TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Maarja Heinsoo 178233IVCM

IMPLICATIONS OF INFORMATION SECURITY CULTURE ON RISK MANAGEMENT – CASE OF A TECHNOLOGY COMPANY

Master's thesis

Supervisor: Hayretdin Bahsi
PhD

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Maarja Heinsoo 178233IVCM

INFOTURBE KULTUURI MÕJUD RISKIHALDUSELE TEHNOLOOGIAETTEVÕTTE NÄITEL

Magistritöö

Juhendaja: Hayretdin Bahsi

PhD

Tallinn 2019

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: Maarja Heinsoo

13.05.2019

Abstract

This master thesis is a study combining qualitative and quantitative research methods – interviews with different stakeholders and a survey to analyse the connections information security culture and involvement in IT risk management procedures might have. The study is conducted in a young technology company having operations in Estonia.

The author decided to focus on a young technology company as young companies might struggle to handle security risks due to the rapid business development. At the same time the realisation of these risks could put an end to the young company. The author did not see from the literature that special attention to young technology companies has been placed which was another reason to conduct the study in a young technology company.

Information security culture exists in every company and research done in this area indicates that when designed properly it can reduce information security risks more effectively and impacts what employees think or know about information security. Different organisations have different information security cultures and there can be several subcultures within the same organisation.

For the purposes of analysing the connections between the IT risk management procedures and information security culture, the author has designed and conducted a survey in Company A and has carried out semi-structured interviews with 6 stakeholders. The focus on a young technology company, the usage of combined research methods and the fact that next to the chief information security also other stakeholders have been reviewed, adds to the uniqueness of this study.

One of the outcomes of this thesis was that engineers who might have more relation to IT risk management procedures do not differ significantly from non-engineers when it comes to perceiving information security culture. This could mean that information security culture has been established evenly across different groups of people. As an interesting additional outcome it was noted that there are equal amount of engineers and non-engineers among the people who are on average more related to IT risk management procedures. This could mean that in the inspected technology company the IT risk management is not just a responsibility for the engineers but the responsibility is shared also with non-engineers.

Also employees who are more related to IT risk management procedures (group A) perceive the information security culture very similarly compared to the employees who are on average less involved in IT risk management procedures (group B). This once again indicates that information security culture has been established evenly across different groups of employees. The t-tests revealed that the only meaningful difference seems to be the level of uncertainty group A has compared to group B about information security culture, indicating that the people who on average are more involved in IT risk management procedures exhibit more confident opinions about the way they perceive information security culture – they choose to stay neutral less often than people in group B.

This thesis is written in English and is 121 pages long, includes 6 chapters, 7 figures and 12 tables.

Annotatsioon

Infoturbe kultuuri mõjud riskihaldusele tehnoloogiaettevõtte näitel

See magistritöö kätkeb endas uurimust, mis on läbi viidud Eestis tegutsevas noores tehnoloogiaettevõttes. Uurimus kombineerib nii kvalitatiivseid uurimismeetodeid kui ka kvanitatiivseid uurimismeetodeid ning selle eesmärk on analüüsida seoseid infoturbe kultuuri ning IT riskihalduse protseduuride vahel.

Autor otsustas keskenduda noorele tehnoloogiaettevõttele, kuna tulenevalt tempokast ärikasvust võib noorte ettevõtete jaoks võib infoturbe riskidega tegelemine olla keeruline. Samal ajal võib riskide avaldumine noore ettevõtte põhja viia. Lisaks ei näinud töö autor, et kirjanduses oleks noortele ettevõtetele eraldi tähelepanu pööratud, mis andis enam alust keskenduda just noorele tehnoloogiaettevõttele..

Infoturbe kultuur eksisteerib igas organisatsioonis ning selle ümber läbi viidud uuringud näitavad, et õige rakendamise ja disaini korral võib infoturbe kultuur aidata infoturbe riske efektiivselt vähendada. Ühtlasi aitab see suunata, kuidas töötajad infoturbest mõtlevad. Infoturbe kultuur on igas organisatsioonis ise näoga ja ühes organisatsioonis võib esineda ka mitu alamkultuuri.

Selleks, et analüüsida infoturbekultuuri ja IT riskihalduse vahelisi seoseid, on töö autor kasutanud Ettevõttes A küsimustikku ning viinud läbi pool-struktureeritud intervjuud kokku kuue inimesega Ettevõttest A. See, et käesoleva töö fookus on noorel tehnoloogiaettevõttel, kasutatud on kombineeritud uurimismeetodeid ja lisaks infoturbejuhile on intervjueeritud ka teisi isikuid lisab juurde käesoleva töö unikaalsusele.

Käesoleva magistritöö üks olulisematest tulemustest on see, et insenerid, kellel võib esineda rohkem seost IT riskihaldusega, ei erine oluliselt infoturbe kultuurile antud hinnangute poolest mitte-inseneridest. See võib viidata, et infoturbe kultuur on ühtlase tasemega kogu ettevõttes. Täiendava huvitava tulemusena selgus, et nende inimeste hulgas, kes on IT riskihaldusega keskmisest rohkem seotud, on võrdselt nii insenere kui mitte-insenere, mis viitab, et IT riskihaldus ei ole tehnoloogiga tegelevas Ettevõttes A pelgalt inseneride teema vaid vajab tähelepanu kõigilt.

Töötajad, kes on riskihaldusega igapäevaselt rohkem seotud (grupp A) tunduvad tajuvat infoturbe kultuuri sarnaselt nendega, kes IT riskihaldusega keskmiselt vähen seotud on (grupp B). Ka see indikeerib, et ettevõttes on infoturbe kultuur rakendatud ühtlaselt. Teostatud t-test tõi välja, et ainus oluline erinevus tundub seisnevat selles, kui suurel määral grupp A võrrelduna grupiga B peab vajalikuks väljendada neutraalsust infoturbe kultuuri osas. See tähendab, et inimesed, kes pidasid end keskmiselt rohkem seotuks IT riskihaldusega kasutasid infoturbe kultuuri küsimustele vastamiseks erineval määral neutraalseks jäämise võimalust kui inimesed, kes on keskmisel vähem seotud IT riskihaldusega. Esmane analüüs viitab, et grupi A liikmed on enesekindlamad oma vastustes ning jäid vähemal määral neutraalseks kui grupi B liikmed.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 121 leheküljel, 6 peatükki, 7 joonist, 12 tabelit.

Acknowledgements

My sincerest gratitude goes to my supervisor Dr Hayretdin Bahsi, who has always found the time to guide, support and encourage me. I am also thankful for Dr Tiiu Kamdron who was willing to support me whenever I had questions relating to social sciences and statistics.

I would like to thank the people who were willing to participate in this study and the people who helped me improve the study.

Last but not least, I am thankful to my husband who has shown utmost patience and care during the two years I have been studying on this curriculum. Thank you!

List of abbreviations and terms

ENISA	European Union Agency for Network and Information Security
ERM	Enterprise risk management
HAIS-Q	Human aspects of information security questionnaire
ISC	Information security culture
ISCA	Information security culture assessment
IT	Information technology
NIST	National Institute of Standards and Technology

Table of contents

List of figures

List of tables

1 Introduction

1.1 Motivation

Various news articles in the media and other sources have reported that over the recent years the technology startups scene has been vivid. Compared to 2017 the number of young companies that were valued at more than one billion US dollars (the so-called unicorns) in 2018 has doubled in Europe [1], and next to the well-known startup ecosystems in the US (e.g. Silicon Valley and New York), new hubs for innovative technology startups have emerged globally [2]. Compared to 2016 the number of new technology companies established in the UK during 2017 rose approximately by 60% [3]. We are witnessing the era of technology ventures.

Many businesses have adopted IT solutions to support their business processes, ant this most likely applies also to young technology companies. They place reliance on information technology which also brings risks regarding IT and security closer to the these companies. This means that at least part of the enterprise risk management should be focused specifically on information security risks. No venture is born mature in terms of risk management and corporate governance, but the various risks will still surround the business right from the beginning, no mercy there.

An example of a young company not being able to continue its business operations after a cyber incident, is Code Spaces [4]. The company had operated just for seven years when they suffered an intrusion attack which destroyed most of the data and its backups which the company was holding on behalf of their customers [4][5]. Code Spaces immediately notified that they were no longer able to continue their business [4].

Although building up risk management and paying special attention to enterprise information security management may usually not be the first thing a young company starts thinking of, they eventually have to invest time and other resources to these areas too. Depending on the industry the company operates in, it might even be required by the regulators who are allowed to assess whether the company is allowed to continue their operations in the market or not.

Substantial part of information security management and risk management focuses on the people. The reason behind this is that the way people interact with information assets determines the effectiveness of the information security controls [6]. Information security management and risk management can for example entail building the information security control environment (e.g. designing procedures, implementing policies) in which the people need to operate, or raising employees' awareness about information security. The aim to focus on people is designed to be part of enterprise information security management and risk management practises.

When talking specifically about information security risks then according to the 2018 Insider Threat Report [7] issued by Cybersecurity Insiders in collaboration with Crowd Research Partners, 90% of organizations feel at least slightly vulnerable to possible insider attacks. The same report suggests that the top five risk factors enabling the feared vulnerability are [7]:

- the amount of users who have wide range of access rights to the company's information systems,
- the growing number of devices that have access to sensitive data,
- the general chaos or disorder relating to information technology that keeps increasing,
- the growing amount of sensitive data, and
- the deficiencies relating to employee awareness training.

51% of the respondents are more concerned about unintentional insider threats, and 47% are more concerned about malicious insider threats [7]. As for unintentional insider threats, 67% of the respondents see that phishing attempts are the biggest concern [7]. Other commonly mentioned concerns are the use of inappropriate passwords (i.e. passwords are weak or reused), devices which are left unlocked, user credential sharing practises and the use of untrusted *Wi-Fi* networks [7].

When it comes down to making a risk treatment decision, it is possible to address insider threat with technical security measures such as monitoring of assets, monitoring of employees, implementation of intrusion detection systems, putting access controls in place, but also with organisational security measures such as establishing policies and whistleblowing programs, conducting mandatory information security awareness trainings, conducting background checks on prospects, and conducting internal audits [7].

It can be difficult to keep up with the implementation of appropriate technical and organisational security measures to address all the relevant risks. The difficulty is probably higher for the young companies where the number of information assets and people and complexity of information technology is constantly increasing [8][9][10]. At the same time, managing risks is one of the things that the startups have to get right to experience globalization and growth [11].

In order to design and maintain organisational values and perceptions companies use their organisational culture. Similarly, it would be beneficial to consider establishing a strong information security culture in order to improve the way people think about information security and the associated risks. Without a supporting information security culture, information security policies can go overlooked, technical security controls might not operate as intended due to employee reluctance, and information security awareness programs might not target the audience in the most effective ways [6] [12]. It could be reasonable to benefit from something that all organisations already have – an information security culture [13].

As information security has become an integral part of almost every organisation, information security culture is one part of general organisational culture which focuses on the way people perceive information security [12][14]. As a comparison, information security awareness focuses on improving people's knowledge about information security, controls and procedures [15], but in simple terms, information security culture deals with the way people feel (reluctant vs promoting) about information security and what kind of information security behaviour is promoted by the people.

The term 'information security culture' is not a very new one as there are references about this term which date back to year 2000, but the existing research is limited and still needs to mature[1] [16]. Most of the research papers focus on defining the concept of information security culture and its roots (e.g. relation to organizational culture) [16]. Not much has been written about the benefits (e.g. effects on information security risk management, effectiveness of technical and organizational security controls) of information security culture [16].

The author has decided to write their thesis about information security culture because the concept is an underlying element for every information security control environment, a root cause that could determine how effectively the information security control environment operates. In order to provide a new angle to the whole information security culture research area, the author has decided to tie the information security culture topic with risk management aspect. In addition the author would like to contribute to this research area with an empirical study which combines the analysis of quantitative and qualitative data – hoping to bring the state of research closer to being mature.

1.2 Objective

The main objective of this thesis is to interpret what kind of the implications employee level perception of information security might have on IT risk management procedures in a young technology company. The idea is to see how does the existing information security culture reflect in the company's IT risk management domain.

In order to achieve the objective the author has decided to conduct an information security culture assessment which also includes questions about IT risk management procedures The assessment statements about IT management risk procedures help to divide the respondents into two groups: the first group being employees who are more involved in dealing with various risk management procedures on a daily basis (employee group A)

[1] Maturity of the field being defined by the research purposes: state of research is considered to be mature if next to descriptive, philosophical and theoretical research there also exists research which generates new theories or tests existing theories [16].

and the second group representing the employees who are less involved in dealing with various risk management procedures on a daily basis (employee group B).

The author has conducted this assessment in a young (less than 10 years old) technology company based in Estonia (Company A). One of the reasons for choosing Estonia is, of course, that this region is conveniently accessible for the author. Another reason for choosing Estonia is that there exist quite a few companies that match the profile the author is seeking for as Estonia has many startups and [17] is seen as one of the leading countries in 21st century Europe in terms of digital innovation [18].

In order to provide further reasoning why the author has decide to focus on a young technology company is that these companies are usually driven by agile software development principles, fast business development speed and do not have much hierarchy, also the teams within the company lack the typical corporate culture which the more established and mature companies might have. The author is interested in seeing how does information security culture look like and what kind of relations it has with IT risk management in a less corporate and young work environment which is tightly bound to the usage of information technology solutions. When conducting literature research, the author noticed that young technology companies have not been studied much from information security culture and IT risk management perspective.

The author believes that in established work environments the risk management procedures and responsible stakeholders are usually defined well. This should provide clarity to daily risk management procedures. Although the whole risk management framework might not be as clearly defined in younger companies and therefore is perhaps more influenced by employees’ personal perception and judgement, risks have to also be managed in the young companies. Naturally, in a technology company much of the risks are related to the usage of information technology (IT) solutions which automatically should bring specifically information security risks closer to the general risk management procedures established in the company.

The author has assumed that the employees who are managing risks in a technology company should indicate promoting or favorable values towards company’s information security culture as they are probably by default required to have more visibility and responsibility about the usage IT solutions too. In order to conclude whether the attitude is more promoting or not, the author has simply compared if the average grade given to information security culture is more close to the positive values or negative values.

Another assumption the author has made, is that the engineers (software developers, IT infrastructure engineers etc, security engineers) working in the company should indicate more favorable results towards information security culture than the people who are not engineers (i.e. non-engineers). The author believes that as engineers should have more knowledge about information technology in general then they might also feel more comfortable about the existing information security culture. The engineers might also have more connection to specifically IT risk management procedures which is why the author is investigating engineers in the first place. In order to test this, the author has compared the average grades the engineers and non-engineers have given to the information security culture and conduct a t-test to see if the potential differences between the engineers and non-engineers are significant enough. For the purposes of conducing the t-test the author has come up with the following hypotheses:

- $H0_{EC}$ – null-hypothesis: There is no difference in information security culture grades between engineers and non-engineers.
- $H1_{EC}$ – alternative-hypothesis: There is a meaningful difference in information security culture grades between engineers and non-engineers.

