at current position	less than 1 year	25	305.2
	1 - 3 years	42	306.3
	4 - 6 years	18	304.2
	over 6 years	26	306.7

From this comparable Table11 seen that there are no significant differences for ISA scores based on respondents' gender. In case of the age, there can be noticed that the respondents from the age group 21 -30 and 61 or older have the lowest scores. The highest scores are in the age group 51-60. Due to the unequable number of responses in each age group and no linear dependencies through all 5 groups (age group 20 and younger is not counted, as there are no responses from employees within this age group), the author considers these as no relationship between ISA scores and age. The author also tried to group five age groups into two (from 21 to 40 and from 41 to 61 and older). Calculation showed that these two groups have equal average ISA scores (305.8). The previous studies [4],[6] also reported mixed results of correlation between ISA scores, age, and gender.

It is good to mention the trend that can be seen between the groups separated based on work experience at the current employer. It can be seen that people who work at the organization, based on which example the author does a case study, from 4 to 6 years have the highest average ISA scores.

There has not seen any trend in work experience at the current position. However, the author decided to re-group these 4 groups into three, as less than 1 year, from 1 to 6 years, and over 6 years, and check possible correlation with ISA and other variables. Such groups the author decided to compose and test due to personal experience and impression, that level of stress and involvement in work could be different when an employee works for less than a year and more than 6 years. The correlation test shows an interesting relationship, namely, the re-grouped work experience at the current position is positively related to the

groups (r(109)=0.206, p<0.05). That would mean that employees in the Group 3 have worked in their current position longer than employees in Group 1 and Group 2.

4.5 HAIS differences per main three groups

In order to test whether the differences in means between the three groups are meaningful in relation to the information security awareness level, the paired-samples t-Test was conducted. As a reminder, the RQ2 was stated to determine whether employees who are more involved in risk management procedures more aware of information security than the employees from business units and IT-related employees. First, in order to clarify whether the difference between these groups is meaningful enough, the author carried out a paired-samples t-Test. The paired sample test is chosen as it is more powerful than the independent sample t-Test and it is better able to find differences that exist, even in small samples.

The null-hypothesis was defined as:
H0-21: People in Group2 and Group3 not having a meaningful difference in terms of ISA.
H0-23: People in Group2 and Group1 not having a meaningful difference in terms of ISA.

Preliminary data screening showed that scores began to deviate from normality but not sufficiently to warrant transforming the data, Shapiro-Wilk test (p>0.005). Assumption test use p<.01 or p<.001, thus, it is non-significant for all pairs, indicating that the distributions are not different than a normal curve (see Table 12).

Table 12. *Test of Normality (Shapiro-Wilk).*

			W	p
Group2	-	Group1	0.880	0.005
Group2	-	Group3	0.932	0.049

The mean for Group 2 (M=307.7, SD=16.7) was not significantly different than Group 1 (M= 301.6, SD=20.2) and Group3 (M=306.8, SD=24.2). The Table 13 below shows that the t-test values are 1.031 and 0.057, that do not exceed critical values CV(26)=+/-2.0555 and CV(30)=+/-2.0423 respectively. The t-test value should either be smaller than the negative "t-Critical two-tail" or larger than the "t-Critical two-tail". We can also see that the significance values for our t-tests are 0.312 and 0.955, which are large than .05.

Table 13. *Paired Samples T-Test.*

Measure 1		Measure 2	t	df	p
Group2	-	Group1	1.031	26	0.312
Group2	-	Group3	0.057	30	0.955

All these findings tell us that the means of these pairs of groups do not differ statistically significantly. These do not support the idea that people in Group 2 are more aware of information security than people in Group 1 and Group 3.

In order to calculate the ISA scores for each group and check the distribution of scores over KAB dimensions and seven focus areas, the author calculated average percent values, which are presented in Table 14.

Table 14. *ISA results of Group 1.*

Focus area	**Knowledge**	**Attitude**	**Behaviour**	**Average**
1. Password management	91.1	88.9	91.6	90.5
2. Email use	82.5	90.6	86.9	86.7
3. Internet use	85.4	86.2	84.2	85.3
4. Social Media use	83.5	89.1	84.0	85.5
5. Mobile devices	92.0	94.4	92.2	92.9
6. Information handling	83.5	91.3	85.4	86.7
7. Incident reporting	79.3	87.9	80.7	82.6

The higher scores in Group 1 belong to the Mobile devices focus area. It came as a surprise to the author. The reason behind this could be the fact that employees from this group are mostly directly or indirectly working with customers and terms of privacy and confidentiality they know like no one else. The focus area of Incident reporting on the contrary has fewer scores. This could be related to the fact that employees of this group are less involved in such processes as incident management. The people in Group 1 are usually reporting incidents, while people from Group 2 and Group 3 are also part of these reported incident solving and mitigation. This assumption is also reflected in the results of Incident reporting for Group 2 and Group 3 (see Tables 15,16).

Table 15. *ISA results of Group 2.*

Focus area	**Knowledge**	**Attitude**	**Behaviour**	**Average**
1. Password management	93.3	91.6	91.4	92.1

Continues...

Table 15 – *Continues...*

Focus area	**Knowledge**	**Attitude**	**Behaviour**	**Average**
2. Email use	77.6	95.1	88.8	87.2
3. Internet use	87.7	92.5	83.2	87.8
4. Social Media use	84.1	88.4	83.4	85.3
5. Mobile devices	91.9	92.1	89.0	91.0
6. Information handling	91.1	96.5	87.1	91.6
7. Incident reporting	88.4	89.7	85.6	87.9

There are three focus areas in Table 15 that have percentage scores higher than 91%. These are Password management, Mobile devices, and Information handling. The weakest point of the Group 2 is the Social Media use, which had three sub-areas:

1. Social Media privacy settings
2. Considering consequences
3. Posting about work

The same trend is valid for Group 3 as well, which can be seen in the Table 16 below:

Table 16. *ISA results of Group 3.*

Focus area	**Knowledge**	**Attitude**	**Behaviour**	**Average**
1. Password management	93.8	90.3	93.6	92.6
2. Email use	83.4	92.1	89.4	88.3
3. Internet use	86.0	91.1	86.2	86.6
4. Social Media use	85.8	90.2	84.4	86.8
5. Mobile devices	90.6	90.8	90.1	90.5
6. Information handling	85.7	93.2	88.4	89.1
7. Incident reporting	87.3	90.1	87.0	88.1

To have all final ISA scores consistent, the author applied the Kruger's Scale [104] here as well. The results are shown in the Table 17 below:

Table 17. *ISA results comparison.*

Group name	**Total score**
Group 1	87
Group 2	89
Group 3	89

The ISA scores of all three groups are in threshold 80 - 100, that according to Kruger [104], is considered Good. When asked why should the people in Group 3 have the same high scores as those in Group 2, the interviewees agreed that similarly to risk managers also the people in Group 3 might be more critical of information security as they are those who ensure that services are securely protected and IT risk management procedures are an integral part of their work.

4.5.1 Differences in ISA level per subgroups

The next research question that the author aimed to validate is **whether there can be found some correlation between the level of ISA and vulnerability management efficiency**. For this purpose, the author decided firstly to determine the level of information security awareness in sub-groups of Group 3: Top Target Met and Top Target Missed. We received 26 responses from people in the group Top Target Mat and 25 responses from the group Top Target Missed. The people, who were in both groups, are excluded from this analysis. The size of the subgroups are almost equal, however, there are more males than female. This could be explained by the fact, that all over the world men outnumber women in the IT engineering industry. The age distribution is also unexpectedly similar. In terms of tenure, these subgroups seem to be substantially similar as well (see Table 18).

Table 18. *Demography of subgroup respondents.*

Variable	**Category**	**Top Target Met**	**Top Target Missed**	**Total**
Responses	n	26	25	51
Gender Identity	Male	19	20	39
	Female	7	3	10
	No answer	0	2	2
Age Group	20 and younger	0	0	0
	21 - 30	3	0	3
	31 - 40	12	12	24
	41 - 50	7	8	15
	51 - 60	4	4	8
	61 or older	0	1	1
Work experience at current employer	less than 1 year	4	2	6
	1 - 3 years	2	6	8
	4 - 6 years	5	2	7
	over 6 years	15	15	30

Continues...

Table 18 – *Continues...*

Variable	**Category**	**Top Target Met**	**Top Target Missed**	**Total**
Work experience at current position	less than 1 year	6	2	8
	1 - 3 years	8	12	20
	4 - 6 years	6	1	7
	over 6 years	6	10	16

Using a similar approach, the author conducted a paired samples t-Test to determine whether employees in Top Target Met group are more aware of information security than the employees in Top Target Missed group. Thus, the null-hypothesis was defined as:
H0: People in Top Target Met Group and Top Target Missed Group not having a meaningful difference in terms of ISA.

Preliminary data screening (see Table 19) showed that scores began to deviate from normality but not sufficiently to warrant transforming the data, Shapiro-Wilk test (p>0.05).

Table 19. *Test of Normality (Shapiro-Wilk).*

			W	p
Top Target Met	-	Top Target Missed	0.920	0.051

The mean for Top Target met Group (M=308.9, SD=25.6) was not significantly different than Top Target Missed Group (M= 304.5, SD=23.9). From Table 20 we can also see that the significance value for our t-test is 0.613, which are large than .05, which indicates that t-test was not significant. The t-test value is 0.512, that does not exceed critical value CV(24)=+/-2.0639.