There is a chance that information security culture is not established as strongly as the author might expect. The study is conducted in a young company and this could mean that there is substantive amount of uncertainty around the way the employees perceive information security culture. To the author it would make sense, if engineers expressed less uncertainty towards information security culture than non-engineers. The author assumes this because engineers might have more exposure to the information security in general and therefore have more understanding of the domain. This is the reason why the author has decided to also compare whether the level of uncertainty differs when comparing engineers and non-engineers. The author conducts a t-test and has come up with the following hypotheses:

- $H0_{EU}$ – null-hypothesis: The level of uncertainty perceived about information security culture is not different for engineers and non-engineers.

- $H1_{EU}$ – alternative-hypothesis: The level of uncertainty perceived about information security culture is different for engineers and non-engineers.

The author also assumes that the employees more involved in IT risk management procedures (group A) should provide higher grades for information security culture than the people less involved in IT risk management procedures (group B). This should be because having more visibility about IT risk management could also help perceive information security culture as something the respondent has control over. In order to test this, the author has compared the average grades these groups have given to the information security culture and conduct a t-test to see if the potential differences between the two groups are significant enough. For the purposes of conducing the t-test the author has come up with the following hypotheses:

- $H0_{GC}$ – null-hypothesis: There is no difference in information security culture grades between group A and group B.

- $H1_{GC}$ – alternative-hypothesis: There is a meaningful difference in information security culture grades between group A and group B.

As the author mentioned before, we might see substantive amount of uncertainty around the way the employees perceive information security culture. The author assumes that for employee group A the uncertainty should be smaller than for employee group B as group A has more focus on IT risk management procedures. In order to compare whether the levels of uncertainty about information security culture differ, the author conducts a t-test and has come up with the following hypotheses:

- $H0_{GU}$ – null-hypothesis: The level of uncertainty perceived about information security culture is not different for group A and group B.

- $H1_{GU}$ – alternative-hypothesis: The level of uncertainty perceived about information security culture is different for group A and group B.

In order to be able to interpret the quantitative data, i.e. the state of the information security culture and its relation to IT risk management procedures in Company A, the author has also conducted semi-structured interviews with the relevant stakeholders from

Company A. The author believes that the selected interviewees have provided better reasoning for quantitative data.

1.3 Scope

The scope of this thesis project is limited to conducting information security culture assessment (ISCA) combined with assessment about employee’s involvement in IT risk management procedures in one young (established less than 10 years ago) technology company that has operations in Estonia (Company A).

Conducting a study just in Company A clearly does not give enough data to be able to extrapolate the conclusions for all the young technology companies operating Estonia, but it could be a valuable learning point before conducting other larger scale researches within the same scope. The author has also carried out a pilot assessment with limited scope in another young technology company having operations in Estonia (company B).

This assessment combines the analysis of quantitative data (the survey responses) and the analysis of qualitative data (interviews held with the stakeholders – chief information security manager, senior information security specialist, junior information security specialist, HR specialist focusing on organisational culture, software engineer not working in security team and a customer service agent – from Company A).

The combination of quantitative and qualitative methods is used for two main reasons. Firstly, the literature review revealed that the studies focusing on information security culture only tend to use one method which leaves little room to interpreting the results, and secondly, the author sees that adding a qualitative method helps to put quantitative data into context and therefore provides a better understanding about what is behind the numbers. The literature review pointed out that some studies use interviews as a research method but interviews do not include other stakeholders besides the chief information security officer. The author of this thesis has interviewed also other stakeholders.

As mentioned before, in order to add qualitative measure to the data analysis, the author has conducted semi-structured interviews during which the interviewees got an overview of the quantitative data and were asked to speak their mind. To gather quantitative data, the author has used a survey consisting of four main parts:

1. General questions about the respondents work (tenure, location, business unit, role) – these were designed by the author to be able to assess whether there are differences in responses for example across tenure, etc.
2. Statements to determine the respondents' involvement in IT risk management procedures – these statements were designed by the author and are mainly based on the general risk management procedure flow.
3. Statements to assess the respondents' knowledge about information security – although modified this part of the survey is largely based on an ISCA tested by other researchers [19][20].
4. Statements to assess the respondents' information security culture – this serves as the main part of the survey and is also largely based on ISCA [19].

1.4 Research questions

This thesis project aims to provide answers to the following research questions (RQs):

- RQ1: What characterises the state of IT risk management in Company A today?

- RQ2: How does information security culture in a young technology company compare to the results measured previously in other companies?

- RQ3: What has shaped the information security culture in Company A until this day?

- RQ4: Are engineers perceiving information security culture more positively than non-engineers and what could be the reasons?

- RQ5: Are the employees who are more involved in risk management procedures (employee group A) more promotively minded towards information security than the employees who are less involved in risk management procedures (employee group B)?

- RQ6: What can possibly cause the differences in perception between employee group A and employee group B?

1.5 Chapter overview

In chapter 2 the author provides definition for information security culture and covers literature review, explains what IT risk management is, and briefly discusses the importance of risk management culture. The chapter is completed by explaining the problems young technology companies might face when doing business.

Chapter 3 is dedicated to describing the methodology the author used to conduct the study. The development of the survey and semi-structure interview is also covered in chapter 3.

Chapter 4 focuses on the data analysis and also describes the information received during the interviews. Reliability tests and t-tests are also described in chapter 4. Chapter 5 provides answers to the research questions and is followed by chapter 6 which is for conclusion.

2 Theoretical background

2.1 Information security culture

2.1.1 The concept

In this chapter the author provides an overview of ‘information security culture’. The concept of ‘information security culture’ (ISC) can also be described by using other similar terms, such as ‘cybersecurity culture’ and ‘security culture’. The author has decided to also use the similar terms to explain in a more clear way what information security culture entails.

Among the first ones to define the ‘information security culture’ were Martins and Elofe in 2002 [6]. They explained that businesses are dependent on information assets (e.g. data, hardware, software, etc.) and as need to protect their information assets [6]. To achieve the protection of information assets, technical information security controls can be implemented, but the problem is that these alone are not sufficient [6]. Martins and Elofe claimed that the way people interact with the information assets and the previously mentioned controls determines how effectively the information security controls operate [6].

Martins and Elofe outlined that the way people interact with information security controls and information assets shapes the behaviour and way of working in an organisation [6]. Eventually, the evolved behaviours and ways of working that the people have regarding information security become one part of the wider organisational culture [6]. This part is called the information security culture and can be seen as something that defines and encourages tolerable information security behaviour on three levels [6]:

- Organisational level – this level entails establishing information security policies and procedures and allocating budget for information security purposes. This level is also about measuring and reviewing information security culture in the organisation and conducting thorough risk analysis around the information assets so that the organisation would reach to the desired information security culture;

- Group level – this level means that the management is participating in information security discussions and has responsibilities regarding information security. This level is also about building trust between employees;
- Individual level – this level focuses on improving people's awareness about information security and cultivating good practices and ethical behaviour relating to information security.

According to ENISA[1] 'cybersecurity culture' relating to organisations is described by the knowledge, opinions, perceptions, attitudes, and expectations the employees have about cybersecurity, but also about the norms and values that already have been established within the company [21]. Cybersecurity culture should also cover the way all these previously mentioned aspects exhibit themselves in the organisation [21]. A very similar definition was initially proposed by Da Veiga and Eloff for 'information security culture' in 2010 [22]. Although a slightly different term has been used, the definitions are the same.

Petric and Roer have defined the term 'security culture'. According to them, the security culture revolves around ideas, customs and social behaviour which influence (either positively or negatively) the organisation's security [23]. Although no clear definition was provided to it back then, that same term was also explored by Ruighaver, Maynard and Chang in 2007 [24] – beliefs, long-term strategy, employee motivation, continuous improvement, and staff's social participation in security were recognised as important aspects of security culture.

The described definitions do not differ too much. For the purposes of this paper the author has decided to follow the definition suggested by Da Veiga and Eloff [22] and also ENISA [21] because their definition also takes into account that other norms and values which do not necessarily have to be directly related to information security, can also have an

[1] ENISA stands for European Union Agency for Network and Information Security

impact on shaping information security culture. The author of this thesis also feels that the mentioning of norms and values also provides reasonable coverage for the levels information security culture should work on as mentioned by Martins and Elofe [6].

The following table (see **Table 1**), compiled by the author, conclusively describes information security culture from selected aspects. The author of this thesis has decided to describe information security culture by using five main aspects:

1. parent concept which has wider scientific coverage,
2. general attributes related to information security culture,
3. main influencers that can affect the information security culture,
4. what could organisations benefit from their information security culture,
5. what describes a successful information security culture.

As can be seen from the table below (see **Table 1**), the parent concept to information security culture, as also mentioned in the introduction, is organisational culture [6] [21] [22] [19]. One of the older concepts relating to organisational culture is ‘industrial psychology’ [19] which can also be seen as one of the parent concepts for information security culture. This means that the information security culture is a subdomain of organisational culture – it is the part of organisational culture which pays special attention to information security.

The general attributes that characterise information security culture is that it exists in every organisation (see **Table 1**) [13]. At the same time information security culture may follow different characteristics in various organisations [6] [21]. This means that from organisation to organisation, the information security cultures can differ. This is not the only level where information security cultures can have various presentations as the information security culture can also have several faces within the same organisation. This refers to the fact that several subcultures relating to information security can coexist in the same company [25].

One of the attributes supported by several sources (see **Table 1**) is that the information security culture has the ability to either cultivate the protection of information assets or introduce the information assets to more risks [12] [13] [23] [25]. As already mentioned before, information security culture has several layers which means that information security culture can be viewed from an organisational level, group level and individual level – it covers policies, security budgets, building trust, management, individuals awareness [6].

Table 1. Information security culture described (composed by the author)

Aspect	**Attribute**	**Reference**
Parent concepts	• Organisational culture • Industrial psychology	[6] [21] [22] [19] [19]
General attributes of ISC[1]	• Exists in every organisation • Distinctive across organisations • Either promotes the protection of information assets or imposes risk • Can have subcultures • Has levels/layers	[13] [6] [21] [12] [13] [23] [26] [25] [6]
Influencers	• Changes in the business environment • National culture	[21] [27]
Benefits of ISC	• Promotes security awareness • Minimises threats posed by employees • Enables security while not burdening key business functions • Indirectly determines the effectiveness of information security controls	[21] [19] [6] [21] [6] [12]
Attributes of a successful ISC	• Involves all staff from all levels • Overarches security awareness • Integral part of organisational culture • Adjustable and maintainable • Is maintained continually • Considerate to the needs and practices of the people • Have an effect on the thinking of employees	[21] [6] [21] [6] [21] [21] [26] [21] [21]

[1] ISC stands for information security culture

The author found that there are two main influencers mentioned in the literature. One of them being the national culture as this determines how do people from different nationalities perceive risk in general and whether these people are more focused on placing the wellbeing of the organisation above their own needs [27]. The second main influencer should be the changes that happen in the general business environment (e.g. new regulations, the decision to comply with security standards) [21].

One of the main benefits that ISC brings (see **Table 1**), is the opportunity to enable information security measures without having to complicate the business processes too much [21]. What this means is that the implementation of additional technical or organisational information security controls might reduce the efficiency of business processes and make the business processes slower – not something business managers prefer. This is where information security culture can be of help as it aims to promote values, behaviour and attitudes relevant for effective operation of information security controls [6] [12]. Control environment depends on the people working in that control environment and having negative attitudes towards information security might affect the effectiveness of the controls [6] [12].

From the table above (see **Table 1**), we can see that the attributes that describe a successful information security culture is that it goes beyond security awareness and becomes an integral part of an organisation's culture [6] [21]. In order to be successful it also has to include staff from all levels as this is the only way to take into account what kind of an information security culture would meet the needs of the employees in the best possible way and how to start influencing the way people think about information security [21]. At the same time it is important that the information security culture would be managed continually and that it would be maintainable [21] [26].

To better conclude the concept of 'information security culture', the author has used an illustration (see **Figure 1**). The figure is based on the references mentioned in **Table 1**. The employees knowledge, opinions, perception, attitudes and expectations towards information security determine the information security culture. To avoid the situation where the reader thinks that the information security culture is just another fancy term to describe user awareness about the information security, the author would like to point out that information security awareness relates directly only to the knowledge part illustrated in the figure but as a tool can help improve other aspects of information security culture too.

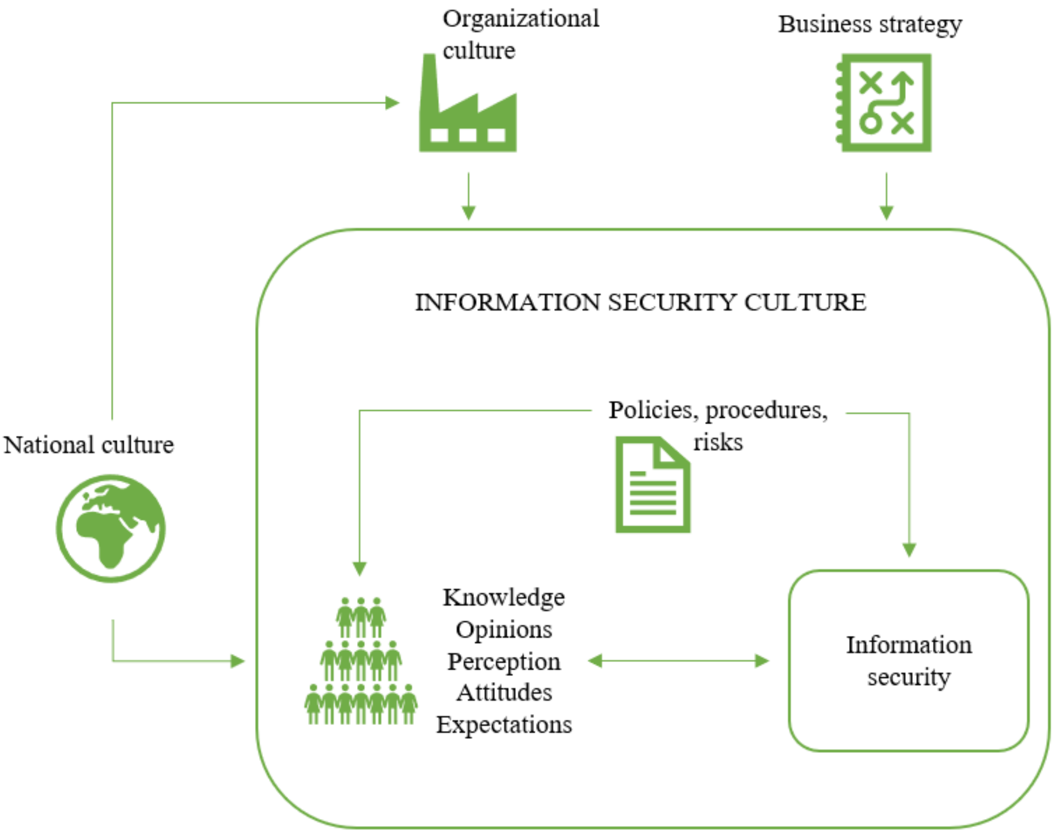

Figure 1. Information security culture illustrated (composed by the author based on the references in **Table 1**)

Employees might have opinions and attitudes which are less dependent on their information security awareness levels and which relate to their national background (national culture) [27]. For example people from individualistic societies tend to put their needs and interests above the needs of the organisation and this might draw them to neglect security controls [27]. In contrast, people who tend to rely more on cooperation and are prone to help each other out also tend to prevent security risks [27].

Information security culture is not only dependent on the people. It is also influenced by business strategy, e.g. changes in the business environment that trigger changes in strategy and reshape the information security culture (see **Figure 1**) [21]. The norms and values agreed within the company (i.e. organisational culture) also influences information security culture [21].

To conclude, every organisation has an information security culture – a set of attitudes, values, norms, behaviour and knowledge that affects the way people interact with information assets and information security controls. Information security culture is different from organisation to organisation and can also have subcultures within the same organisation. Information security culture can exist in a company but without proper work the culture might not turn out to be successful. Without a successful information security culture it is more difficult to promote security awareness, change the way employees think about information security or create a favourable environment for the operation of information security controls. A proper information security culture is managed on various levels – organisational, group and individual level – and meets the needs of the employees. While becoming one part of organisational culture a successful information security culture needs to be managed continually and remain to be maintainable.

2.1.2 Literature overview

As mentioned already in the thesis introduction, the concept of information security culture is not a very recent one. Followingly the author has provided a brief overview on the nature and extent of the academic papers written on that subject. In the second part of the literature overview references to the most relevant studies have been provided.

General literature overview. One of the most extensive state-of-the-art review that has been conducted on information security research papers, was published in 2014 [16]. In this review the researchers assessed the maturity of information security culture as a research field and reviewed 72 scientific papers published between 2000 and 2013 [16].

Maturity of the research area was assessed through the type of research that had been conducted about information security culture [16]. Research that would simply focus on describing the concept of information security culture without clear data or supportive theory was referring to a more emergent type of the research (less mature) [16]. Research which attempted to also interpret qualitative or quantitative data obtained on information security culture or studies which were testing a theory were referring to a more mature type of the research [16].

The researchers found that the information security culture research area is not very mature. The researchers conducting the literature review found that 68 per cent of the papers focused on either just on the concept of information security culture or tried to explain where does the concept of information security culture derives from [16]. As explained before having studies mostly about the concept itself indicates that the research area is not very mature and that more can be achieved in this research area.

Although approximately third of the reviewed papers investigated information security culture cultivation topics, it was evident that no research had been done about gaining more understanding on what kind of impact do different types information security cultures have on information security [16]. This makes it look like the researchers believe into the importance of information security culture (as they are already looking for ways to properly cultivate it), but at the same time it is not too clear what are the benefits of information security culture i.e. how do different information security cultures impact information security or other areas in the organisation.

Although most of the reviewed papers from period 2000 to 2013 were either descriptive, philosophical or theoretical, the researchers noted that during the last years (period from 2009 to 2013) there had been an increase in publishing papers which purpose was to generate new theories or to test different theories [16]. As testing of theories indicates that the research field is becoming more mature, this means that the research around information technology culture is showing signs of moving towards maturity.

The variety of research methods used in information security culture papers was found to be smaller than in the papers focusing on wider information systems research area: the three most popular methods were subjective, case studies, and surveys, and the three least popular methods were qualitative analysis, consultancy, and grounded theory [16]. As for the most popular research methods, similar results were found also by Mirza and AlHogail in their literature review paper in which they reviewed 62 papers from 2003 – 2013 [14]. In addition they have emphasised that only seven papers out of 62 that were reviewed, had relied on more than one research method [14]. This means that in order to drive the information security culture research area even further towards maturity, we should have more studies that use a combination of two or more research methods, for example by combining qualitative and quantitative research methods.

The low usage of combined research methods (e.g. combining qualitative and quantitative methods) was also found to be true in another literature review that included 40 papers published between 2000 – 2014 [28] – only five per cent of the reviewed papers indicated the usage of several research methods. Other parts of the results are somewhat contradicting to the previous literature reviews described above: case studies were found to be the least popular method and for example qualitative studies were the second most popular ones [28].

Although there are some contradicting conclusions made in previous literature reviews, it can be said that as of 2014 the information security culture as a research area still had room for studies that look beyond the definition of the concept. In addition, studies that combine more than one research methods would help to explore the implications of information security culture even further.

However a question might arise on what could be an accepted or possible combination of research methods. In their critical analysis, Okere, Niekerk and Carroll have presented their vision of a thorough approach for assessing information security culture and the usage of several research methods [29]. They argue that using the survey alone is not sufficient when trying to assess information security culture [29]. In addition to surveys, the researchers should also make use of [29]:

- Document analysis – researchers should use document analysis in order to understand what kind of practices, values and goals relating to information security culture are established in the policies and procedures (e.g. analysis of information security policies);
- Interviews – e.g. interviews with the chief information security officer to gather information about the supported values and the general goals relating to the information security culture. It is important to keep in mind that in order to get better understanding about information security culture interviews should also be conducted with people who are not part of information security team;
- Observations – observations could be used to assess whether the information security policies are followed in practice. Observations should follow a formal auditing guideline or procedure so that the observations would be repeatable also in other organisations.

The author of this thesis also searched for newer literature reviews which would cover information security culture research conducted after 2013. The author run advanced searches in Emerald Insight[1], IEEE Xplore Digital Library[2] and Elsevier[3] databases but did not find literature reviews which would be up-to-date. At the same time the author has noticed that information security culture is not just a theoretical topic covered by the researchers. Today, the importance of information security culture is emphasised by overarching organisations such as ENISA [21] and first commercial frameworks have evolved which help businesses measure their security culture [23].

As for the scientific papers, it seems that during recent years the researchers have gone more into detail and have moved towards empirical research. For example Da Veiga, who has for years contributed to the information security culture research area, has switched focus from developing an information security culture assessment framework to investigating what could be the dominant information security cultures and subcultures within a company [25]. Her contribution together with Martins has brought out that people in different job levels (e.g. executive officers vs specialists) perceive security culture similarly but the people who work in IT tend to perceive security culture significantly more positively than the people who do not work in IT indicating the existence of subcultures [25].

During recent years, Da Veiga has also issued other papers. In her 2016 paper she was able to conclude that employees who have read information security policy have a more favourable attitude towards information security culture than the employees who had not read information security culture [30]. In addition Da Veiga’s focus has been on how to transition to the desired culture [26] and how to improve the existing information security culture [31].

When looking into what other authors have written during recent years, it looks like some of them have decided to design their own assessments for measuring information security culture [32], some focus on defining the information security cultural framework [27]. Parsons together with many other collaborators has similarly to Da Veiga focused on

[1] Emerald Insight - https://www.emeraldinsight.com/

[2] IEEE Xplore Digital Library - https://ieeexplore.ieee.org/Xplore/home.jsp

[3] https://www.elsevier.com/

investigating the details [33]. Their work has been able to draw out that organisational information security culture relates positively to having better understanding on and attitudes towards the information security policy [33],

It seems that during recent years the researchers have issued many articles focusing on empirical studies in the information security culture research area. It is possible to see movement from theoretical to empirical and also the topics have gone from more general to more detailed meaning that the papers investigate the relationships information security culture might have with various other aspects such as job levels or professions.

To the author it looked as if previously a lot of focus was on organisational information security culture, but now it seems that information security culture might soon be more researched also on national culture levels. Shifaiz has issued a paper in 2017 whethe indications between national level information security culture are discussed [27]. The author did not find papers about information security culture focusing specifically on young companies and IT risk management procedures which means that this thesis has the opportunity to focus on a possibly new area.

Specific research papers most relevant for this thesis. When concerning the research papers about ISC most relevant for this thesis, the author is able to point out a couple of scientific papers. One of the most important parts of this thesis is the survey the author has conducted. The author has relied on information security culture assessments designed and tested by other researchers which means that some of the most important research papers for this thesis are about security culture assessments.

One of the most important academic papers was issued already over 10 years ago – back in 2008 – by Da Veiga [19]. It is Da Veiga’s PhD thesis which is about cultivating and assessing information security culture. In her thesis, the researcher describes the development and usage of information security culture assessment (ISCA) which to a large extent (with some modifications) has also been used by the author of the current thesis. Da Veiga’s work emphasises the importance of strong ISC within an organisation.

Although the topic is covered in a comprehensive way, the definition Da Veiga provides [19] for the information security culture is similar to the one presented in the beginning of this subchapter and expectedly revolves mainly around shared values, knowledge and behaviours relating to information security. The greatest value about this research paper in connection to this thesis is the survey which development and contents have been disclosed in full – the author did not find any other scientific papers that would disclose so much about the way information security culture could be assessed.

2.1.3 Assessing information security culture

Ways have been developed to measure and cultivate information security culture. In this chapter the author gives an overview of the previous work done in this matter. The research papers written about measuring information security culture would also be a cornerstone for this thesis.

As described already in chapter 2.1.2 it is expected from the researchers that they would use many assessment methods – document analysis, interviews, observations and questionnaires [29]. In addition Okere, Niekerk and Carroll emphasize the importance of using multi-layered assessment meaning that the following four assessment items should be covered in a thorough information security culture assessment [29]:

- Artifacts – these include information security policies, documentation about procedures, content of the information security awareness courses. In order to assess the artifacts the researchers should conduct interviews, document analysis and observations described in chapter 2.1.2.
- Espoused values – the espoused values is a similar layer to artifacts but has more focus on strategy, goals and the vision of the organisation. The same research methods mentioned in the list item above could be used to assess espoused values.
- Shared tacit assumptions – the values, beliefs and assumptions that have become shared and are taken for granted as they have become the core part of organisation’s general culture. This layer is usually assessed by using questionnaires and interviews.
- Information security knowledge – helps to assess whether the employees have adequate knowledge about information security (artifacts), whether the employees know how to address the organisation’s security needs (espoused values), whether the employee’s beliefs contradict to the espoused values (shared tacit assumptions). Knowledge could be assessed by using questionnaires.

One of the few researches that to a large extent follows the assessment approach described above was issued by Schlienger and Teufel [34]. They analysed the information security policy, had interview with chief information security officer, conducted an observation and this way they covered artifacts and espoused values in their assessment [34]. As for shared tacit assumptions they used a questionnaire which was sent to all employees and carried out an interview with chief information security officer. Information security knowledge (the fourth assessment item proposed by Okere, Niekerk and Carroll [29]) was not directly assessed [34]. From the downside, the observation Schlienger and Teufel carried out was not based on formal auditing guidelines (which makes it difficult to reperform the observation [29]) and interviews were limited just to questioning one person – chief information security officer [34].

To the author of this thesis it seems that the most common research method when assessing information security culture in an organisation, is the utilization of a survey/questionnaire and usually the focus is only on a couple of assessment items mentioned above (e.g. on information security knowledge and shared tacit assumptions). Thorough researches which would follow most of the assessment approach defined by Okere, Niekerk and Carroll seem to be a rarity [29].

The questionnaire which serves as the underlying part of the ISCA instrument and which was used by Da Veiga in 2008 in an multi-location organisation [19], was validated a year before [35]. The questionnaire consisted of three main parts – (1) biographical questions (length of employment, office location, etc), (2) information security knowledge statements (statements testing whether the respondent has read information security policy and understands the risk of opening emails from unknown senders, etc.), and (3) information security culture statements (statements helping to determine how the respondents perceive information security culture within the company). ISCA was designed in a way that the respondents were able to use simple scale (“Yes”, “No”) to provide answers to knowledge statements and for the information security culture statements five-point Likert scale was used (“strongly agree”, “agree”, “unsure”, “disagree”, “strongly disagree”) [19].

Before the questionnaire was tested for it reliability, the survey and its purposes were also discussed with the relevant stakeholders from IT, information security, risk management, HR, etc who were working for the financial organisation [35]. After having conducted the survey in the financial organisation, the researchers conducted factor and reliability analysis to make conclusions about the quality of the questionnaire [35]. The authors concluded that although some areas of the questionnaire should be revised, the reviewed version of the questionnaire should provide reliable results [35]. Although the ISCA is already over 10 years old, it was largely based on ISO standard ISO17799: 2005 which today has been replaced with ISO27002 [19] [36]. As ISO standards are also used today in the industry, this should make reviewing and renewing the statements easier for the author of the current thesis.

Another questionnaire which the author of this thesis considers more important, is the human aspects of information security questionnaire (HAIS-Q) which also had been validated by the researchers [20]. The purpose of HAIS-Q was to measure information security awareness with the knowledge-attitude-behaviour model, but in the opinion of the author it includes more up-to-date statements which could be used to further improve and modernize the ISCA [20]. Just like ISCA, also HAIS-Q was tested for validity. It was concluded that HAIS-Q is also a reliable instrument to measure information security awareness. Although HAIS-Q is not directly about information security culture, it is much recent than the ISCA and therefore the author thought this could be used to modernize ISCA.

Da Veiga's study [19] focused on espoused values, shared tacit assumptions and also had a few questions about information security knowledge. She did this by conducting a survey and did not use document analysis, interviews or observation to assess information security culture [19], also Parsons *et al.* [20] did not use other research methods besides a survey, but it had better focus on information security knowledge. Schein argues that questionnaires or surveys cannot be used to assess culture properly in an organisation mainly because the dimensions of culture which are targeted to be covered with the survey items might not match with what is considered important in the organisation [37]. In addition the respondents might interpret the survey questions differently and that diminishes the reliability of the survey [37]. This is the main reason why the usage of several research methods is beneficial when trying to measure information security culture.

2.2 Background on risk management

2.2.1 The concept of risk management

Followingly, the author has explained the concept of risk management and procedures related to risk management. The chapters dedicated to explaining risk management topic are the basis for designing the appropriate statements related to information security risk management procedures to be used in the survey the author has conducted. Special emphasis has been placed on understanding the term ‘information security risk management’ or ‘information technology risk’ as these terms resonate more accurately with the empirical study the author has conducted.

According to Douglas W. Hubbard, risk management is defined as a complex set of processes where the aim is to understand, minimize and control the likelihood and impact the occurrence of a negative event might bring [38]. The goal is not only to avoid the negative scenarios from happening, but also to strategically promote the realization of opportunities [39]. Hubbard believes that the abovementioned complex set of processes consist mainly of [38]:

- risk identification,
- risk assessment,
- risk prioritization, and
- coordinated and economical resource allocation.

In their risk taxonomy standard, the Open Group has explained that the core of risk management is about making decisions – what kind of risks are more critical, what kind of risks can the organisation tolerate, and how to share the budget between the risks that should be addressed [40].