Table 20. *Paired Samples T-Test.*

Measure 1		Measure 2	t	df	p
Top Target Met	-	Top Target Missed	0.512	24	0.613

These findings tell us that the means of this pair do not differ statistically significantly. Thus, this do not support the idea that people in Top Target Met Group are more aware of information security than people in Top Target Missed Group.

4.6 Personality differences

Further, the author focuses on personality differences and aimed to analyze how the sample can be characterized and whether there can be found some personality traits are more typical for the employees in each of the selected groups.

In order to find the factor that contributes to the level of information security awareness, the author analyzed respondents' age, gender, job experience, and Big Five inventory results gathered in the third assessment part of the survey.

Firstly, the author calculated average percent scores for each personality trait. The present study used the Ten-Item Personality Inventory (TIPI). This measure consists of 10 items each using 5-point ratings (Disagree strongly = 1 to Agree strongly = 5). Each personality trait, namely, Agreeableness, Conscientiousness, Extroversion, Openness, and Emotional stability is represented by two items. A measure for each trait is calculated as the sum of the scores for the two relevant items. This abbreviated method of measuring personality traits was considered adequate and appropriate for an exploratory study of this nature because it consumed much less time to complete than longer versions of the BFI [22].

As is shown in the figure 7, the conscientiousness dimension has the highest score. A high score of conscientiousness has been shown to relate to high work performance [79].

Agreeableness, extroversion, and openness to experience have a moderate score. Personality traits should be assessed as ranked on a scale between the two extreme ends. These could be read as that the respondents are more inclined to be helpful, cooperative (agreeableness), outgoing, sociable (extroversion), and curious, independent (openness to experience). The neuroticism dimension is, on the contrary, scaled quite low (36%), which shows that people who participated in the survey are emotionally stable.

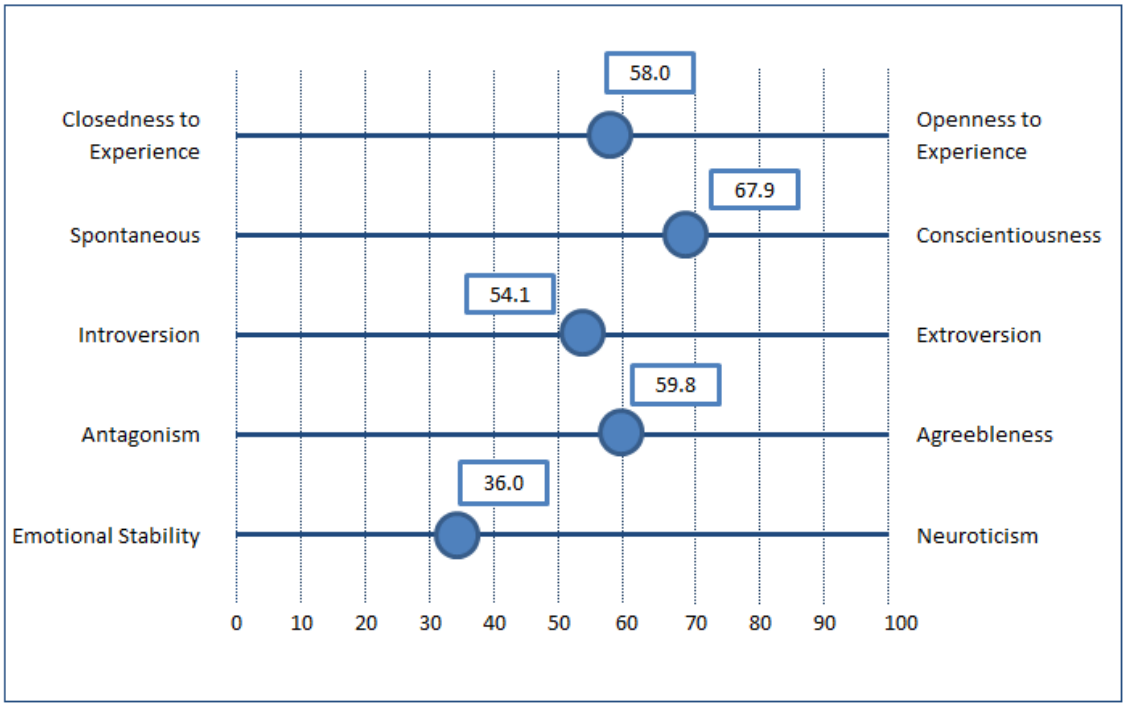

Figure 7. *The Big Five results of survey respondents (composed by author).*

To test the relationship between personality traits, the author run Pearson's correlation test. The result of this is shown in the Table 22. It can be noticed that the conscientiousness dimension has a negative relation to neuroticism. This should mean that people who are higher in conscientiousness, are more emotionally stable, and vice versa.

Table 21. *Pearson's Correlations.*

Variable		O	C	E	A	N
1. O	Pearson's r	–				
	p-value	–				
2. C	Pearson's r	0.113	–			
	p-value	0.239	–			
3. E	Pearson's r	−0.071	0.073	–		
	p-value	0.457	0.449	–		
4. A	Pearson's r	−0.004	−0.039	0.147	–	
	p-value	0.970	0.683	0.124	–	
5. N	Pearson's r	−0.019	-0.247**	−0.162	−0.062	–
	p-value	0.845	0.009	0.089	0.519	–

* p < .05, ** p < .01, *** p < .001

Next, the author decided to check whether there is some correlation between ISA scores and personality traits.

Table 22. *Pearson's Correlation for ISA scores and OCEAN.*

			Pearson's r	p
O	-	ISA	0.191*	0.045
C	-	ISA	0.183	0.054
E	-	ISA	0.055	0.568
A	-	ISA	0.078	0.414
N	-	ISA	−0.060	0.533

* p < .05, ** p < .01, *** p < .001

From Table 22 can be seen, that Openness was positively related to ISA, r(109)=0.191, p<0.05. That could mean that people who are high in openness traits have more high ISA scores. Because the ISA score consists of the sum of scores for seven focus areas, the author also tested the correlation between personality traits and ISA focus areas. Due to the significant number of pairs, the author decided to leave in the Table 23 only correlated pairs, where p<0.05 or less.

Table 23. *Pearson's Correlations for ISA focus areas and OCEAN.*

			Pearson's r	p
O	-	Internet use	0.273**	0.004
C	-	Email use	0.199*	0.037
C	-	Internet use	0.193*	0.043

* p < .05, ** p < .01, *** p < .001

In order to get an answer to the fourth research question (RQ4) and found what factors can contribute to the efficiency of vulnerability management, we decided to test our expectations that are rooted in the literature. It was assumed that conscientiousness and agreeableness can influence the effectiveness of vulnerability management. As result, two hypotheses have been raised:

H1: Employees with high Conscientiousness scores are more likely to deal with vulnerabilities more effectively.
H2: Employees with high Agreeableness scores are more likely to deal with vulnerabilities more effectively.

The paired samples t-Test has been conducted to test two hypotheses at once. The mean for Top Target met Group was not significantly different than Top Target Missed Group for both cases - when checking Conscientiousness scores and Agreeableness scores (see Table 24).

Table 24. *Descriptives.*

	N	Mean	SD	SE
Top Target Met-A	26	7.269	1.079	0.212
Top Targer Missed - A	25	7.000	1.258	0.252
Top Target Met-C	26	7.231	1.366	0.268
Top Targer Missed - C	25	7.640	1.350	0.270

The t-test critical value for these pair samples is +/-2.0639. The Table 25 below shows that t-test values do not exceed critical value and that the significance values for our t-test h are large than .05 (0.584 for agreeableness and 0.339 for conscientiousness). Thus it can be concluded that there are no significant difference between these two groups in means of two personality traits conscientiousness and agreeableness.

Table 25. *Paired Samples T-Test.*

Measure 1		Measure 2	t	df	p	Cohen's d
Top Target Met-A	-	Top Targer Missed - A	0.555	24	0.584	0.111
Top Target Met-C	-	Top Targer Missed - C	−0.975	24	0.339	−0.195

Thereby the two raised hypotheses have not been accepted on the example of this study.

Further, with the purpose to check the distribution of ISA scores, points for seven focus areas are summed up. The minimum value among the whole sample is 209 and the maximum is 341 from the maximum possible 345. Consequently, the higher an aggregated score, the better awareness the participant was likely to have. Only 8 respondents had scores less than 276, that is 80% if transmit scores to percentage. From the picture 8 below, it can be noted that the scores of the majority of the ISA survey correspondents lie on the range of 300 to 320.