There are two main approaches an organisation can use to manage risks [41]:

1. decentralised approach – risks would be managed one by one and perhaps even in separate business units;
2. centralised approach – the whole risk space is viewed as a whole using a coordinated and strategic framework, also known as enterprise risk management (ERM).

No matter what the approach is, the risk management cannot be seen as a project which has a beginning and an end – risk management is an iterative process [42]. Below (see **Figure 2**) you can see a simplified risk management cycle. Once a company has identified relevant risks, it is important to give the risks a scoring which can then be used to prioritise risks.

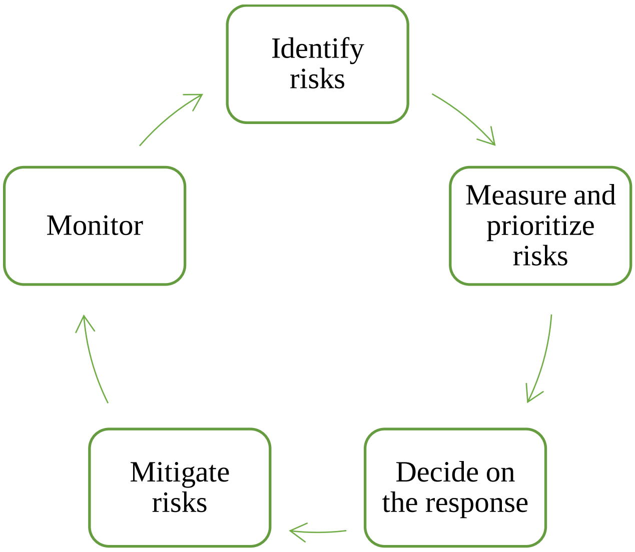

Figure 2. Simplified risk management process (composed by the author based on [38], [43])

Next step (see **Figure 2**) in risk management process is to decide what should be the proper way to address the risks. Risks can be avoided, accepted, reduced or shared [43]. After the decision on risk response has been made, it is possible to start mitigating the risks. However the process does not end there as the mitigative actions and risks should still be monitored for changes: some mitigative actions might prove to work better than others and some risks may become more relevant over time (e.g. whenever there are some changes in the business environment).

2.2.2 Risk management culture

Earlier the author explained that information security culture exists and that it relates to other types of cultures – national culture and organisational culture. The literature claims that there is also a relationship between organisational culture and enterprise risk management, some even have defined risk management culture, also sometimes referred to as risk culture [44].

Study conducted by Kimbrough and Componation in 2015 found that there is a positive correlation between organisational culture and ERM [45]. They divided organisational cultures between two main types – organic cultures and mechanistic cultures [45]. The definitions for organic cultures and mechanistic cultures originated from Reigle's PhD dissertation [46]. Before explaining what did Kimbrough and Componation found, the author gives an overview of Reigle's approach to defining cultures.

According to Reigle, cultures have five culture elements – language, artifacts/symbols, patterns of behaviour, espoused values, and basic underlying assumptions [46]. Language is about the style and direction of communication, and artifacts/symbols is for example about the attire, chain of command and hierarchy, also about the level of openness between the employees working on different levels [46]. Both – patterns of behaviour and espoused values are about the reward system but the first one focuses more on the way achievements are celebrated and espoused values has more focus on the way organisational/business goals are achieves (e.g. through individualism or collaboration) [46]. The last element – basic underlying assumptions – focuses on hierarchy in decision making, also on the level of independence the employees have and how much guidance they need [46]. These five elements were used to define organic culture and mechanistic culture [46]:

- Organic culture – language focuses on heroes and storytellers and on telling positive myths. In organic cultures the employee commitment is emphasised. The communication tends to be lateral. The symbols and artifacts represent support and integration and there are no barriers between employees working in different levels of hierarchy. Celebrating work accomplishments and looking for ways to do even better job are part of the main pattern of behaviour. The espoused values are collaboration and innovation and the basic underlying assumptions are that employees are seen as assets who need little direction.
- Mechanistic culture – language focuses on jargon, negative comments and is usually vertical not lateral. The symbols and artifacts represent segregation of employees based on their hierarchical status within the organisation. Micromanagement and believing that the paycheck itself is the reward are part of the main patterns of behaviour. The espoused values focus on rewards and punishments in order to promote good behaviour. The basic underlying

assumptions are that the employees need detailed guidance and must be forced to work.

Kimbrough and Componation used the culture definitions described above to see if the organisational culture has any effect on ERM [45]. They saw that the study subjects who were from organisations which had established organic culture stated more often that they are happy with the ERM program and its deployment speed and effectiveness within their organisation [45]. One of the conclusions the researchers made based on their study was that organic qualities in an organisational culture might be more desirable when deploying ERM [45].

There are also others who see a relation between risk management and organisational culture. According to Beasly, the iterative process of risk management described in the previous subchapter relates to risk culture [42]. Deloach mentions that culture is one of the key elements in a risk management program [43]. Hubbard believes that it is possible to create an organisational culture which fosters risk management [38].

The ideas covered above could mean that some cultural settings (organisational culture or perhaps even specifically information security culture when talking about IT risk management) have positive effect on enterprise risk management programme. Some set of values, norms, beliefs and attitudes can make the risk management a regular part of everyday work which is favoured by the employees. For example in their work issued back in 1984, Hofstede and Bond [47] discovered that the countries which have more people who avoid uncertainty as they are easily threatened by ambiguous situations, also tend to have more legislations, regulations and laws to have better control over uncertainty [48]. Similar phenomenon might also work on organisational level with risk management.

To take this even further, risk culture as a term has already been defined in the literature. Risk culture is defined as the values and behaviours in an organisation that determine how the employees and management make decisions about risks [49]. The concept was first coined by the Institute of International Finance back in 2008 [50] and focuses on ensuring that the employees are risk-conscious and that the actions taken by the employees would be aligned with the organisational objectives [51].

In order to achieve strong risk culture, the employees need to have a clear understanding about the organisation's business purpose and awareness about compliance rules that are applicable to the business but also the ethics around their own behaviour [49]. Strong risk culture helps to ensure that the decisions made about risks are consistent, effective, timely and sound [49][44].

2.2.3 Information security risk management

Information security risk management, IT risk management and/or cyber risk management are subdomains for general enterprise risk management. Risk management is an integral part of strong information security standards and frameworks – for example it is included in ISO/IEC 27001, PCI DSS, and is also covered by NIST [52][53].

It is natural to believe that these days enterprise risk management revolves at least to some extent around information security risks as businesses have become more dependent on IT solutions. Although the risk domain is more specific, the process of IT risk management is similar to the general enterprise risk management iterative process (see **Figure 2** in chapter 2.2.1) [52]. ISO/IEC 27005 that focuses specifically on information security risk management, outlines the following steps for risk management [54]:

- Identify information risks,
- Estimate probabilities and impacts,
- Generate probability-impact graph,
- Compare and prioritize risks,
- Decide on the risk treatment,
- Treat the risks,
- Evaluate the treatment,
- Monitor, update and learn.

The previously listed steps align with the iterative risk management process described in chapter 2.1.1. So far, we know that the effectiveness of risk management relates to organisational culture and also depends on national culture. Although it seems that this has not been explored in such detail, the author believes that also the effectiveness of IT/security risk management depends on organisational culture. As IT/security risk management relates to information security it might also have connections to information security culture which serves as a subdomain for general organisational culture.

2.3 The challenges faced by young technology companies

As the empirical part of this thesis is focusing on a young technology company, the author finds it is reasonable to also explore what usually describes young technology companies or startups. The author considers the company to classify as a young company if it is less than 10 years old – these companies usually already have strong business operations but they have not achieved the level of maturity in information security and risk management that the established companies have over the decades.

It is reasonable to assume that new companies are established to achieve success, therefore this chapter covers the problems young technology companies might face on their journey towards success. This should provide context when analysing IT risk management procedures and information security culture in relation to the company in the empirical scope of this thesis.

When talking about startups it is believed that their high growth (potential) also links to bigger uncertainty [8]. Establishing the right culture, controls and metrics within the organisation can be a difficult task as the rapid business growth makes the operating environment to change often [8][10]. Technology startups have intense competition. They fight for the investors, skilled labour, and customers [9]. In order to keep up, the leaders of young technology companies have to be able to make their business model attractive to external stakeholders and at the same time they have to be able to secure the stakeholders' trust and loyalty [9].

When comparing young companies to established (more mature) companies, then one of the main differences is that young companies are still fine-tuning their culture, designing their internal processes and finding ways to optimise their performance [10]. Even a single failure can end the operations of a young company [55], whereas experiencing one failure might not bring that drastic outcome for a more mature business. Established companies are also believed to have less problems with communication and collaboration than young companies [55].

A case from 2014 illustrates the fragility of young companies clearly [4]. Code Spaces – a company that was established in 2007 and provided secure code hosting and software collaboration platform [5] – went out of business because it lost most of its customer data, backups and configurations to a hacker [4]. The attack started with a DDoS attack which might have served as a smokescreen attack to distract the attention [56]. The main goal for the attackers was to conduct intrusion attacks targeting Code Spaces’ Amazon EC2 control panel and destroy the data [4]. By the time Code Spaces got their panel access back, the attackers had already deleted substantial amount of data and the young viable business had to close its doors in 12 hours after the attack [57]. The author of this thesis would like to point out that there is no information about the way attackers got the access, but this example illustrates how security risks can put an end to a young company.

General risks and information security risks are incapable of choosing which companies to lure. No company is mature in terms of risk management or information security management at the moment of establishment. At the same time even the newly established companies should somehow deal with risks, corporate governance and information security management. When focus is heavily on growth and innovation (or else the young company might lose its competitive advantage), the activities supporting the business – risk management and information security management – might receive less attention.

Perhaps this is one of the reasons why startups should pay extra attention on establishing organisational culture and other sub-cultures (e.g. information security culture and risk management culture) – this way the company is still able to focus on innovation and growth but the risks would not go unseen. As the company matures, the various risk management processes also mature – with the proper culture the process of becoming more mature might mean less struggle.

3 Methodology

3.1 Research method

The author decided to use a combination of two research methods: survey and interviews. As discussed in chapter 2.1.3, surveys alone might not provide a fair indication of a company's information security culture which means that the author could benefit from the usage of other – qualitative type – research methods. The data received by conducting a survey would be analysed using quantitative analysis and the information received via interview process would add a qualitative dimension.

Using a combination of research methods is one of the aspects which makes this study a more relevant addition to the information security culture research area as still not many researchers use hybrid approach when it comes to research methods (see chapter 2.1.2). The benefit of using a hybrid approach is that once the survey results have been analysed, it is possible to use the information gathered during interviews to put the data analysis into a context applicable in the company.

The research analysed in chapter 2.1.3 emphasised that interviews should not only seek the opinion of the chief information security officer and also other stakeholders should be interviewed. The author of this thesis gathered the views, opinions and experience from different stakeholders of Company A (see chapter 3.5.2 for more details). Combining quantitative and qualitative research methods and conducting several interviews with different stakeholders is one the aspects that makes this thesis unique.

The author has decided that a semi-structured interview would work the best. The idea is that the author would be able to prepare some questions for the interview but at the same time also follow-up on the unforeseen topics or aspects that rise during the interview discussion. Semi-structure interviews allow the interviewer to prepare the interview structure which does not restrict the discussion too much allows the interviewee to express their own views [58].

3.2 Request for collaboration

The author was interested in conducting a research in a young technology company operating in Estonia. The author reached out to four young technology companies and presented a general request for collaboration. Two out of the four companies responded that they felt unprepared for participating in such a research as they both had just started building up their information security function. The same two companies mentioned that they might be ready and willing to participate in such a research in the following years.

The other two companies responded positively and with those two companies the author started the collaboration. Company B was the first one to respond positively to the request for collaboration and a few weeks later also Company A gave a positive response. A more detailed request for collaboration explaining the purpose and scope of work was presented to both companies. Also non-disclosure agreements were signed with both companies.

The survey ran in Company B served as a pilot survey after which the author was able to adjust the survey to be more usable to the respondents, and the survey ran in Company A served as the main part of this thesis. Data analysis was conducted on the data obtained from Company A. Data analysis was not conducted on the data obtained from Company B as the response rate was too small. The author has described this in more detail in the following chapters.

3.3 Ethical considerations

Information security as a topic is most likely a sensitive one for many companies. Revealing too much information about company's information security practises or culture can for example be used by adversaries for intelligence gathering. This is why it was important to clearly communicate the purpose of the research to the relevant stakeholders in Company B and Company A right from the beginning. It was agreed with both Company B and Company A that real company names will not be used in the thesis, also it was agreed that the opportunity to describe the companies in the thesis with various well known statistics should be limited. This is because Estonia is a small country and there are not many similar young technology companies operating here – most of them are slightly different and therefore easily identifiable.

At the same time the survey results provided by the employees of Company B and Company BA should be disclosed prudently. As some of the questions in the survey contained company specific information, the results have been provided on an aggregate level without disclosing for example the full list of departments or job position names relating to the company. This is also the reason why these parts in the survey are obfuscated in the appendices (see Appendix 1) – the author has presented the survey questions but has not presented the detailed response items relating to these questions.

The survey respondents are all natural identifiable persons. Having information on how they perceive information security culture, what is their knowledge about information security, or how involved they are in IT risk management procedures means that personal data will be processed. It is essential to follow the best scientific practices when analysing or disclosing the results from such data. In order to provide anonymity, the author used data obfuscation and data aggregation methods so that the analysis would not make it possible to connect the results with an identifiable natural person.

In some cases the respondents gave very specific descriptions of their job tasks and for these cases the author replaced the specific descriptions with a more general classification according to the official classifications defined in Company A. In addition, as it is also possible to identify natural persons when combining two or more survey items (e.g. knowing the job title and the office location), the author also decided to carry out the analysis on a more aggregate level.

In other words, although there were more office locations listed, the author defined two general locations – office within Europe and office outside of Europe – and conducted further analysis on aggregated data. The same aggregation method was used for job titles – instead of conducting the analysis on detailed job titles, they were mapped as engineering positions (e.g. software developers, product development project managers) and non-engineering positions (e.g. HR analysts, marketing specialists).

As the data confidentiality was important, the author set up a separate and dedicated account where to store the online survey results. The data gathered will be deleted after the thesis project has been defended. The same will be done with the notes taken during the interviews.

3.4 Survey preparation

3.4.1 Designing the draft survey

The author designed a survey that would allow gathering of general data about the respondent’s job status, data about the way respondent’s daily job tasks relate to risk management procedures and data about their perception towards information security culture. This means that the designed survey consited of four main parts:

1. Background information/demographical questions (such as the length of employment, their office location, current role and business unit)
2. Exposure to risk management processes
3. Information security knowledge statements
4. Information security culture assessment (ISCA)

The first part of the survey (see questions 1 to 4 from Appendix 1) was separately tailored to fit first with Company B and later on with Company A. This gave the respondents a simple way to choose the most applicable job description and most applicable office location. Data analysed across these questions was obfuscated and aggregated in order to not reveal the structure of the company or the specific respondents.