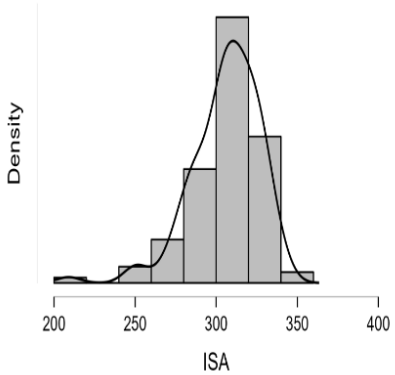

Figure 8. *ISA score distribution plots.*

In order to test whether there are differences in personality traits between people with high

and low scores, the author decided to divide all responses into 4 groups by ISA points. The idea is to have in each group more or less the same number of responses for comparison. In this way, the author composed the following groups and calculated the average percentage for all 5 personality dimensions OCEAN (see Table 26):

Table 26. *Responses grouped by ISA scores.*

Score range	**N**	**Scores Mean**	**O**	**C**	**E**	**A**	**N**
1. From 209 to 292	28	277.7	62.5	70.7	61.4	63.2	51.4
2. From 293 to 308	28	302.8	66.1	75.7	67.9	71.4	46.4
3. From 309 to 321	27	314.5	69.6	73.7	61.5	69.3	50.4
4. From 322 to 341	28	328.8	67.5	77.1	62.1	67.5	47.1

The author has been most interested to compare the results of the group with scores from 209 to 292 and the group with the highest scores (from 322 to 341).

When looking at the conscientiousness dimension, it can be seen that the groups with higher ISA scores have a significantly higher level of this dimension than the group with the lowest scores. Highly conscientious people tend to have thoughtfulness and goal-directed behaviors. These people are organized, and mindful of details and deadlines [107]. This explanation seems to be relevant that people with a high level of information security awareness pay more attention to details and think about how their behavior could affect others.

Openness to experience is one more personality trait in the Table 26 that attracts attention. It has a lower percentage score for the group with lower ISA values. This trait features characteristics such as imagination and creativity. People who are high in this trait tend to be eager to learn new things and enjoy new experiences. People low in this trait are often much more traditional and may struggle with abstract or theoretical concepts [107]. Although all four groups have quite high values (more than 60%), there can be noticed some difference among the groups. Especially this can be explained in the information security area, as the people in this area should be able quickly to adapt to changes and newly introduced challenges.

In terms of the agreeableness trait, the same as for the conscientiousness and openness to experience, the first group in the Table 26 has a lower percentage score than the other three groups. The agreeableness was examined in correlation to job performance and was found that it is negatively related to individual pro-activity [108]. That means that agreeableness

people are better to perform when working in teams. Agreeableness can be described as a tendency of being cooperative, trusting, and helpful nature [107]. This could, for example, mean that people, who are high in agreeableness, are more likely not to report suspicious co-worker behavior.

Meanwhile, it is interesting to note that the group with the lowest ISA scores has the higher percentage scores compared to the other three groups in the neuroticism dimension. This could be related to the stress level people experience in this group. However, the values of all these groups are somewhere in the middle of the scale.

The author aimed also to analyze what individual characteristics are more typical for each group. Further, the author decided to make a more detailed review of personality traits and check the relationship between traits and respondent gender, age, belonging to a group, and ISA scores.

4.6.1 Conscientious

As was mentioned previously, highly conscientious people tend to be more organized, enjoy having a set schedule, and finish important tasks right away [107]. Considering this definition, we could make an assumption, that the level of conscientiousness could be one of the factors, why some groups of people are more strict to follow deadlines and others are not. There was used a 5-point Likert scale for the Big Five assessment. That means that people who answered two conscientious statements as "Strongly agree" and "Agree" or for reverse statement accordingly "Strongly disagree" and "Disagree", should in total have scores from 8 to 10. These responses were collected in the group where conscientiousness is high. The responses with the rest scores were grouped into a separate group.

Table 27. *Responses grouped per conscientious scores.*

Variable	**Category**	**Group with high C (%)**	**Group with low C (%)**
N		57	52
ISA scores	Mean	307.9	303.3
Gender Identity	Male Female No answer	28 (45.9%) 28 (62.2%) 1 (33.3%)	33 (54.1%) 17 (37.8%) 2 (66.7%)
Age Group	21 - 30 31 - 40 41 - 50	6 (42.9%) 24 (55.8%) 19 (57.6%)	8 (57.1%) 19 (44.2%) 14 (42.4%)

Continues...

Table 27 – *Continues...*

Variable	Category	Group with high C (%)	Group with low C (%)
	51 - 60	8 (47.1%)	9 (52.9%)
	61 or older	0 (0%)	2 (100%)
Group	Group 1	13 (48.1%)	14 (51.8%)
	Group 2	20 (64.5%)	11 (35.5%)
	Group 3 - Top Target Met	12 (46.2%)	14 (53.8%)
	Group 3 - Top Target Missed	12 (48%)	13 (52%)

Table 27 above shows that the author's assumption, that Group 3 two subgroups could have differences in the level of conscientiousness, has not found confirmation. The distribution among groups is not significantly different, people from subgroup Top Target Met and Top Target Missed are presented in both conscientious groups in almost equal numbers. This result has been confirmed by paired t-test presented in this chapter earlier.

However, it can be noticed that female distribution per group is different: 62.2% of females are part of the group with a high level of conscientiousness. The same trend is shown for Group 2 as well.

It is also not worse to mention that the mean value for ISA is higher in the group with a high conscientious level.

4.6.2 Agreeableness

Using the same logic and approach as in the analysis part conscientious, the author composed the table for the agreeableness trait (see Table 28).

Table 28. *Responses grouped per agreeableness scores.*

Variable	Category	Group with high A (%)	Group with low A (%)
N		41	68
ISA scores	Mean	307.8	304.5
Gender Identity	Male	21 (34.4%)	41 (65.6%)
	Female	19 (42.2%)	26 (57.8%)
	No answer	1 (33.3%)	2 (66.7%)
Age Group	21 - 30	5 (35.7%)	9 (64.3%)

Continues...

Table 28 – *Continues...*

Variable	Category	Group with high A (%)	Group with low A (%)
	31 - 40	15 (34.9%)	28 (65.1%)
	41 - 50	11 (33.3%)	22 (66.7%)
	51 - 60	10 (58.8%)	7 (41.2%)
	61 or older	0 (0%)	2 (100%)
Group	Group 1	7 (25.9%)	20 (74.1%)
	Group 2	9 (29%)	22 (71%)
	Group 3 - Top Target Met	14 (53.8%)	12 (46.2%)
	Group 3 - Top Target Missed	11 (44%)	14 (56%)

The respondents' distribution among these two groups was 41 and 68. The majority of employees from the Group 1 and Group 2 have low agreeableness scores. Because there are more women than men in the Group 1, the male and female ratio in the Group 2 is equal, it could be assumed the relation to gender belonging. However, this is in contradiction to Soto finding [109] that on average females at each age are somewhat more agreeable and altruistic, than males.

4.6.3 Openness to experience

Table 29. *Responses grouped per openness scores.*

Variable	Category	Group with high O (%)	Group with low O (%)
N		24	85
ISA scores	Mean	311.3	304.2
Gender Identity	Male	16 (26.2%)	45 (73.8%)
	Female	7 (15.6%)	38 (84.4%)
	No answer	1 (33.3)	2 (66.7%)
Age Group	21 - 30	7 (50%)	7 (50%)
	31 - 40	2 (4.7%)	41 (95.3%)
	41 - 50	15 (45.5%)	18 (54.5%)
	51 - 60	0 (0%)	17 (100%)
	61 or older	0 (0%)	2 (100%)
Group	Group 1	7 (25.9%)	20 (74.1%)
	Group 2	6 (19.4%)	25 (80.6%)
	Group 3 - Top Target Met	4 (15.4%)	22 (84.6%)

Continues...

Table 29 – *Continues...*

Variable	Category	Group with high O (%)	Group with low O (%)
	Group 3 - Top Target Missed	7 (28%)	18 (72%)

The distribution of responses for openness to experience is heterogeneous. However, it should be noted that the ISA average score is very good (311.3) for the people who are more open to experience. This was also confirmed by the correlation test described earlier in this chapter.

4.6.4 Extroversion

Similarly to the Table 29 for Openness to experience, there are only 27 respondents from 109, who were high in extroversion. It was found that extroversion is closely related to risk-taking behavior. For example, according to Pattinson [4] there was found higher InfoSec behavior among individuals who scored high on extroversion and openness. Especially this was noticed for behavior against phishing emails.

Due to heterogeneous distribution among groups, it is hard to find any correlation based on the data in this table.

Table 30. *Responses grouped per extroversion scores.*

Variable	Category	Group with high E (%)	Group with low E (%)
N		27	82
ISA scores	Mean	308.4	304.9
Gender Identity	Male	14 (23%)	47 (77%)
	Female	13 (28.9%)	32 (71.1%)
	No answer	0 (0%)	3 (100%)
Age Group	21 - 30	1 (7.1%)	13 (92.8%)
	31 - 40	8 (18.6%)	35 (81.4%)
	41 - 50	11 (33.3%)	22 (66.7%)
	51 - 60	7 (41.2%)	10 (58.8%)
	61 or older	0 (0%)	2 (100%)
Group	Group 1	5 (18.5%)	22 (81.5%)
	Group 2	7 (22.6%)	24 (77.4%)
	Group 3 - Top Target Met	8 (30.8%)	18 (69.2%)

Continues...

Table 30 – *Continues...*

Variable	Category	Group with high E (%)	Group with low E (%)
	Group 3 - Top Target Missed	7 (28%)	18 (72%)

4.6.5 Neuroticism

There are only six individuals with high neuroticism in the Table 31. Neuroticism is a trait that is usually characterized by sadness, moodiness, and emotional instability [109], while Russell reported that there is a correlation between neuroticism and secure cyber behaviors [28]. He found that as neuroticism increased, cybersecurity behaviors decreased. It was explained such as that a high level of stress might limit the mental resources required to maintain secure cyber behaviors. The correlation test performed earlier in this chapter also showed a negative correlation between ISA scores and neuroticism. However, this can not be confirmed by the figures in the table below.