The second part of the survey (see statements 5 to 19 from Appendix 1) included statements about IT risk management aspects and procedures. For these statements the respondents had to evaluate how much does their daily work revolve around various IT risk management procedures. The statements were derived from the theoretical background about information security and IT risk management process (see chapter 2.2 and its subchapters).

Statements 8 to 13 (see Appendix 1) have more direct connection to the theory of IT risk management described for example in chapter 2.2.3. Statements 5 and 6 aim to determine the owners of information assets and business processes as in a technology company these people might also focus more on IT risks around these assets and business processes. For the 7th statement the author has assumed that IT risks stored in company’s risk register and the people who know how to find the register, should have a more significant role to play in risk management procedures on a daily basis. The rest of the statements (statements 14 to 19 in Appendix 1) about IT risk management procedures were included by the author to also cover more specific areas (e.g. ensuring physical security, collaborating with external auditors, managing access rights) indicating the respondent's participation in IT risk management procedures.

The third part of the survey – information security knowledge part – and the fourth part of the survey – information security culture assessment part – were mostly adopted from Da Veiga's work [19]. Da Veiga's dissertation from 2008 was used because it was a relevant and reliable tool designed to measure information security culture within companies. It was also the only publicly available research paper that included the full description of information security culture assessment. This gave the author the opportunity to adopt an assessment that had already been tested and proved to be reliable.

In the field of IT a lot can change over the years. Da Veiga's work was from 2008 which meant that at the time of adoption it was already over 10 years old. Da Veiga's latest articles suggested that the ISCA has evolved over the years but there were no clear details available about the direction of this evolvement [26]. The author of this thesis tried to reach out to Da Veiga in order to obtain more information on the current state of the ISCA, but unfortunately did not receive a response. Therefore the author decided to analyse the statements in the information security culture assessment and modify them so that the ISCA would include relevant and modern statements.

Firstly, the author learned what served as the base framework for Da Veiga when designing the assessment. It turned out that to a large extent Da Veiga followed ISO/IEC 17799 – code of practice for information security management , which according to the International Organization for Standardization has been replaced by ISO/IEC 27002 [36]. As the assessment items in Da Veiga's thesis were structured according to the structure of ISO/IEC 17799, it gave the opportunity to compare the structure to the new standard to evaluate the need for possible changes. For that the author followed an online description of ISO/IEC 27002 [59]. As a result the author of this thesis decided that no major changes should be introduced, which means that at this point the structure of ISCA remained the same.

Next, the author decided to analyse the statements and evaluate their relevance to young technology companies. Many of statements needed to be clarified and simplified for the reader. Also as time was an important constraint for collecting the responses, it was decided to remove repetitive statements. The author is aware that repetition does have an important role to play in surveys used in social sciences but the focus of this study would not take full advantage of repetition simply because the author is not fully familiar with the methodology behind the analysis of similar statements. In addition, the author was advised to reduce the number of questions as otherwise the time spent on completing the survey would have been longer which would have meant less responses.

The author noticed that in many cases the examples initially provided to clarify the information security assessment statements to the reader were outdated. These were replaced with more relevant examples. Some of the statements in the information security knowledge part were completely replaced as they seemed not to fit well with the rest of the statements. More appropriate statements were found from HAIS-Q – a survey designed to measure the human aspects of information security [20].

Da Veiga had used a five-point Likert scale ("strongly agree", "agree", "unsure", "disagree", "strongly disagree") to measure the respondents' information security culture perception [19]. The author of this thesis discussed the usage of five-point Likert scale with a social scientist working in TalTech – Dr. Tiiu Kamdron – and at first it seemed as if a six-point Likert scale ("strongly agree", "agree", "slightly agree", "slightly disagree", "disagree", "strongly disagree") should be used instead. Dr. Kamdron's advised that leaving the respondents the opportunity to give a neutral response does not help to measure the perception that well. The author saw that the six-point Likert scale had its advantages compared to the five-point Likert scale and therefore, the first version of the survey used six-point Likert scale.

As a last step the whole survey was assessed by four peers. One of them had technical background – the peer was a software engineer – and three of them had no background in IT – legal specialist, human resource analyst and a sales representative. The feedback gathered from the peers helped to detect which of the statements were difficult to read (i.e. the peer had to read the statement more than once to understand it) and needed to be adjusted or which ones did not make sense at all. They also helped to spot grammatical and typographical errors. As a result some of the statements were rephrased and/or accompanied with examples.

The fact that the author made modifications (removed statements, rephrased statements) to the information security culture assessment tool which once proved to be reliable, means that the reliability of the tool was now under question. In addition, the reliability of other parts of the survey – i.e. the IT risk management procedure statements – was unknown as this was developed specifically for the purposes of the current study. This means that the author would be basing their conclusions on an assessment tool which reliability is unknown making it also difficult to draw meaningful conclusions. In order to understand whether the tool can be relied on, the author calculated the Cronbach's alpha values after the results from Company A had been obtained. See chapter 4 for more detailed results.

3.4.2 Conducting the survey in Company B

The survey conducted in Company B served as a pilot survey. Before the survey launched in Company B, it was introduced to the information security officer and reviewed by the information security specialist. The main feedback was that the amount of questions is too big (it was close to 100 statements at this stage) and that some people might not know how to respond to certain statements as there is no way to respond in a completely neutral way (because the author decided to use 6-point Likert scale which excludes the opportunity to respond with "Unsure" or similar).

The author decreased the number of questions to 77 but decided to still use six-point Likert scale (strongly agree, agree, slightly agree, slightly disagree, disagree, strongly disagree) for the statements about information security culture. The author wrote a description to introduce the survey and its goals and also committed to donate two euros to a charity for each response that would be received. The information about donation was also included in the survey description. It was agreed that all the communication and promotion about the survey would be done by the information security specialist working in Company B, the author was not given direct access to help with the internal communication.

The survey launched in March and the survey was open for three weeks. One official reminder was sent out during that period. During this time the author managed to obtain 19 responses. In order the data analysis to be meaningful the minimum number of responses needed was 82. In Company B, this sample size (82) would have provided the confidence level of 95% and confidence interval of 10 [60] – the author felt that tolerating a larger confidence interval would have decreased the strength of conclusions too much.

Due to the low response rate, the survey conducted in Company B served as a pilot survey or test run which the author used to improve the survey experience for the prospective respondents in the future. Running the survey in Company B gave a strong indication that the survey was not easy enough to respond to: the statements were too difficult to follow and not all employees must know how to respond to all of the statements. The feedback received from Company B's information security specialist confirmed the same.

Conducting the survey in Company B forced the author to conclude three main things: (1) it might be worth to change the answers back to five-point Likert scale just like Da Veiga [19] used as this would provide the respondents with the option to exhibit neutral opinions about the information security culture statements; (2) the wording of the statements needs to be reviewed again to further simplify the reading process for the respondent; (3) it is worth trying to send more notifications about the survey as this might increase the number of respondents. The author followed all three conclusions to further improve the survey and response rate for other companies.

3.5 Data collection

3.5.1 Conducting the survey in Company A

The author took the experience gained from conducting the survey in Company B and adjusted the survey. In the new version of the survey a five-point Likert scale was used, leaving the respondents the opportunity to stay neutral with their response.

Overview of the survey was given to information security officer and senior information security specialist but as the survey relates to organisational culture their recommendation was to confirm the contents of the survey also with the human resources specialist focusing specifically on organisational culture. The human resources specialist had a lot of experience conducting similar surveys within Company A and agreed to have a meeting to analyse each and every statement in the survey. This allowed to further simplify the language and examples used in the statements.

The human resources specialist also mentioned that usually it is not possible to reach to the desired response rate by simply advertising the survey in general communication channels. From her experience the rule was that if an *x* amount of responses are needed, then a random sample of *2x* employees had to be messaged directly about the survey. The author needed to get at least 91 responses from Company A to be able to draw meaningful conclusions. Sample size of 91 was determined using the online sample calculator: according to the online sample calculator the sample size of 91 would give confidence level of 95% and confidence interval of 10 [60]. This meant that approximately 180 employees needed to be messaged directly.

The survey was launched in the end of March and was closed in the beginning of April. Two posts were made in the general communication channel (the second one serving as a reminder). The whole count of responses received was 104 and the general communication done about the survey brought about 40% of the responses. The rest of the responses were obtained thanks to sending direct and more personalised messages to a random sample of employees. Altogether 188 employees were directly messaged about the survey.

3.5.2 Preparing and holding the interviews

As mentioned before, it was decided that a semi-structured interview should be used to conduct the interviews as this would leave the interviewees more room for their own thoughts. The author decided to have interviews with six employees – chief information security manager, senior information security specialist, junior information security specialist, human resources specialist focusing specifically on organisation culture topics, software engineer not working in security team and a customer support agent. The people from security team were selected as interviewees as they are responsible for information security in Company A. The HR specialist was selected as she works specifically on organisational culture matters. The software engineer and customer support agent were selected for the interviews as these two job positions have the most people in Company A.

The author came up with the following interview structure to be used during the interviews:

1. Introduce the purpose of the discussion to the interviewee.

2. Emphasize that the results of the discussion is to be presented in the thesis and that the interviewee should feel free to let know if any of the questions or discussion points seem inappropriate or they do not want this to be recorded in the thesis.
3. Explain what was the survey about, which parts did it consist of and what is the general purpose of analysing the survey results.
4. Accompanied by the appropriate visuals (charts) provide a general overview of the survey results to the interviewee.
5. Ask the interviewee to describe the company from (IT) risk management perspective.
    a. Related terms to lead the discussion: centralised vs decentralised approach, maturity, confidence, proactive vs detective approach, risk prioritisation, ownership employee involvement, risk management guidelines, methodology
    b. Related questions to lead the discussion: Does risk management cover entire enterprise or only some parts of the organisation? Are risks continuously assessed or not?
6. Ask the interviewee to describe what currently serves as the most underdeveloped part of (IT) risk management in the company.
    a. Related questions to lead the discussion: What should be handled better?
7. Accompanied with the appropriate visuals (charts) introduce the interviewee the results about risk statements and hold a general discussion on the results.
8. Ask the interviewee to describe the information security culture in the company.
    a. Related questions to lead the discussion: Is the information security team visible enough? Do people find the security rules too restraining as the company is not a corporate environment?
9. Ask the interviewee to describe what could be done in the company to further foster the favourable perceptions employees have about information security.
10. Accompanied by appropriate visuals (charts) introduce the interviewee the results on selected (ten strongest, ten weakest and biggest uncertainty) information security culture statements and hold a general discussion on the results.

11. Explain how do the information security culture results compare to other researches and let the interviewee discuss what could cause the similarities or dissimilarities.
12. Present the interviewees with a table (see Appendix 2 – Organisational culture characteristics perceived by the interviewees (complied by the author based on **[45][46]**)) based on Reigle’s work [45][46] that in a random order lists organisational culture elements and characteristics of organic culture and mechanistic culture. Do not reveal to the interviewees which characteristics respond to which culture type and ask the interviewees to select the culture characteristics that in their opinion are strongly applicable to Company A. Mention that they can choose as many or as little characteristics they want.

The author conducted separate interviews with each interviewee by following the interview structure described above. The author did not record the discussions but took notes on the responses during the interview. In order to store the opinions of the interviewees for the 12th interview point a separate file was created for each interviewee so that they could record their opinion in the table (see Appendix 2 – Organisational culture characteristics perceived by the interviewees (complied by the author based on **[45][46]**)). Each interview lasted for about 45 minutes.

4 Data analysis

In this chapter the author has presented the analysis relating to the survey. For IT risk management procedure statements and the security knowledge statements the respondents were able to respond using a three-point Likert scale (“yes”, “no”, “unsure”). For the information security culture statements the respondents were able to respond using a five-point Likert scale (“strongly agree”, “agree”, “unsure”, “disagree”, “strongly disagree”). In order to conduct data analysis, the author transformed the scales into integers. Responses on three-point scale were assigned numbers from 3 to 1 and responses on five-point scale were assigned numbers from 5 to 1.

The survey included also some reversed statements (marked with an asterisk in Appendix 1) which means that the responses should not be graded the same way as the rest of the statements as the meaning of the response is opposite. The responses relating to the reversed statements were assigned to integers in the opposite direction (e.g. “strongly agree” was not transformed to a 5 but a 1 instead). After this was done, the author was able to carry on with the data analysis.

Followingly, the author has described how the reliability of the survey parts were assessed and how reliable the survey parts are. In the proceeding parts of chapter 4, the author has described the general information obtained during the interviews. Part of the information gathered during the interviews has been analysed together with the quantitative analysis as presenting the quantitative and qualitative analysis next to each other, should provide better context for the survey results.

4.1 Reliability of the survey

The author described the creation and modification of the survey in chapter 3.4. In that chapter it was described that the survey has largely been based on existing surveys which had been tested for their reliability. However, the author felt the need to modify the existing survey and also add a survey part focusing on IT risk management statements.

This means that as an assessment tool the survey reliability is unknown and should be assessed before drawing any conclusions on the data.

The author has used Cronbach’s alpha to determine whether the survey parts are reliable or not. The reliability which can be determined by using Cronbach’s alpha test helps to estimate how consistent the survey results would be if the same respondent took the survey several times [61]. The Cronbach’s alpha values normally stay between 0 and 1 – the closer the result is to 1, the more reliable the survey instrument is [61]. Values above 0.70 are associated with good reliability and values starting from 0.90 are associated with the best reliability [61].

The formula for calculating Cronbach’s alpha consists of three variables (see **Equation 1** below) – number of questions/statements (k), variance of the scores across the questions/statements ($\sigma_{y_i}^2$), and variance of the total scores across respondents (σ_x^2) [62]. The formula is the following:

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

Equation 1. Cronbach's alpha calculation formula [62]

As the survey used by the author consist of three assessment parts – statements about IT risk management procedures, statements about security knowledge, and statements about information security culture – the author decided to calculate the reliability for each part separately. This approach makes sense as these survey parts resemble different logical parts and are also measured differently. The following table (see **Table 2**) presents the results across survey parts.