Table 31. *Responses grouped per neuroticism scores.*

Variable	Category	Group with high N (%)	Group with low N (%)
N		6	103
ISA scores	Mean	307.3	305.6
Gender Identity	Male	4 (6.6%)	57 (93.4%)
	Female	2 (4.4%)	43 (95.5%)
	No answer	0 (0%)	3 (100%)
Age Group	21 - 30	0 (0%)	14 (100%)
	31 - 40	3 (7%)	40 (93%)
	41 - 50	1 (3%)	32 (97%)
	51 - 60	2 (11.8%)	15 (88.2%)
	61 or older	0 (0%)	2 (100%)
Group	Group 1	0 (0%)	27 (100%)
	Group 2	3 (9.7%)	28 (90.3%)
	Group 3 - Top Target Met	1 (3.8%)	25 (96.2%)
	Group 3 - Top Target Missed	2 (8%)	23 (92%)

4.7 ISA Predictors

In order to answer RQ5, this study posits the following hypotheses:

H3: Human age is negatively associated with ISA
H4: Men are more information security aware than women
H5: Conscientiousness is positively associated with ISA
H6: Agreeableness is positively associated with ISA
H7: Openness is positively associated with ISA
H8: Neuroticism is negatively associated with ISA
H9: Extraversion is positively associated with ISA

Nine multiple regressions were run to determine whether collected variables could predict level of information security awareness. The only model that showed statistically significant relationship was for the regression of Openness against ISA (p=0.045; p<0.05). Full summaries of the results are presented in Table 32.

Table 32. *Model Summary Results of Level Big Five Personality Traits Analyses.*

Group name	**Total score**
Model 1: Age, ISA	F(1,109)=0.656, p=0.420 (p>0.05); R=0.077, $R^2 = 0.006, R^2adj = -0.003$
Model 2: Gender, ISA	F(1,109)=0.391, p=0.533 (p>0.05); R=0.060, $R^2 = 0.003, R^2adj = -0.006$
Model 3: General Tenure, ISA	F(1,109)=0.319, p=0.574 (p>0.05); R=0.054, $R^2 = 0.006, R^2adj = -0.003$
Model 4: Position Tenure, ISA	F(1,109)=0.016, p=0.898 (p>0.05); R=0.012, $R^2 = 0.000, R^2adj = -0.009$
Model 5: Openness, ISA	F(1,109)=4.117, p=0.045 (p<0.05); R=0.191, $R^2 = 0.036, R^2adj = 0.028$
Model 6: Conscientiousness, ISA	F(1,109)=3.794, p=0.054 (p>0.05); R=0.183, $R^2 = 0.034, R^2adj = 0.025$
Model 7: Extraversion, ISA	F(1,109)=0.329, p=0.568 (p>0.05); R=0.055, $R^2 = 0.003, R^2adj = -0.006$
Model 8: Agreeableness, ISA	F(1,109)=0.673, p=0.414 (p>0.05); R=0.078, $R^2 = 0.006, R^2adj = -0.003$
Model 9: Neuroticism, ISA	F(1,109)=0.392, p=0.533 (p>0.05); R=0.060, $R^2 = 0.004, R^2adj = -0.006$

The strength of the correlation between openness and ISA was fairly weak, and statistically significant (R=0.191;p=0.045; p<0.05). Openness contributed 3.6% of the variance in ISA ($R^2 = 0.036$).
When adjusted, this contribution amounted to 2.8% ($R^2adj = 0.028$). The openness trait added statistically significantly to the prediction of ISA, F(1,109)=4.117, p=0.045 (p<0.05); R=0.191, $R^2 = 0.036$. There was a positive relationship between openness and ISA such that for each unit increase of the openness trait, ISA increases by about 3.5 points. Thus. Hypothesis seven (H7), which stated that Openness is positively associated with ISA, was supported.

The strength of the correlations between all other eight predictors and ISA was weak (from 0.012 to 0.183), and statistically non-significant (p>0.05). Therefore, hypotheses from H3 to H6 and H8, H9 were not supported.

5. Results

This chapter brings out key results and discusses answers to research questions. The main analysis has presented in the previous section. This also includes Research limitations, that discuss methodological approaches and challenges.

In this research, the questions were created based on previously validated tools, such as HAIS-Q and the Big Five personality test. The HAIS-Q has been complemented by 6 additional statements following the initial questionnaire construct. In terms of the Big Five test, based on the received feedback from people who participated in the interview, it was decided to use a ten-item long version, which reliability was validated in the previous research [81]. The reliability and validity of these two mentioned instruments have long been established in prior research. However, since the HAIS-Q tool has been adjusted, it became necessary to re-assess in terms of reliability. The adjusted HAIS-Q construct has been validated with 11 people from 4 groups. The sample size and group used for validation are relatively small, as result, the validation of newly added questions to an existing and published questionnaire is challenging. However, due to environmental changes and the fact that remote working and information classification were not covered in the existing tools, the author still sees that this methodology is appropriate. The sample size limitation is covered in the Limitation section.

The survey responses were analyzed using different techniques:
1. The reliability analysis of the HAIS-Q has been performed using Cronbach's alpha. By performing this analysis, we expected to find a good reliability level of the survey and compare these results with previous research reliability test results.
2. A descriptive analysis (Mean, Standard Deviation) of the sample and selected groups of the sample. Descriptive statistics were used to obtain a general summary of the data and the main variables of interest.
3. Pearson's correlation analysis to determine and explain the statistical differences in the whole sample and the selected groups.
4. Paired samples t-Test to examine the difference between population means for a set.
5. Multiple Linear Regression to determine the variation of the model and the relative contribution of each independent variable in the total variance.

The Cronbach's alpha, which was used for reliability measurement, indicates that the combination of HAIS-Q statements is reliable (0.908). The calculated Cronbach's alpha for the KAB survey components shows weaker correlations than these were in the comparative study, performed by Parson [64]. However, The scores for the attitude and behavior constructs exceeded the recommended cut-off value of 0.7, which provides evidence of a high degree of reliability [101].

This research work aimed to find answers to five research questions. The first research question was **"What is the overall ISA level in the examined company?"** The impression, that author got during the interview with people from selected groups, was that the overall level of information security could be slightly higher than average, or 6 points from a possible 10. The interviewees rated ISA in different groups based on their personal experiences and feeling. In general, all participants feel that their level and the level in the team should be higher than the overall level in the organization. The responses collected during the interview should be considered in terms of social desirability bias, which is mentioned in Section 4.1 and described in the Limitation section. However, the data obtained from the interviews to not have any effect on this study's results.

The survey results have not confirmed this notion. The calculation of the ISA score shows that the ISA for all seven focus areas is on a high level - the scores are in the range from 86.6% to 92.0%, where the lowest belongs to Social Media use and the highest to Password management focus area.

The social media focus area correlates with the content posted by the user. This could be related to the prevalence of at-home workers attributed to the Covid-19 pandemic. The employees at home might have more opportunities to engage in social media activities [21]. While overall social media usage is in the 80% to 100% range, which considers "good" on the Kruger scale [104], there are some options for improvement. For example, training that includes role-playing in risky IS behaviors might be beneficial to companies [21].

The second research question was formulated as **"Are the employees who are more involved in risk management procedures more aware of information security than the employees from business units and IT-related employees?"** The initial expectation was that employees in Group 2, who are more in risk management procedures, could perceive information security culture more positively than employees in two other groups reviewed in the present study. The author recognizes that security is everyone's business and everyone is responsible to report the risk in case of such identification. Nevertheless, the idea was that risk managers, information security managers, and people from the vulnerability management team deal with information security issues on daily basis. Their

job role involves identifying and assessing various types of risks that might affect the business. They are involved in the strategy design to identify what could go wrong and its impact on the business.

The employees in the Group 1 are people from business units, who work with customers. The author's impression is that this group of people could have more focus on privacy topics and some essential information security subjects could be brought to the secondary plan. The author is convinced, that the third group, who mostly consists of IT service owners, has a very good acknowledgment of possible threats and their impact on running the business. Everyone in the company shares common goals of protecting data, devices, and people, but various groups have a focus on different issues and could use very different approaches.

A paired samples t-Test was conducted to determine whether the differences in means between the three groups are meaningful in relation to the information security awareness level. The null-hypotheses were stated as:
H0-21: People in Group2 and Group3 do not have a meaningful difference in terms of ISA.
H0-23: People in Group2 and Group1 do not have a meaningful difference in terms of ISA
T-test findings tell us that the means of this pair do not differ statistically significantly. These do not support the idea that people in Group 2 are more aware of information security than people in Group 1 and Group 3.

The third research question was stated as **"Are there some correlations between the level of ISA and vulnerability management efficiency?"**. The author has analyzed the gathered data in order to calculate the ISA score for two groups, which consist of employees of IT units. These employees are service owners or assigned persons for one or more IT services and respectively responsible for keeping these services secure. Using extracted statistical data from the company's vulnerability management system, the author composed 2 groups based on historical data on vulnerability elimination speed. Further, the ISA scores have been calculated for each group.

It turned out, that ISA scores calculated for these two groups do not differ statistically significantly. This was tested by paired sample t-Test and the results are confirmed by ISA scores obtained according to Kruger's Information Security Awareness scale (88% and 89% accordingly). Since the difference is not statistically significant, the author would conclude that the efficiency of vulnerability management doesn't depend on the ISA level of the individuals involved in the vulnerability elimination process.

Nevertheless, this doesn't exclude any other factor, that could affect the vulnerability management efficiency. The other possible factors have been reviewed under the fourth research question **" What factors can contribute to the efficiency of vulnerability management?"**

To answer this question, the author analyzed all available data, such as age, gender, tenure at the current employer, and the current position. The trend all over the world shows that males outnumber women in the IT engineering industry. This was also the case for this group. The age distribution among the two groups was unexpectedly similar and gives no reason to conclude that the employee's age could somehow be a contributing factor to vulnerability management efficiency. In terms of tenure, the author hasn't revealed any interesting trends.

Additionally, it was decided to analyze personality traits and check whether one of the groups includes individuals, who are more organized, goal-directed, open to new experiences, or emotionally stable. In order to get an answer to the fourth research question (RQ4) and found what factors can contribute to the efficiency of vulnerability management, we decided to test our expectations that are rooted in the literature. It was assumed that conscientiousness and agreeableness can influence the effectiveness of vulnerability management. As result, two hypotheses have been raised:

H1: Employees with high Conscientiousness scores are more likely to deal with vulnerabilities more effectively.
H2: Employees with high Agreeableness scores are more likely to deal with vulnerabilities more effectively.

The paired samples t-Test has been conducted to test two hypotheses at once. The mean for Top Target met Group was not significantly different than Top Target Missed Group for both cases - when checking Conscientiousness scores and Agreeableness scores. The results showed that there is no significant difference between these two groups in means of two personality traits conscientiousness and agreeableness. Thereby the two raised hypotheses have not been accepted in the example of this study.

The fifth research question was **"What factors are associated with ISA? "** Based on reviewed previous research work results, it was expected that age, gender, and five personality traits are positively or negatively associated with ISA. Therefore, this study posits the following hypotheses:

H3: Human age is negatively associated with ISA

H4: Men are more information security aware than women
H5: Conscientiousness is positively associated with ISA
H6: Agreeableness is positively associated with ISA
H7: Openness is positively associated with ISA
H8: Neuroticism is negatively associated with ISA
H9: Extraversion is positively associated with ISA

Nine multiple regressions were run to determine whether collected variables could predict the level of information security awareness. The only model that showed a statistically significant relationship was for the regression of Openness against ISA ($p=0.045$; $p<0.05$). There was a positive relationship between openness and ISA such that for each unit increase of the openness trait, ISA increases by about 3.5 points. Thus, Hypothesis seven (H7), which stated that Openness is positively associated with ISA, was supported. Similar results in terms of Openness personality traits were reported by Pattinson and McCormac [22],[4],[110].

The strength of the correlations between all other eight predictors and ISA was weak (from 0.012 to 0.183), and statistically non-significant ($p>0.05$). Therefore, hypotheses from H3 to H6 and H8, and H9 were not supported.

In addition, the author checked how the whole sample can be characterized using OCEAN traits. It was revealed that participants can be described as cooperative, outgoing, and curious individuals. As the neuroticism dimension showed quite low results, it could be concluded, that the sample majority is emotionally stable. Also, using the Pearson's correlation test, it was indicated that neuroticism has a negative relation to the conscientiousness dimension. That means that more emotionally stable people are more efficient, organized, and goal-oriented. Interestingly, it turned out that the group with the lowest ISA scores has a higher level of neuroticism dimension. However, it should be mentioned, that the neuroticism level in all groups is moderate.

Interestingly, despite the relation between such personality traits, like agreeableness, conscientiousness, and ISA has not been statistically proven, the trend is seen when making a deeper look at figures. The figures show that the groups with higher ISA scores are higher in agreeableness, conscientiousness, and openness traits. This finding corresponds to Pattinson's research results, which showed that people who score low on extraversion and score high on agreeableness, conscientiousness, and openness are less likely to engage in risky information security behavior [90].

Our findings are in line with earlier studies that reported mixed results on factors, that

could predict the level of information security awareness.

5.1 Research limitations

The research has certain design and timing limits and the results above should be read in the context of possible limitations that the author is aware of.

This is one case study and research is limited to the one particular financial service provider that mainly operates in Baltic and Nordic countries. Since the study was based on specific inclusion and exclusion criteria, for example, specific vulnerability detection processes and tools used within one particular organization, the results cannot be generalized beyond all financial organizations. The composition of different nationalities among employees and cultural or social-economic differences could also produce a different outcome. Our recruiting methods may have produced a rather unique sample. Caution needs to be applied to derive conclusions as there may be hidden variables (skill level, education, previous working experience, etc) that have not been examined in the present study but could have stronger correlations. Thus, further research could examine if the findings of this study can be generalized to other samples and populations.

Another limitation, that should be considered, is the sample size. Some authors recommend a sample size between 100 and 400 participants [111]. The larger sample size increases statistical power and improves the generalization of the findings. The sample size used in our study (n=111) is closed to the minimum recommendation. Meanwhile, according to Roscoe [112] and Abranovic [113], the sample size in behavioral research should be larger than 30 and less than 500. We also agree with Martin's and Bateson's [114] point of view, that the more data collected the better. However, we do not envisage that a larger sample size would radically change the results [115]. The small size is also a limitation in terms of validation of the adjusted HAIS-Q instrument.

Third, the nature of our data collection should also allay the criticism of self-report. The self-reporting of the data may have biased the study in several ways. Since our data was collected online through a third-party website (Netigate), the results of this study may be limited by its use of Internet-based data collection. For example, Meade and Craig [99] believe that the lack of a controlled setting could result in environmental distraction and divided attention. The large standard deviation (of over 50 min) in the time taken to complete the HAIS-Q suggests that some part of participants may have been alternating survey completion with other work. Furthermore, it was not possible to check the truthfulness of answers [116]. Even though respondents were guaranteed anonymity of responses, people still could feel uncertain and choose self-favoring responses. Self-

reported data pose a risk to validity [117]. In addition, although the answers received during the interview do not affect the result of the current work, we should consider the probability of social desirability bias, when respondents answer the questions in a way that presents them in the best possible manner [118].

The language of the survey is also an important consideration because the wording may lead the respondent to favor one answer over another or they may be confused by the wording and select a random answer. Although it is recommended to use the Big Five test in the respondent's native language, the time pressure, and availability of reliable measurement tools have dictated to go with the English version. In addition, it was acknowledged that the English language level in the company is comprehensive, as it is an international company that uses English as a common business language. It should be also noticed, that due to the time constraints and received feedback, the ten-item tool has been used in this study, which results could be less comprehensive than when using the 44-item instrument. However, the 10-item measure has been evaluated and confirmed its validity earlier by several researchers. A 10-item measure of the Big-Five dimensions is recommended for situations where very short measures are needed, although personality traits are not the primary topic of interest. This is exactly the case in this study.

The recent information security training, that was mandatory for all employees might be a limitation for the present study as well. The author is aware of the forgetting curve, which shows that learned information slips out of our memories over time [119]. Taking into account that training took place at the end of January and the survey performed at the end of March, the obtained training materials could remain fresh in the mind.

6. Conclusion

This study aimed to examine and compare the levels of ISA among different groups within one financial institution. Given the vital role of employees in organizational security management, attention has recently been paid to understanding the factors influencing vulnerability management efficiency and employees' security perception.

HAIS-Q framework was chosen in this study to measure employees' ISA through the sampling method. User security awareness is critical to the overall security of any company. Information security awareness is a preventive measure that should be used to establish correct security principles and procedures in the minds of all employees. Knowing the IS awareness level allows employers timely detect and improve weaknesses. Information security awareness can be improved by providing various educational training, such as web-based training or mentoring training.

The most interesting finding was that all groups of people, examined in this study, had a good level of information security awareness. This shows that the effort put into security culture and information security awareness training seems convenient to all types of personalities. This might be validated in the future by assessing the level of ISA of newcomers and employees, who have been on an extended vacation.

This study showed that the efficiency of vulnerability management is not dependent on independent variables, such as age, gender, tenure, openness, conscientiousness, agreeableness, extroversion, and emotional stability. Given the limited scope of this research, other individual variables might be included for further investigation. It might be job satisfaction, educational level, or cultural factors.

The personality traits have been measured using the Big Five inventory tool. The personality dimensions of the Big Five have been observed across cultures and in many different measurement systems. They are the fundamental building blocks for describing personality. Each of the Big Five aspects has significant validity and reliability, making them extremely valuable for a business that wants to evaluate potential new hires or make a hiring decision on current staff. Personality should always be a factor when hiring and team-building, and further, in employee development and career planning.

"People flourish in their work environment when there is a good fit between their personality type and the characteristics of the environment. Lack of congruence between personality and environment leads to dissatisfaction, unstable career paths, and lowered performance." [120] Knowing the personality of the employee, enables the employer to choose an appropriate approach to training and motivating employees. An understanding of how individuals' personalities differ can use this understanding to improve their leadership effectiveness and lead to improving employees' job performance [121].