Table 2. Reliability indicators across survey parts (composed by the author)

Survey part	Indicator	Value
IT risk management procedure statements	Number of statements	15
	Sum of $\sigma_{y_i}^2$	11.6066
	vσ_x^2	52.9955
	Cronbach's alpha	0.8368
Security knowledge statements	Number of statements	10
	Sum of $\sigma_{y_i}^2$	3.2104
	vσ_x^2	6.5588
	Cronbach's alpha	0.5672

Survey part	**Indicator**	**Value**
Information security culture statements	Number of statements	48
	Sum of $\sigma_{y_i}^2$	34.2718
	vσ_x^2	359.0662
	Cronbach's alpha	0.9238

Table 2 above shows that the set of IT risk management procedure statements are reliable as the Cronbach's alpha value is above 0.8 (minimum tolerance is at 0.7). This value indicates that although the combination of statements is reliable, it has room for improvement in the future. The only part of the survey which has lower value for Cronbach's alpha is the set of security knowledge statements. The author takes this into account and understands that the set of knowledge statements should not be used to measure the respondents knowledge levels. We can also see that although the author removed and modified some of the statements the set of information security culture statements are still reliable – the Cronbach's alpha value is over 0.9. The author takes into account that the knowledge statements do not provide reliable measures, but the rest of the survey is reliable and conclusions can be based on the data gathered.

4.2 General results from interviews

The author has presented part of the interview results together with quantitative data analysis in the following chapters. The more general information obtained during the interviews has been briefly described in the current chapter as this aims to provide background information to the reader.

In order to get an indication on what type of organisational culture dominates in Company A, the author decided to use Reigle's [46] definition for organic culture and mechanistic culture (see Appendix 2 – Organisational culture characteristics perceived by the interviewees (complied by the author based on **[45][46]**). As organisational culture and information security culture and organisational culture and enterprise risk management share a connection (see from chapter 2), the author saw that getting an indication about the prevailing organisational culture might help to build a better context for data analysis.

In order to indicate which characteristics strongly relate to Company A, the interviewees were able to choose as few or as many organisational culture characteristics as they wanted. The results are presented in Appendix 2 – Organisational culture characteristics perceived by the interviewees (complied by the author based on **[45][46]**). The only characteristics which did not receive a single vote by the interviewees represented mechanistic culture. None of the interviewees felt that the workhours are closely monitored, paycheck is the reward or that micromanagement exists in Company A. They also did not believe that carrot and stick reward system exists and that people push away responsibility or that employees must be forced to work.

The interviewees did vote for some characteristics which represent mechanistic culture, but mostly these characteristics only got one vote out of six possible: negative comments, symbols enforce segregation, and employees need detailed direction being those characteristics. As an exception, there was one mechanistic culture characteristic that received four votes out of six: it turns out that the language used in Company A might have too much acronyms and jargon in it. See more detailed results from Appendix 2 – Organisational culture characteristics perceived by the interviewees (complied by the author based on **[45][46]**).

All the characteristics connected to organic culture received at least one vote from the interviewees. The organic culture characteristics that received at least four votes out of six possible were: collaboration, employees are important assets, employees need little direction, and people look for ways to do their job better. See more detailed results from Appendix 2 – Organisational culture characteristics perceived by the interviewees (complied by the author based on **[45][46]**).

The previously described results indicate that in the eyes of interviewees a more organic culture prevails in Company A. There are some signs of mechanistic culture, but they do not seem to be as strong (except for the language using jargon and acronyms). Based on the Kimbrough and Componation's study results [45] this might mean that the employees also in Company A have a positive mindset towards the risk management practices. On an employee level and in the scope of this thesis this can perhaps be seen from how many of the survey respondents claim to be involved in IT risk management procedures.

The discussion with the interviewees also revealed some other general aspects of organisational culture in Company A. One of the main revelations was related to the way communication works in Company A – although there is some communication that flows from top management down to the non-managerial employees, the most natural way of communication flow in Company A is from non-managerial employees to top management. According to the interviewees this refers to the non-corporate style of communication: the messages, goals or whatever other incentives must first be vouched by the people in the first layers of hierarchy so that they could then convince their leaders and managers to do the same thing.

The interviews outlined that the way communication works in Company A is also related to the autonomy the different teams within the company have. Teams are allowed to decide the direction of the project because Company A trusts the team effort. The people working in Company A have shared responsibility. Many of the people are not working in the company just for the money but they want to feel that they have a bigger mission to carry out in Company A. There is no focus on fear and people get to put more emphasis on the projects or making decisions which they believe would further fuel the business development. At the same time the interviewees admitted that the business growth being rapid poses some challenges to establishing and cultivating information security culture. This resonates also with what Hall [8] and Hunckler [10] stated (see chapter 2.3).

It was pointed out that some of the information security culture aspects already have merged with the general organisational culture in Company A. For example, the employees in Company A notice whenever someone leaves their computer screen unlocked and in a friendly way make the user of the computer understand that they have been misbehaved. Interviewees mentioned that although the general attitude towards information security has been positive, the security team should focus more on involving other people into security matters and decreasing the distance between security team members and the rest of the employees in Company A. That would help to increase the visibility over the space of problems handled by the security team and share responsibilities with the rest of the company.

The (IT) risk management domain in Company A was described by the interviewees as something that is still maturing. This means that officially the risk management is usually the responsibility of a few people and teams in Company A. At the same time it was pointed out that there is significant collaboration with regards to learning from past mistakes. According to the interviewees the teams are open about the risks and talk about them, give feedback and if needed make corrections to address the found risks.

The interviewees brought out even more details about information security culture and risk management in Company A. The author has decided to cover these details together with the survey data analysis in the following chapters.

4.3 General statistics relating to the survey

The total number of responses needed for this survey was 91. This number of responses gave the confidence level of 95% and confidence interval of 10[1]. The author has presented the general statistics about the survey results in the following table (**Table 3**): the first column lists indicators about the demographical questions, the second column provides the value for the indicators, the third column states the total observations per each indicator and the last column presents the shares across the indicators (e.g. answers the what was the share of engineers from the total sample size).

The sample size *N* achieved was 104 (see **Table 3**). Around 58% of the respondents have worked in Company A longer than a year (*TENURE: LONGER*) and around 42% have worked in Company A less than a year (*TENURE: SHORTER*). As these two shares do not differ much then in terms of tenure the sample does not seems to be skewed towards one tenure group or other tenure group.

Table 3. General statistics on survey responses - whole sample (composed by the author)

Indicator	Value	Total	Value share out of total (%)
N	104	104	100.00
TENURE: LONGER	60	104	57.69
TENURE: SHORTER	44	104	42.31
EU	79	104	75.96
NON-EU	25	104	24.04
ENG	30	104	28.85
NON-ENG	74	104	71.15

[1] The author is aware that usually confidence interval of 4 is set as a goal in scientific research papers. However when planning the survey, it was clear to the author that the restrictions (time and respondents' interest to fill in the survey) will only make it possible to achieve confidence interval of 10.

The sample is more skewed towards employees who work in Europe (*EU*) (see **Table 3**) – their share is around 76%. Only 25% of the respondents work from outside Europe (*NON-EU*). The sample is also more skewed towards non-engineers (*NON-ENG*) – employees who do not work in IT engineering departments or whose current role in the company is not related to software engineering (e.g. software development) – as their share in the responses is respectively about 71%. Almost 30% of the respondents work as engineers (*ENG*).

At first, the sample being skewed towards non-engineers and employees who work from Europe seemed to be something to worry about. But when the author compared the respective sample shares with the shares calculated for the whole company, the shares were similar. Therefore, the author believes that the sample represents the population in Company A fairly.

The following table (see **Table 4**) presents the average values for three indicators – involvement in IT risk management procedures (*RISK*), average grade for information security knowledge (*KNOWLEDGE*), average grade given to information security culture (*CULTURE*). Next to the average values also maximum possible value and value share out of maximum possible is presented. The last two columns present count of statements that the survey had about each indicator and the average rate of statements to which the respondents replied with "Unsure".

Table 4. Risk-knowledge-culture results - whole sample (composed by the author)

Indicator	**Average value (value)**	**Maximum possible (max)**	**Value share out of max (%)**	**Count of statements**	**Average unsure rate (%)**
RISK	5.59	15.00	37.27	15	10.93
KNOWLEDGE	8.13	10.00	81.30	10	10.96
CULTURE	3.92	5.00	78.40	48	18.60

We can see from the table that the average respondent associates their daily job to about five out of 15 IT risk management procedure statements presented in the survey (see **Table 4**). As Company A is a technology company, it is reasonable to believe that various people in the company are involved in IT risk management procedures. When presented the results, the interviewees in Company A revealed that they did not expect to see that high involvement in risk management procedures as they mentioned that in general risk management procedures are only the responsibility of certain teams and people, and IT risk management procedures are even more specific.

The respondents were also able to respond with “Unsure” to the IT risk management procedure statements, but it seems as they were mostly confident in their responses (i.e. they were able to choose either “Yes” or “No” and not reply with “Unsure” extensively). On average the respondents used “Unsure” only for about 11% of the IT risk management procedure statements (see **Table 4**).

As for the ten information security knowledge statements, the respondents were able to answer with “Yes” on average about eight times out of 10 (see **Table 4**) which means that the information security knowledge describing the average respondent is approximately at 80%. This was seen as a positive result by the interviewees. As for the information security culture, the average grade given by the respondents was 3.92 (out of 5.00) which indicates that employees in Company A seem to have a favourable perception towards information security. At the same time on average around 19% of the information security culture statements (out of 48) were responded to with “Unsure”. This could indicate that there is a substantial share of uncertainty in the way the employees perceive information security culture in Company A. Uncertainty can indicate that in Company A, the information security culture is something which is in the process of taking shape in the eyes of the employees.

IT risk management procedure statements. When exploring which were the most favourable IT risk management procedure statements among the respondents (see **Figure 3**), it can be seen that employees’ work tasks are more often related to classifying information assets, also over 50% see themselves as being the owner of at least one business process and having to detect risks around the usage of information technology solutions.

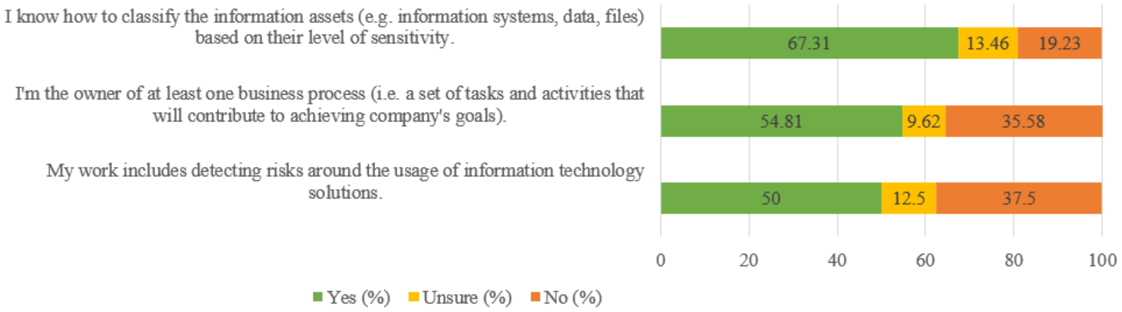

Figure 3. IT risk management statements favoured at least by 50% of the respondents (composed by the author)

As for the least popular IT risk management statements (see **Figure 4**), it can be noted that not that many respondents work with physical security, data retention topics, policies, or need to conduct due diligence procedures when choosing new software vendors. Also not many people know where to find company's risk register.

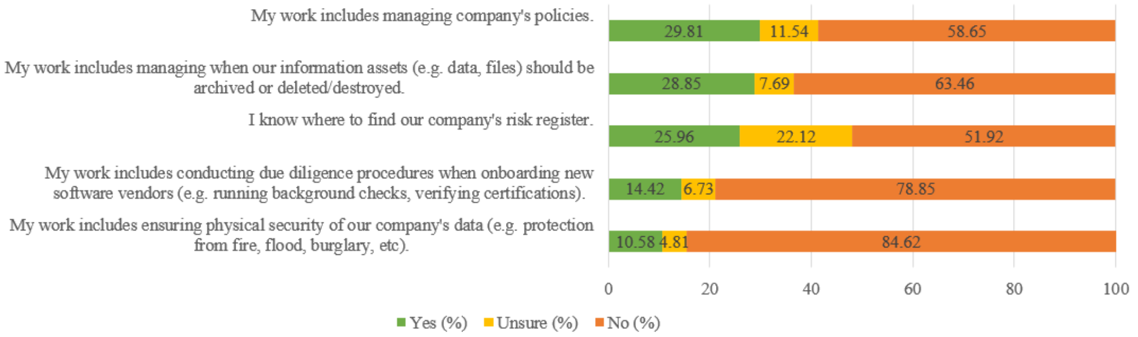

Figure 4. IT risk management statements favoured by less than 30% of the respondents (composed by the author)

When asked from the interviewees about the way the company's IT risk management is currently organised, the interviewees described that in general there is a positive and favourable attitude towards risk management in Company A, but at least for now risk management is the responsibility of a few people from few teams across Company A. According to the interviewees this also means that risk management execution could be better. According to the interviewees, although the employees in Company A do not always talk about risks, in general the people in Company A are transparent and open about risks and their behaviour indicates that risks will not go unseen. The interviewees believe that the knowledge on where the risks are has been going up which means they are able to spot the risks more accurately.

According to the interviewees, there are teams that deal with risks on a continual basis and there are teams within Company A that check the risks once a year. According to the interviewees, one of the weakest points in current risk management approach is that the teams should try to have even better visibility about the risks, documenting them is not that vital. Another problem is legacy applications – in company A these are considered to be all the systems which are more than three years old. It is often difficult to find the time and go back redesigning the older systems.

The interviews outlined that in order the employees to pay more attention to risks, it is always beneficial to come up with a joyful incentive – e.g. one of the things which has become part of the general organisational culture in Company A, is the way people let their colleagues know that leaving the computer unlocked: when seeing free access to someone's laptop a friendly message is sent to the rest of the company on behalf of the user who accidentally left their laptop unlocked. According to the interviewees these kind of joyful incentives get more attention and make people wanting to be involved in the security matters.

The interviewees were able to provide additional reasoning for the IT risk management procedure statements for which the involvement is lower (see **Figure 4**). Although work on that has been started, data retention is not something that is widely spoken about in Company A, as the company is less than 10 years old and the legislation allows to keep the focus away from that area, at least for now.

As for conducting due diligence procedures in relation to new software vendors, the lower value can be explained by the fact that many of the technological solutions used to be built in-house and Company A has only recently started collaborating with external software vendors on a larger scale. Also, the responsibility to conduct due diligence procedures is limited to few people. The reason why many people do not know where to find company's risk register relates to the fact that the company-wide risk register is not something that is shared with all the employees – only designated people have access to the risk register.

Information security knowledge statements. Due to the fact that information security knowledge part of the survey turned out to be not reliable, no definite conclusions can be made about knowledge statements, but the author has still decided to present the results and discussed them with the interviewees.

As mentioned before, the average grade for information security knowledge statements was above eight (maximum possible was 10). All respondents were sure that they knew what the risk is when opening e-mails from unknown senders (see **Figure 5**). The result might be related to the fact that phishing exercises and trainings had been recently conducted in the company. What is more interesting though is that over 88% of the respondents knew that Company A has a written information security policy but at the same time only around 63% of the respondents knew where to find the information security policy. Interviews brought out that there is a lot of information to absorb it is often difficult to find all the relevant information at once in Company A.