The major conclusion of this study in relation to personality was that more open individuals had higher ISA scores. This finding partially aligned with previous studies, that reported that conscientiousness, agreeableness, and openness explain the most variance in information security behavior [90]. Thus, future research might consider the evaluation of these two traits using a more comprehensive measure of personality.

To summarise, this research work had a practical contribution to the company by measuring the information security awareness among employees. The study provided the assessed company with evidence that their current regular information security training and risk communication programs were efficient. The scientific contribution was that this work looked into the relationship between vulnerability management efficiency and personality, which has not been done before and therefore filled this gap in the academic literature. In addition, this study contributes to the construct validity, called known-groups validity, of the ISA measurement tool HAIS-Q.

Bibliography

[1] Mann Charles Riborg. “A Study of Engineering Education”. In: *Bulletin Number Eleven. New York City* (1918).

[2] Emma Johns. “Cyber security breaches survey 2020”. In: *London: Department for Digital, Culture, Media & Sport* (2020).

[3] Tobias Fertig and Andreas Schütz. “About the measuring of information security awareness: a systematic literature review”. In: (2020).

[4] Agata McCormac et al. “Individual differences and information security awareness”. In: *Computers in Human Behavior* 69 (2017), pp. 151–156.

[5] Kwesi Hughes-Lartey et al. “Human factor, a critical weak point in the information security of an organization’s Internet of things”. In: *Heliyon* 7.3 (2021), e06522.

[6] Malcolm Robert Pattinson et al. “The Information Security Awareness of Bank Employees.” In: *HAISA*. 2016, pp. 189–198.

[7] Alvin Cindana and Yova Ruldeviyani. “Measuring information security awareness on employee using HAIS-Q: Case study at XYZ firm”. In: *2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*. IEEE. 2018, pp. 289–294.

[8] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma. “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior”. In: *computers & security* 49 (2015), pp. 177–191.

[9] Jörg Uffen, Nadine Guhr, and Michael H Breitner. “Personality traits and information security management: An empirical study of information security executives”. In: (2012).

[10] Nigel Nicholson et al. “Personality and domain-specific risk taking”. In: *Journal of Risk Research* 8.2 (2005), pp. 157–176.

[11] Rajarshi Chakraborty, Claire Vishik, and H Raghav Rao. “Privacy preserving actions of older adults on social media: Exploring the behavior of opting out of information sharing”. In: *Decision Support Systems* 55.4 (2013), pp. 948–956.

[12] Galen A Grimes et al. “Older adults’ knowledge of internet hazards”. In: *Educational Gerontology* 36.3 (2010), pp. 173–192.

[13] Ronnie L McGhee et al. “The relation between five-factor personality traits and risk-taking behavior in preadolescents”. In: *Psychology* 3.8 (2012), p. 558.

[14] M Whitty et al. “Cyberpsychology, behavior, and social networking”. In: *Mary Ann Liebert, Inc* 18.1 (2015), pp. 3–7.

[15] Margaret Gratian et al. “Correlating human traits and cyber security behavior intentions”. In: *computers & security* 73 (2018), pp. 345–358.

[16] FB Fatokun et al. “The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities”. In: *Journal of Physics: Conference Series*. Vol. 1339. 1. IOP Publishing. 2019, p. 012098.

[17] Alexander T Shappie, Charlotte A Dawson, and Scott M Debb. “Personality as a predictor of cybersecurity behavior.” In: *Psychology of Popular Media* 9.4 (2020), p. 475.

[18] Fayez Alotaibi and Aziz Alshehri. “Gender Differences in Information Security Management”. In: *Journal of Computer and Communications* 8.3 (2020), pp. 53–60.

[19] Agnetha Broos. “Gender and information and communication technologies (ICT) anxiety: Male self-assurance and female hesitation”. In: *CyberPsychology & Behavior* 8.1 (2005), pp. 21–31.

[20] Jun He and Lee A Freeman. “Are men more technology-oriented than women? The role of gender on the development of general computer self-efficacy of college students”. In: *Journal of Information Systems Education* 21.2 (2010), pp. 203–212.

[21] Cartmell Warrington, Javaid Syed, Ruth M Tappin, et al. “Personality and Employees’ Information Security Behavior among Generational Cohorts”. In: *Computer and Information Science* 14.1 (2021), pp. 1–44.

[22] Malcolm Pattinson et al. “Factors that influence information security behavior: An Australian web-based study”. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer. 2015, pp. 231–241.

[23] Malcolm Pattinson et al. “Why do some people manage phishing e-mails better than others?” In: *Information Management & Computer Security* (2012).

[24] Jörg Uffen, Nico Kaemmerer, and Michael H Breitner. “Personality traits and cognitive determinants–an empirical investigation of the use of smartphone security measures”. In: *Journal of Information Security 4 (2013), Nr. 4* 4.4 (2013), pp. 203–212.

[25] Tzipora Halevi, James Lewis, and Nasir Memon. “A pilot study of cyber security and privacy related behavior and personality traits”. In: *Proceedings of the 22nd international conference on world wide web*. 2013, pp. 737–744.

[26] Allaire K Welk et al. “Will the “Phisher-Men” Reel You In?: Assessing individual differences in a phishing detection task”. In: *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL)* 5.4 (2015), pp. 1–17.

[27] Javaid Syed and Ruth M Tappin. “IT Professionals’ Personality, Personal Characteristics, and Commitment: Evidence from a National Survey.” In: *Comput. Inf. Sci.* 12.3 (2019), pp. 58–71.

[28] Justin D Russell et al. “Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors”. In: *Journal of Cyber Security Technology* 1.3-4 (2017), pp. 163–174.

[29] ISACA - Information Systems Audit and Control Association. *Glossary*. [Accessed: 06-03-2022]. URL: https://www.isaca.org/resources/glossary/.

[30] Abhishek Narain Singh et al. “Information security management (ism) practices: Lessons from select cases from India and Germany”. In: *Global Journal of Flexible Systems Management* 14.4 (2013), pp. 225–239.

[31] Rodrigo Werlinger, Kirstie Hawkey, and Konstantin Beznosov. “An integrated view of human, organizational, and technological challenges of IT security management”. In: *Information Management & Computer Security* (2009).

[32] Shuchih Ernest Chang and Chin-Shien Lin. “Exploring organizational culture for information security management”. In: *Industrial management & data systems* (2007).

[33] Zahoor Ahmed Soomro, Mahmood Hussain Shah, and Javed Ahmed. “Information security management needs more holistic approach: A literature review”. In: *International Journal of Information Management* 36.2 (2016), pp. 215–225.

[34] Anthony Vance, Paul Benjamin Lowry, and Dennis Eggett. “Using accountability to reduce access policy violations in information systems”. In: *Journal of Management Information Systems* 29.4 (2013), pp. 263–290.

[35] RIA - Riigi Infosüsteemi Amet. *Küberturvalisuse aastaraamat 2022*. [Accessed: 20-02-2022]. URL: https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2022_eng.pdf.

[36] International Organization for Standardization. *ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT*. [Accessed: 25-03-2022]. URL: https://www.iso.org/isoiec-27001-information-security.html.

[37] Alexander McLeod and Diane Dolezel. “Information security policy non-compliance: Can capitulation theory explain user behaviors?” In: *Computers & Security* 112 (2022), p. 102526.

[38] J-C Spender and Hugo Kijne. *Scientific management: Frederick Winslow Taylor’s gift to the world?* Springer Science & Business Media, 2012.

[39] C Morais et al. “Human reliability analysis–accounting for human actions and external factors through the project life cycle”. In: *Safety and Reliability–Safe Societies in a Changing World* (2018), pp. 329–338.

[40] RIA - Riigi Infosüsteemi Amet. *2021 Security Vulnerability Report*. [Accessed: 20-02-2022]. URL: https://stack.watch/stats/2021/.

[41] Norman Hänsch and Zinaida Benenson. “Specifying IT security awareness”. In: *2014 25th International Workshop on Database and Expert Systems Applications*. IEEE. 2014, pp. 326–330.

[42] Mikko T Siponen. “A conceptual foundation for organizational information security awareness”. In: *Information management & computer security* (2000).

[43] Detmar W Straub and Richard J Welke. “Coping with systems risk: Security planning models for management decision making”. In: *MIS quarterly* (1998), pp. 441–469.

[44] Mark E Thomson and Rossouw von Solms. “Information security awareness: educating your users effectively”. In: *Information management & computer security* (1998).

[45] Mark Wilson, Joan Hash, et al. “Building an information technology security awareness and training program”. In: *NIST Special publication* 800.50 (2003), pp. 1–39.

[46] Ruben Mancha and Glenn Dietrich. “Development of a framework for analyzing individual and environmental factors preceding attitude toward information security”. In: (2007).

[47] Yacine Rezgui and Adam Marks. “Information security awareness in higher education: An exploratory study”. In: *Computers & security* 27.7-8 (2008), pp. 241–253.

[48] Elmarie Kritzinger and Elme Smith. “Information security management: An information security retrieval and awareness model for industry”. In: *Computers & security* 27.5-6 (2008), pp. 224–231.

[49] Information Technology Laboratory. *Glossary*. [Accessed: 24-03-2022]. URL: https://csrc.nist.gov/glossary/.

[50] Icek Ajzen. “The theory of planned behavior”. In: *Organizational behavior and human decision processes* 50.2 (1991), pp. 179–211.

[51] Ronald W Rogers. “Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation”. In: *Social psychophysiology: A sourcebook* (1983), pp. 153–176.

[52] Anthony Ellis. “A deterrence theory of punishment”. In: *The Philosophical Quarterly* 53.212 (2003), pp. 337–351.

[53] Tom Baranowski et al. “Are current health behavioral change models helpful in guiding prevention of weight gain efforts?” In: *Obesity research* 11.S10 (2003), 23S–43S.

[54] Icek Ajzen and Martin Fishbein. “Attitudinal and normative variables as predictors of specific behavior.” In: *Journal of personality and Social Psychology* 27.1 (1973), p. 41.

[55] Kathryn Parsons et al. “Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)”. In: *Computers & security* 42 (2014), pp. 165–176.

[56] Barbara Schneider. *Measuring results: Gaining insight on behavior change strategies and evaluation methods from environmental education, museum, health, and social marketing programs*. Coevolution Institute, 2003.

[57] Wenhua Xu et al. “Knowledge, attitude, and behavior in patients with atrial fibrillation undergoing radiofrequency catheter ablation”. In: *Journal of interventional cardiac electrophysiology* 28.3 (2010), pp. 199–207.

[58] Mari Karjalainen. “Improving Employees’ Information Systems (IS) Security Behavior-Toward a Meta-Theory of IS Security Training and a New Framework for Understanding Employees’ IS Security Behavior”. In: *PhD. University of Oulu* (2011).

[59] Marlies Sas et al. “The impact of training sessions on physical security awareness: Measuring employees’ knowledge, attitude and self-reported behaviour”. In: *Safety science* 144 (2021), p. 105447.

[60] Tova Rosenbloom et al. “The effectiveness of road-safety crossing guards: Knowledge and behavioral intentions”. In: *Safety Science* 46.10 (2008), pp. 1450–1458.

[61] Doni Dwi Hantyoko Wahyudiwan, Yudho Giri Sucahyo, and Arfive Gandhi. “Information security awareness level measurement for employee: Case study at ministry of research, technology, and higher education”. In: *2017 3rd International Conference on Science in Information Technology (ICSITech)*. IEEE. 2017, pp. 654–658.

[62] Jeffrey M Stanton et al. “Analysis of end user security behaviors”. In: *Computers & security* 24.2 (2005), pp. 124–133.

[63] Alessandro Acquisti and Ralph Gross. “Imagined communities: Awareness, information sharing, and privacy on the Facebook”. In: *International workshop on privacy enhancing technologies*. Springer. 2006, pp. 36–58.

[64] Kathryn Parsons et al. “The human aspects of information security questionnaire (HAIS-Q): two further validation studies”. In: *Computers & Security* 66 (2017), pp. 40–51.

[65] AL Fadhilah et al. “Measurement of Information Security Awareness Level: A Case Study of Digital Wallet Users”. In: *IOP Conference Series: Materials Science and Engineering*. Vol. 1077. 1. IOP Publishing. 2021, p. 012003.

[66] Philip J Corr and Gerald Ed Matthews. *The Cambridge handbook of personality psychology*. Cambridge University Press, 2020.

[67] Gordon Willard Allport. “Personality: A psychological interpretation.” In: (1937).

[68] Sigmund Freud. *The ego and the id*. Simon and Schuster, 2019.

[69] Hans JÃ1/4rgen Eysenck. *The biological basis of personality*. Vol. 689. Transaction publishers, 1967.

[70] Hans Jurgen Eysenck. “The scientific study of personality.” In: (1952).

[71] William B Swann Jr and Conor Seyle. “Personality psychology’s comeback and its emerging symbiosis with social psychology”. In: *Personality and Social Psychology Bulletin* 31.2 (2005), pp. 155–165.

[72] Raymond B Cattell. *The scientific analysis of personality*. Routledge, 2017.

[73] Donald W Fiske. “Consistency of the factorial structures of personality ratings from different sources.” In: *The Journal of Abnormal and Social Psychology* 44.3 (1949), p. 329.

[74] K Cherry and S Gans. *What Are the Big 5 Personality Traits? Verywell Mind*. 2018.

[75] Robert R McCrae. “Cross-cultural research on the five-factor model of personality”. In: *Online readings in psychology and culture* 4.4 (2002), pp. 1–12.

[76] Li-fang Zhang. “Thinking styles and the big five personality traits revisited”. In: *Personality and individual differences* 40.6 (2006), pp. 1177–1187.

[77] Paul T Costa Jr and Robert R McCrae. *The Revised Neo Personality Inventory (neo-pi-r)*. Sage Publications, Inc, 2008.

[78] Lewis R Goldberg. “The development of markers for the Big-Five factor structure.” In: *Psychological assessment* 4.1 (1992), p. 26.

[79] Oliver P John, Sanjay Srivastava, et al. “The Big Five trait taxonomy: History, measurement, and theoretical perspectives”. In: *Handbook of personality: Theory and research* 2.1999 (1999), pp. 102–138.

[80] Gerard Saucier. “Mini-Markers: A brief version of Goldberg’s unipolar Big-Five markers”. In: *Journal of personality assessment* 63.3 (1994), pp. 506–516.

[81] Samuel D Gosling, Peter J Rentfrow, and William B Swann Jr. “A very brief measure of the Big-Five personality domains”. In: *Journal of Research in personality* 37.6 (2003), pp. 504–528.

[82] Maranda McBride, Lemuria Carter, and Merrill Warkentin. “Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies”. In: *RTI International-Institute for Homeland Security Solutions* 5.1 (2012), p. 1.

[83] Lee Hadlington, Jens Binder, and Natalia Stanulewicz. “Exploring role of moral disengagement and counterproductive work behaviours in information security awareness.” In: *Computers in Human Behavior* 114 (2021), p. 106557.

[84] Simon Trang and Ilja Nastjuk. “Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour”. In: *Computers & Security* 104 (2021), p. 102222.

[85] Ashleigh Wiley, Agata McCormac, and Dragana Calic. “More than the individual: Examining the relationship between culture and Information Security Awareness”. In: *Computers & Security* 88 (2020), p. 101640.

[86] Tanja Grassegger and Dietmar Nedbal. “The role of employees’ information security awareness on the intention to resist social engineering”. In: *Procedia Computer Science* 181 (2021), pp. 59–66.

[87] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma. “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior”. In: *computers & security* 49 (2015), pp. 177–191.

[88] Mark Harris and Steven Furnell. “Routes to security compliance: Be good or be shamed?” In: *Computer Fraud & Security* 2012.12 (2012), pp. 12–20.

[89] Mitchell Kajzer et al. “An exploratory investigation of message-person congruence in information security awareness campaigns”. In: *Computers & security* 43 (2014), pp. 64–76.

[90] Malcolm Pattinson et al. “Managing information security awareness at an Australian bank: A comparative study”. In: *Information & Computer Security* (2017).

[91] MARY ADDO, WINIFRED EBOH, and R Taylor. *Qualitative and quantitative research approaches*. Sage, 2014.

[92] John W Creswell et al. “Best practices for mixed methods research in the health sciences”. In: *Bethesda (Maryland): National Institutes of Health* 2013 (2011), pp. 541–545.

[93] Robert K Yin. *Case study research: Design and methods*. Vol. 5. sage, 2009.

[94] Jordan Shropshire et al. “Personality and IT security: An application of the five-factor model”. In: *AMCIS 2006 Proceedings* (2006), p. 415.

[95] Douglas F Cellar et al. “The five-factor model and safety in the workplace: Investigating the relationships between personality and accident involvement”. In: *Journal of Prevention & Intervention in the community* 22.1 (2001), pp. 43–52.

[96] Oliver E John Veronica Benet-Martinez. “Los Cinco Grandes Across Cultures and Ethnic Groups: Multitrait Multimethod Analyses of the Big Five in Spanish and English”. In: *Journal of Personality and Social Psychology Copyright 1998 by the American Psychological Association, Inc. 1998, Vol. 75, No. 3, 729-750*. 1998.

[97] David Zweig and Jane Webster. “What are we measuring? An examination of the relationships between the big-five personality traits, goal orientation, and performance intentions”. In: *Personality and individual differences* 36.7 (2004), pp. 1693–1708.

[98] Adrian Furnham. “Relationship among four Big Five measures of different length”. In: *Psychological Reports* 102.1 (2008), pp. 312–316.

[99] Adam W Meade and S Bartholomew Craig. “Identifying careless responses in survey data.” In: *Psychological methods* 17.3 (2012), p. 437.

[100] Lee J Cronbach. “Coefficient alpha and the internal structure of tests”. In: *psychometrika* 16.3 (1951), pp. 297–334.

[101] Lee J Cronbach and Paul E Meehl. “Construct validity in psychological tests.” In: *Psychological bulletin* 52.4 (1955), p. 281.

[102] Dominic Edelmann, Tamás F Móri, and Gábor J Székely. “On relationships between the Pearson and the distance correlation coefficients”. In: *Statistics & Probability Letters* 169 (2021), p. 108960.

[103] Mainar Swari Mahardika et al. “Measurement of employee awareness levels for information security at the center of analysis and information services judicial commission Republic of Indonesia”. In: *Adv. Sci. Technol. Eng. Syst.* 5.3 (2020), pp. 501–509.