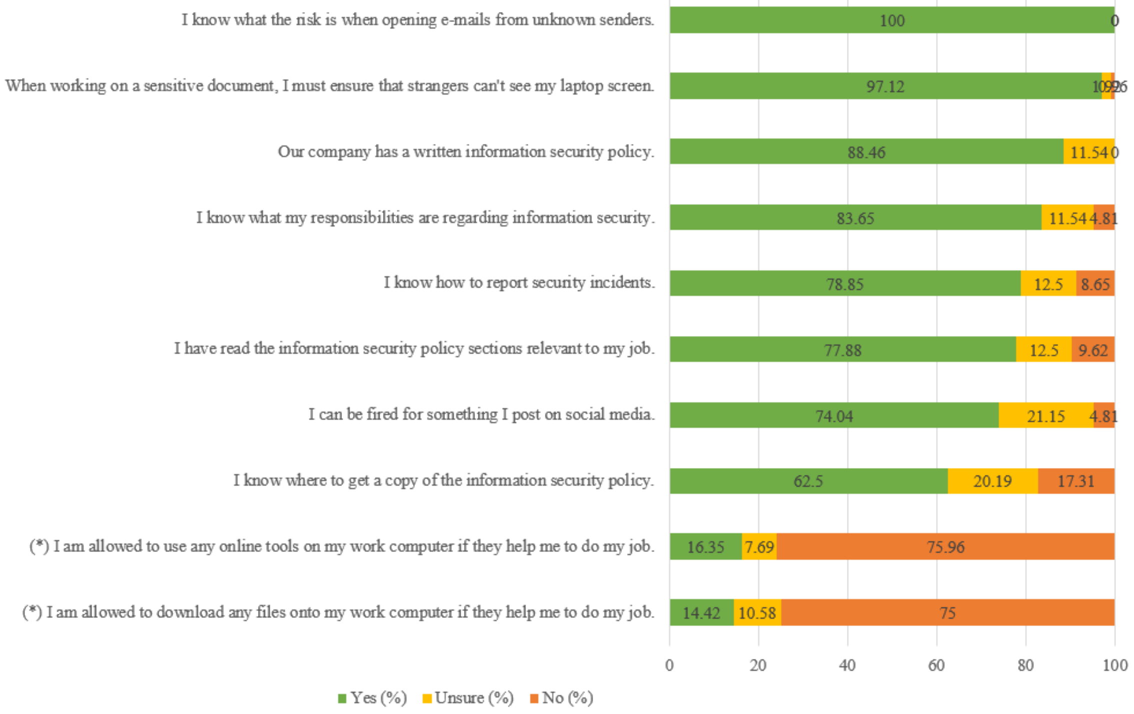

Figure 5. Knowledge statements - whole sample (composed by the author)

The two bottom knowledge statements (see **Figure 5**) seem to have a lower result, but it is not actually a bad result as these two are reverse statements – responding with a “No” is better than responding with a “Yes”. Therefore, it can be seen that the employees in Company A understand that not all files should be downloaded and not all online tools should be used to get the daily tasks done. Interviewees were satisfied with these results as these results indicate that culture is not individualistic and that the people do not put their individual needs above collective needs. At the same time the interviewees were curious to see whether the people who responded with “Yes” or “Unsure” were from engineering side or non-engineering side.

After conducting more detailed analysis, it turned out that when it comes to using any online tools the people who responded with "Yes" or "Unsure" were mostly non-engineers, only a couple of engineers chose to respond the same way. The results are different for downloading any files – almost 40% of the respondents who chose to state that yes, they can download any files for work purposes or were unsure whether they can actually do it were from the engineering side. This might be a matter that could be investigated further in the future.

Information security culture statements. The average grade for information security culture statements was 3.92 (out of 5.00) which, as mentioned before, is not a weak result as it is more on the favourable side, but it does seem to entail a fair amount of uncertainty. For the culture statements the respondents were able to choose between five responses ("strongly agree", "agree", "unsure", "disagree", "strongly disagree"), but in order to simplify the visual representation the author decided to group the responses followingly: favourable ("strongly agree", "agree"), unsure ("unsure"), unfavourable ("disagree", "strongly disagree").

When asked the interviewees about the current state of information security culture in Company A, the main response was that although the company has not reached its goal yet, the information security culture has been getting better. According to the interviewees, Company A is at the point of rapid improvements in relation to information security culture – more people in security team are focusing on training the people, security team's communications with the rest of the employees are becoming more regular thus slowly closing the gap between security engineers and the rest of the employees in the company.

At the same time the interviewees expressed that it can be noted that employees are not indifferent about information security and tend to collaborate. They see that further improvements regarding information security culture are needed. The interviewees pointed out that this can be achieved through education and innovative exercises around education – nobody wants to do boring e-learns or attend lecture type awareness trainings, people want their learning experience to be interesting. The interviewees also believed that speaking in a less technical way about security and having more personal and tailored approach to employees about security might bring better results.

The interviewees pointed out that in terms of organisational culture, the communication in Company A has to flow from bottom to top, not from top to bottom. This also relates to the fact that teams have more autonomy and have more freedom in deciding what is good for the company, not all decisions have to be made at management level. the interviewees believe this is also something that influences information security culture. With this way of communication everyone feels that they are responsible and that the rules and culture are not made up by the people working in higher management for example. According to the interviewees the employees do the right thing only when they believe it is the right thing to do.

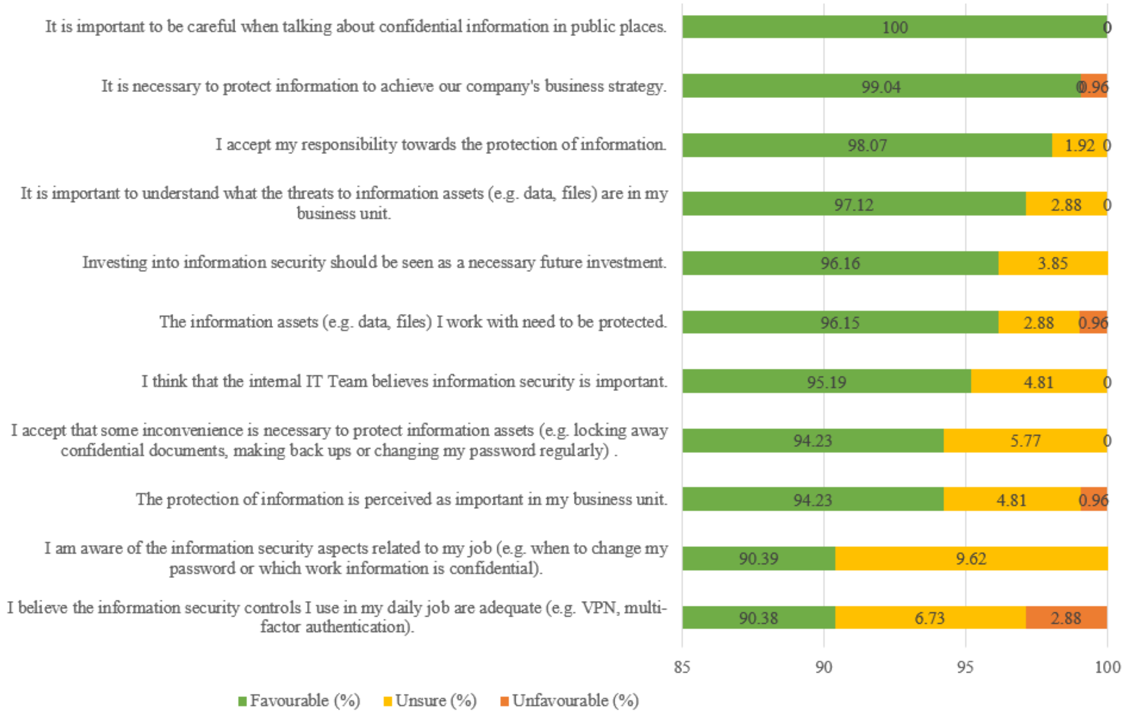

Figure 6. Information security culture statements favoured by over 90% of the respondents (composed by the author)

The statements to which the respondents were the most favourable are presented above (see **Figure 6**). The scale in the figure above starts from 85% to provide better visibility of the numbers in the figure. In general, it can be noted that employees in Company A believe that people need to be careful when talking about confidential information in public places, they see that information needs to be protected in order to achieve business strategy, and they also seem to accept their responsibility towards the protection of information. They feel that experiencing some inconvenience in order to protect information assets is acceptable. This is also an indication that employees in Company A are able to place organisation’s needs above their individual needs.

In the following figure (see **Figure 7**), the ten least favoured information security culture statements are listed. The main difference when comparing to the statements which are graded as the most favourable (see **Figure 6**) is that it seems that the employees in Company A have supportive mindset towards information security culture but they are less supportive to the statements which go into details, i.e. they are not sure what should they do in the event of a disaster or whether their business unit would be able to continue its daily operations in the event of a disaster. Interviewees told that for example the outcome of the least favoured statement is expected as disaster events are handled by designated people who are responsible for the office areas in different locations and not much is expected from an average employee. In addition, the interviewees mentioned that it is expected that the employees have expressed more uncertainty about the more detailed information security culture statements as the security team is on the way of bridging the gap between themselves and the rest of the company.

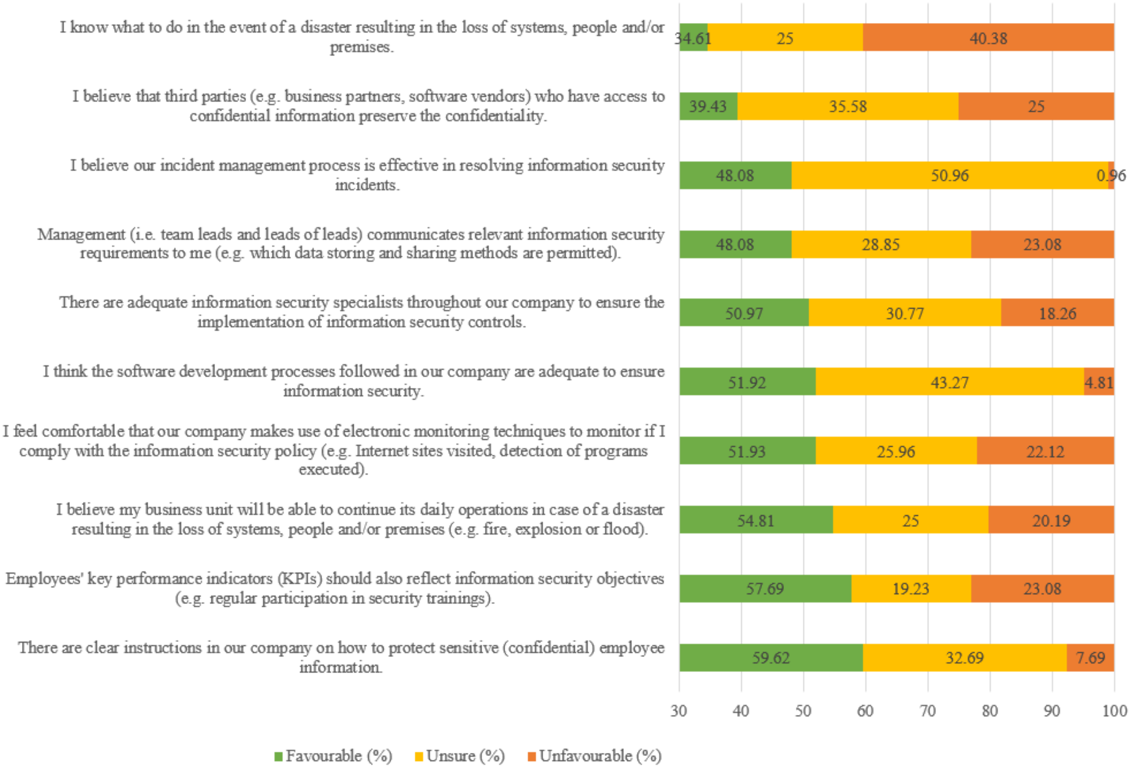

Figure 7. Ten least favoured information security culture statements (composed by the author)

When the author compared the top most favoured statements and the least favoured statements with the information security culture assessment conducted by Da Veiga [19], it turned out that many of the statements overlap, meaning that the ranking of the statements is similar. The statements that overlap with Da Veiga's work are [19] presented in the table below (see **Table 5**).

Table 5. ISCA results compared (composed by the author based on [19])

Statement	Rank in Company A	Rank in Da Veiga's research
It is important to be careful when talking about confidential information in public places.	High – 1st	High – 1st
It is important to protect information to achieve our company's business strategy.	High – 2nd	High – 2nd
I accept my responsibility towards the protection of information.	High – 3rd	High – 6th
It is important to understand what the threats to information assets are /../	High – 4th	High – 7th
Investing into information security should be seen as a necessary future investment.	High – 5th	High – 9th
The information assets I work with need to be protected.	High – 6th	Not in the top 10
I think that the internal IT team believes information security is important.	High – 7th	Not in the top 10
I accept that some inconvenience is necessary to protect information assets.	High – 8th	High – 5th
The protection of information is perceived as important in my business unit.	High – 9th	Not in the top 10
I believe the information security controls I use in my daily job are adequate.	High – 10th	Not in the top 10
I know what to do in the event of a disaster /../	Low – 1st	Low – 3rd
I believe that third parties who have access to confidential information preserve the confidentiality.	Low – 2nd	Low – 2nd
I believe our incident management process is effective in resolving information security incidents.	Low – 3rd	Low – 6th
Management communicates relevant information security requirements to me.	Low – 4th	Low – 9th
There are adequate information security specialists throughout our company to ensure the implementation of information security controls.	Low – 5th	Low – 8th
I think the software development processes followed in our company are adequate to ensure information security.	Low – 6th	Not in the lowest 10
I feel comfortable that our company makes use of electronic monitoring techniques to monitor if I comply with the information security policy.	Low – 7th	Not in the lowest 10
I believe my business unit will be able to continue its daily operations in case of a disaster /../	Low – 8th	Low – 6th

Statement	**Rank in Company A**	**Rank in Da Veiga's research**
Employees' key performance indicators should also reflect information security objectives.	Low – 9th	Not in the lowest 10
There are clear instructions in our company on how to protect sensitive employee information.	Low – 10th	Not in the lowest 10

A notion about the similarities presented in the table above (see **Table 5**) was also introduced to the interviewees. As Da Veiga's research was conducted in a multi-location company which performed audit and advisory assignments [19], the author of this thesis assumed that compared to the Company A, the company chosen by Da Veiga should be more corporate: have more organisational hierarchy, clear communication and decision making lines, have strict information security rules in place and have employees who are by default expected to follow these rules. It was discussed with the interviewees whether similar results between Company A and Da Veiga's company indicate that Company A has achieved strong results in ISCA regardless of the fact that Company A most likely is less mature in terms of information security management than the company viewed by Da Veiga.