[104] Hennie A Kruger and Wayne D Kearney. *Measuring information security awareness: A West Africa gold mining environment case study*. 2005.

[105] Dirk P Snyman and Hennie A Kruger. “Information security behavioural threshold analysis in practice: an implementation framework”. In: *International Symposium on Human Aspects of Information Security and Assurance*. Springer. 2020, pp. 133–143.

[106] Daniel J Kruger. “Brief self-report scales assessing life history dimensions of mating and parenting effort”. In: *Evolutionary Psychology* 15.1 (2017), p. 1474704916673840.

[107] Robert A Power and Michael Pluess. “Heritability estimates of the Big Five personality traits based on common genetic variants”. In: *Translational psychiatry* 5.7 (2015), e604–e604.

[108] Andrew Neal et al. “Predicting the form and direction of work role performance from the Big 5 model of personality traits”. In: *Journal of Organizational Behavior* 33.2 (2012), pp. 175–192.

[109] Christopher J Soto et al. “Age differences in personality traits from 10 to 65: Big Five domains and facets in a large cross-sectional sample.” In: *Journal of personality and social psychology* 100.2 (2011), p. 330.

[110] Agata McCormac et al. “A reliable measure of information security awareness and the identification of bias in responses”. In: *Australasian Journal of Information Systems* 21 (2017).

[111] Leslie Harris. “An Introduction to Survey Research and Data Analysis”. In: *JMR, Journal of Marketing Research (pre-1986)* 14.000004 (1977), p. 621.

[112] John T Roscoe. *Fundamental research statistics for the behavioral sciences [by] John T. Roscoe*. 1975.

[113] Wynn Anthony Abranovic. *Statistical thinking and data analysis methods for managers*. Addison-Wesley Longman Publishing Co., Inc., 1997.

[114] Paul Martin, Paul Patrick Gordon Bateson, and Patrick Bateson. *Measuring behaviour: an introductory guide*. Cambridge university press, 1993.

[115] Robin Hill. “What sample size is “enough” in internet survey research”. In: *Interpersonal Computing and Technology: An electronic journal for the 21st century* 6.3-4 (1998), pp. 1–12.

[116] Eric Emerson, David Felce, and Roger J Stancliffe. “Issues concerning self-report data and population-based data sets involving people with intellectual disabilities”. In: *Intellectual and developmental disabilities* 51.5 (2013), pp. 333–348.

[117] Alan Rosenbaum et al. “A comparison of methods for collecting self-report data on sensitive topics”. In: *Violence and Victims* 21.4 (2006), pp. 461–471.

[118] Robert J Fisher and James E Katz. “Social-desirability bias and the validity of self-reported values”. In: *Psychology & marketing* 17.2 (2000), pp. 105–120.

[119] Erwin Oliver Finkenbinder. “The curve of forgetting”. In: *The American Journal of Psychology* 24.1 (1913), pp. 8–32.

[120] John L Holland. “Exploring careers with a typology: What we have learned and some new directions.” In: *American psychologist* 51.4 (1996), p. 397.

[121] Nadiah Maisarah Abdul Ghani, Nor Sara Nadia Muhamad Yunus, and Norliza Saiful Bahry. “Leader’s personality traits and employees job performance in public sector, Putrajaya”. In: *Procedia Economics and Finance* 37 (2016), pp. 46–51.

Appendices

Appendix 1 - Big Five

Big Five Inventory-10 (BFI-10)					
I see myself as someone who ...	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Extraversion					
... is reserved*	(1)	(2)	(3)	(4)	(5)
... is outgoing, sociable	(1)	(2)	(3)	(4)	(5)
Agreeablenesss					
... is generally trusting	(1)	(2)	(3)	(4)	(5)
... tends to find fault with others*	(1)	(2)	(3)	(4)	(5)
Conscientiousness					
... tends to be lazy*	(1)	(2)	(3)	(4)	(5)
... does a thorough job	(1)	(2)	(3)	(4)	(5)
Neuroticism					
... is relaxed, handles stress well*	(1)	(2)	(3)	(4)	(5)
... gets nervous easily	(1)	(2)	(3)	(4)	(5)
Openness to experience					
... has few artistic interests*	(1)	(2)	(3)	(4)	(5)
... has an active imagination	(1)	(2)	(3)	(4)	(5)
* item is reverse-scored					

Appendix 2 - HAIS-Q

Please note that the statements where that have in the end an asterisk (*) are reverse statements

HAIS-Q items			
	Knowledge	Attitude	Behaviour
Focus area: Password management			
Using the same password	It's acceptable to use my social media passwords on my wok accounts.*	It's safe to use the same password for social media and work accounts.*	I use a different password for my social media and work accounts.
Sharing passwords	I am allowed to share my work passwords with colleagues.*	It's bad idea to share my work passwords, even if a colleague asks for it.*	I share my work passwords with colleagues.*
Using a strong password	A mixture of letters. Numbers and symbols is necessary for work passwords.	It's safe to have a work password with just letters.*	I use a combination of letters, numbers and symbols in my work passwords.
Focus area: Email use			
Clicking on links in emails from known senders	I am allowed to click on any links in emails from people I know.*	It's always safe to click on links in emails from people I know.*	I don't always click on links in emails just because they come from someone I know.
Clicking on links in emails from unknown senders	I am not permitted to click on a link in an emails from an unknown sender.	Nothing bad can happen if I click on a link in an email from an unknown sender.*	If an email from an unknown sender looks interesting, I click on a link within it.*
Opening attachments in emails from unknown senders	I am allowed to open email attachments from unknown senders.*	It's risky to open an email attachment from an unknown sender.	I don't open email attachments if the sender is unknown to me.

	Knowledge	Attitude	Behaviour
Focus area: Internet use			
Downloading files	I am allowed to download any files onto my work computer if they help me to do my job.*	It can be risky to download files on my work computer.	I download any files onto my work computer that will help me get the job done.*
Accessing dubious websites	While I am at work, I shouldn't access certain websites.	Just because I can access a website at work, doesn't mean that it's safe.	When accessing the Internet at work, I visit any website that I want to.*
Entering information online	I am allowed to enter any information on any website if it helps me do my job.*	If it helps me to do my job, it doesn't matter what information I put on a website.*	I assess the safety of websites before entering information.
Focus area: Social media use			
SM privacy settings	I must periodically review the privacy settings on my social media accounts.	It's a good idea to regularly review my social media privacy settings.	I don't regularly review my social media privacy settings.*
Considering consequences	I can't be fired for something I post on social media.*	It doesn't matter if I post things on social media that I wouldn't normally say in public.*	I don't post anything on social media before considering any negative consequences.
Posting about work	I can post what I want about work on social media.*	It's risky to post certain information about my work on social media.	I post whatever I want about my work on social media.*

	Knowledge	Attitude	Behaviour
Focus area: (Mobile)Portable devices			
Physically securing mobile devices	When working in a public place, I have to keep my laptop with me at all times.	When working in a cafe, it's safe to leave my laptop unattended for a minute.*	When working in a public place, I leave my laptop unattended.*
Sending sensitive information via Wi-Fi	I am allowed to send sensitive work via a public Wi-Fi network.*	It's risky to send sensitive work files using a public Wi-Fi network.	I send sensitive work files using a public Wi-Fi network.*
Shoulder surfing	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	It's risky to access sensitive work files on a laptop if strangers can see my screen.	I check that strangers can't see my laptop screen if I'm working on a sensitive document.
Working remotely/ using working device at home	I have to keep my laptop locked when I step away from it, even when work from home.	Nothing bad can happen, if my family members see documents, programs I use at my work laptop.*	I use my working laptop only for work related tasks.
Focus area: Information handling			
Disposing of sensitive print-outs	Sensitive print-outs can be disposed of in the same way as non-sensitive ones.*	Disposing of sensitive print-outs by putting them in the rubbish bin is safe.*	When sensitive print-outs need to be disposed of, I ensure that they are shredded or destroyed.
Inserting removable media	If I find a USB stick in a public place, I shouldn't plug it into my work computer.	If I find a USB stick in a public place, nothing bad can happen if I plug it into my work computer.*	I wouldn't plug a USB stick found in a public place into my work computer.
Leaving sensitive material	I am allowed to leave print-outs containing sensitive information on my desk overnight.*	It's risky to leave print-outs that contain information on my desk overnight.	I leave print-outs that contain sensitive information on my desk when I'm not there.*
Information classification	All documents developed within or by order of the company have to be labelled in accordance with the classification of their content.	Information classification and document labeling makes easier for everyone to understand how to handle information.	I label document only when this contains confidential information.*

	Knowledge	Attitude	Behaviour
Focus area: Incident reporting			
Reporting suspicious behaviour	If I see someone acting suspiciously in my workplace, I should report it.	If I ignore someone acting suspiciously in my workplace, nothing bad can happen.*	If I saw someone acting suspiciously in my workplace, I would do something about it.
Ignoring poor security behaviour by colleagues	I must not ignore poor security behaviour by my colleagues.	Nothing bad can happen if I ignore poor security behaviour by a colleague.*	If I noticed my colleague ignoring security rules, I wouldn't take any action.*
Reporting all incidents	It's optional to report security incidents.*	It's risky to ignore security incidents, even if I think they're not significant.	If I noticed a security incident, I would report it.