The interviewees had different opinions on that matter. One of them felt that as Company A already has implemented information security policies then Company A is already very close to becoming a corporate environment, thus the similar results in the ISCA. Other interviewees were under the impression that achieving similar results to the corporate organisation speaks for the set of values, norms and behaviour developed in Company A. At the same time it was also mentioned that in terms of growth potential Company A might have an advantage compared to a corporate company. The reason for this was said to be that Company A pays special attention to designing healthy organisational culture which is not based on fear but on innovation, trust and collaboration. Interviewees believe that having these values can foster information security culture even further. Interviewees believe that corporate companies might be more focused on fear which does not work in favour for establishing a strong information security culture.

Two of the interviewees also brought out that although there are similarities between the two researches, the result might not be comparable as information security practises have evolved over the years and become an integral part of doing business. The interviewees felt that the survey results can therefore be similar by a lucky accident. This can specially be the case of technology companies which are more dependent on IT solutions – these companies have to deal with information security and therefore some of the ISCA statements might be by default more favourable to the respondents. This would mean that it is not the culture that has promoted the favourable perception, but it is the general way of doing business that has done part of the promotion for information security culture. It was also mentioned by one interviewee that even though businesses today tend to be more focused on IT solutions and therefore have to deal more with IT risks and information security management, the results for information security culture might be similar because people, their perception and attitudes change slowly if at all.

4.4 Differences in grades per subgroups

The author compared the different grades – involvement in IT risk management procedures (represented as *RISK* in the tables), information security knowledge (represented as *KNOWLEDGE* in the tables), and information security culture grades (represented as *CULTURE* in the tables) – the different subgroups of respondents have. The author has focused the analysis on comparing engineers with non-engineers, and comparing employees in group A with employees in group B. In this chapter the main findings have been discussed.

4.4.1 Differences between engineers and non-engineers

Out of 104 respondents, 30 were engineers (see **Table 6**) and 74 were non-engineers (see **Table 7**). In terms of tenure, the engineers and non-engineer subgroups seem to be substantially similar, but in terms of location there are some differences. Only a few engineers have marked that they work from outside Europe (see **Table 6** and **Table 7**).

Table 6. General statistics describing engineers (composed by the author)

Indicator	**Value**	**Total**	**Value share out of total (%)**
N	30	30	100.00
TENURE: LONGER	18	30	60.00
TENURE: SHORTER	12	30	40.00
EU	28	30	93.33
NON-EU	2	30	6.67
ENG	30	30	100.00
NON-ENG	0	30	0.00

Table 7. General statistics describing non-engineers (composed by the author)

Indicator	Value	Total	Value share out of total (%)
N	74	74	100.00
TENURE: LONGER	42	74	56.76
TENURE: SHORTER	32	74	43.24
EU	51	74	68.92
NON-EU	23	74	31.08
ENG	0	74	0.00
NON-ENG	74	74	100.00

When comparing engineers and non-engineers in terms of grades (see **Table 8** and **Table 9**), it can be seen that engineers are on average more involved in IT risk management procedures (7.23 applicable statements out of 15) than non-engineers (4.92 applicable statements out of 15). Also for engineers the grade is slightly above the average calculated for the whole sample (see **Table 4**) and for non-engineers the grade is slightly below the average calculated for the whole sample.

At the same time, it can be noted that engineers also seem to have slightly higher knowledge about information security (8.33 out of 10) compared to the non-engineers (8.05 out of 10). When comparing these numbers against the average knowledge grades calculated for the whole sample, it can be seen that once again engineers are slightly above the general average and non-engineers are slightly below the general average (see **Table 4**, **Table 8**, and **Table 9**).

Table 8. Grades describing engineers (composed by the author)

Indicator	Average value (value)	Maximum possible (max)	Value share out of max (%)	Count of statements	Average unsure rate (%)
RISK	7.23	15.00	48.20	15	11.53
KNOWLEDGE	8.33	10.00	83.30	10	10.33
CULTURE	3.88	5.00	77.60	48	17.35

Table 9. Grades describing non-engineers (composed by the author)

Indicator	Average value (value)	Maximum possible (max)	Value share out of max (%)	Count of statements	Average unsure rate (%)
RISK	4.92	15.00	32.80	15	10.73
KNOWLEDGE	8.05	10.00	80.50	10	11.22
CULTURE	3.94	5.00	78.80	48	19.13

Interestingly, engineers perceive information security culture slightly less favourably than non-engineers. The respective average grades for information security culture are 3.88 and 3.94 (see **Table 8** and **Table 9**). From these results it can also be seen that compared to general average grade engineers have given a slightly lower grade to information security culture, and at the same time non-engineers stay slightly above average (see **Table 4**). This seems to contradict with Da Veiga's research on subcultures where she noticed that the people who work in IT tend to have a more positive perception towards information security culture [26]. This could of course be because the definition for engineers in the current thesis differs from the definition Da Veiga used for IT workers or that the survey simply works differently in Company A.

These results were also presented to the interviewees and they tried to provide explanation to why the engineers who are more included in the IT risk management procedures and on average have slightly more information security knowledge also have on average graded information security culture slightly lower than non-engineers. Their opinion was that as engineers have a better understanding and visibility of information security and used technologies in general, they might also be more critical towards the current information security culture in Company A.

In order to test whether the differences in means between engineers and non-engineers are meaningful in relation to the information security culture grade, the author carried out a t-test. As a reminder, the null-hypothesis ($H0_{EC}$) was defined as engineers and non-engineers not having a meaningful difference in terms of culture grades. In order to clarify whether the difference between these groups is meaningful enough to conclude that the engineers have given the information security culture a lower grade than the non-engineers (alternative hypothesis $H1_{EC}$) the author has carried out a t-test. The t-test was carried out using the *MS Excel* data analysis tools and the results can be seen in **Table 10**.

Table 10. t-Test: Two-Sample Assuming Unequal Variances – testing $H1_{EC}$ (composed by the author)

Indicator	Non-engineers	Engineers
Mean	3.94	3.88
Variance	0.17	0.12
Observations	74	30
Hypothesized Mean Difference	0	
df	63.00	
t Stat	0.75	

Indicator	Non-engineers	Engineers
P(T<=t) one-tail	0.23	
t Critical one-tail	1.67	
P(T<=t) two-tail	0.46	
t Critical two-tail	2.00	

The **Table 10** above shows that the t-test statistic '*t Stat*' is 0.75. In order to be able to drop the null-hypothesis and accept the alternative hypothesis, the value of the t statistic should either be smaller than negative '*t-Critical one-tail*' or larger than '*t-Critical one-tail*' [63]. As this is not the case here, we cannot accept the alternative hypothesis. This means that the current data does not support the idea that the engineers have provided a significantly different grade for the information security culture compared to the non-engineers. We cannot reject $H0_{EC}$ and we cannot accept $H1_{EC}$.

The author also conducted a t-test to see whether there is a meaningful difference in the uncertainty levels perceived by engineers and non-engineers about information security culture. The author has measured uncertainty by counting the number of times each respondent responded with "Unsure" and then calculated its share out of total statements (there were 48 statements for information security culture). As a reminder, the author had defined $H0_{EU}$ as engineers and non-engineers having no differences in uncertainty levels and $H1_{EU}$ as engineers and non-engineers expressing different levels of uncertainty about information security culture. The results of the t-test can be seen from the table below (see **Table 11**).

Table 11. t-Test: Two-Sample Assuming Unequal Variances – testing $H1_{EU}$ (composed by the author)

Indicator	Engineers	Non-engineers
Mean	17.36	19.12
Variance	143.78	159.74
Observations	30	74
Hypothesized Mean Difference	0.00	
df	56.00	
t Stat	-0.67	
P(T<=t) one-tail	0.25	
t Critical one-tail	1.67	
P(T<=t) two-tail	0.51	
t Critical two-tail	2.00	

When comparing '*t Stat*' value with '*t Critical one-tail*' (see **Table 11**) we can see that '*t Stat*' is not bigger than '*t Critical one-tail*' or smaller than negative '*t Critical one-tail*'. This means that there is no significant difference between engineers and non-engineers when comparing their uncertainty levels perceived about information security culture [63]. We cannot reject $H0_{EU}$ and we cannot accept $H1_{EU}$.

4.4.2 Differences between group A and group B

Another comparison the author was interested in was the comparison between employee group A and employee group B. The author has defined group A to be all the respondents who have marked at least half of the 15 IT risk management procedure statements applicable to themselves. The rest of the employees make up group B or in other words they are the employees who are less involved in IT risk management procedures.

When looking at the general statistics (see **Table 12** and **Table 13**), it can be seen that in terms of tenure, group A has more long term employees than group B and in group B there are almost the same amount of long-term employees as there are short-term employees. Both groups are similar in terms of location.

What is different though, is the shares of the engineers and non-engineers in group A and group B. In group B, there are about 80% of non-engineers and 20% of engineers, but for group A – for employees who are more related to IT risk management procedures – the respective indicator is 50-50 (see **Table 12** and **Table 13**). There are equal amount of engineers and non-engineers in group A. When asked for a reasoning about this, the interviewees mentioned that it can be explained by the fact that also non-engineers' work relates strongly to the usage information systems. Non-engineers must therefore also think more how to protect the information assets and keep their business processes running properly, they need to assess risks. This could also relate to the indications discovered when analysing the organisational culture characteristics most relevant for Company A. As it turned out it seemed like Company A seems to have an organic culture type (see chapter 4.2) which in other research has been related to a more positive mindset about risk management practises (see chapter 2.2.2).

Table 12. General statistics describing group A (risk involvement above 7.5) (composed by the author)

Indicator	Value	Total	Value share out of total (%)
N	32	32	100.00

Indicator	Value	Total	Value share out of total (%)
TENURE: LONGER	23	32	71.88
TENURE: SHORTER	9	32	28.13
EU	27	32	84.38
NON-EU	5	32	15.63
ENG	16	32	50.00
NON-ENG	16	32	50.00

Table 13. General statistics describing group B (risk involvement below or equal to 7.5) (composed by the author)

Indicator	Value	Total	Value share out of total (%)
N	72	72	100.00
TENURE: LONGER	37	72	51.39
TENURE: SHORTER	35	72	48.61
EU	52	72	72.22
NON-EU	20	72	27.78
ENG	14	72	19.44
NON-ENG	58	72	80.56

When comparing the grades group A and group B have for *RISK, KNOWLEDGE* and *CULTURE* indicators (see **Table 14** and

Table 15), then for obvious reasons group A has a much higher involvement in IT risk management procedures (10.16 vs 3.56 out of 15). At the same time group A is also slightly stronger at information security knowledge (8.44 out of 10) than group B (8.00 out of 10). It can also be seen that group A has a slightly lower grade for information security culture than group B – respectively 3.87 and 3.94. Although group A consists of equal amount of engineers and non-engineers, the results of group A are similar to the results of all engineers.

Table 14. Grades describing group A (risk involvement above 7.5) (composed by the author)

Indicator	Average value (value)	Maximum possible (max)	Value share out of max (%)	Count of statements	Average unsure rate (%)
RISK	10.16	15.00	67.73	15	6.87
KNOWLEDGE	8.44	10	84.40	10	8.44
CULTURE	3.87	5.00	77.40	48	15.69

Table 15. Grades describing group B (risk involvement below or equal to 7.5) (composed by the author)

Indicator	Average value (value)	Maximum possible (max)	Value share out of max (%)	Count of statements	Average unsure rate (%)
RISK	3.56	15	23.73	15	12.80
KNOWLEDGE	8	10	80.00	10	12.08
CULTURE	3.94	5	78.80	48	19.92

When asked why should the people in group A have higher information security knowledge but lower results in information security culture part, the interviewees agreed that similarly to engineers (see chapter 4.4.1) also the people in group A might be more critical about information security culture as they seem to understand information security a bit better and tend to work more with IT risk management procedures.

The author decided to also test the meaningfulness of the differences here. The null-hypothesis ($H0_{GC}$) was defined as group A and group B not having a meaningful difference in terms of culture grades. In order to clarify whether the difference between group A and group B is meaningful enough to conclude that the employees more involved in IT risk management procedures have given the information security culture a lower grade than the employees less involved in IT risk management procedures (alternative hypothesis $H1_{GC}$) the author has carried out a t-test. The t-test was carried out using the *MS Excel* data analysis tools and the results can be seen in **Table 16**.

Table 16. t-Test: Two-Sample Assuming Unequal Variances – testing $H1_{GC}$ (composed by the author)

Indicators	Group A	Group B
Mean	3.8659	3.9444
Variance	0.1519	0.1600
Observations	32	72
Hypothesized Mean Difference	0	
df	61	
t Stat	-0.9410	
P(T<=t) one-tail	0.1752	
t Critical one-tail	1.6702	
P(T<=t) two-tail	0.3504	
t Critical two -tail	1.9996	

The **Table 16** above shows that the t-test statistic '*t Stat*' is -0.9410. In order to be able to drop the null-hypothesis and accept the alternative hypothesis, the value of the t statistic should either be smaller than negative '*t-Critical one-tail*' or larger than '*t-Critical one-tail*' [63]. As this is not the case here, we cannot accept the alternative hypothesis. This means that the current data does not support the idea that the employees more involved in IT risk management have provided a significantly different grade for the information security culture compared to the employees less involved in IT risk management procedures.

The author also tried to see whether the t-test would give a different conclusion if the definitions of group A and group B would be different – group A being defined as people who marked themselves related to IT risk management procedures at least 10 times out of 15 and group B being defined as people who marked themselves related to IT risk management procedures less than 5 times out of 15. It turned out that even adjusting the definition would still not allow to accept the alternative hypothesis.

As it was also done for the purposes of comparing engineers and non-engineers, the author conducted a t-test to see whether there is a meaningful difference in the way group A and group B express their uncertainty about information security culture. The author measured uncertainty by counting the number of times each respondent responded with "Unsure" and then calculated its share out of total statements (there were 48 statements for information security culture). As a reminder, the author defined $H0_{GU}$ as group A and group B having no differences in uncertainty levels and $H1_{GU}$ as group A and group B expressing different levels of uncertainty about information security culture. The results of the t-test can be seen from the table below (see **Table 17**).

Table 17. t-Test: Two-Sample Assuming Unequal Variances – testing $H1_{GU}$ (composed by the author)

Indicator	Group A	Group B
Mean	15.69	19.91
Variance	103.88	172.99
Observations	32	72
Hypothesized Mean Difference	0.00	
df	76.00	
t Stat	-1.77	
P(T<=t) one-tail	0.04	
t Critical one-tail	1.67	

Indicator	Group A	Group B
P(T<=t) two-tail	0.08	
t Critical two-tail	1.99	

When comparing '*t Stat*' value with '*t Critical one-tail*' we can see that '*t Stat*' is not bigger than '*t Critical one-tail*' but is smaller than negative '*t Critical one-tail*' (see **Table 17**). This means that there should be scientifically meaningful difference between group A and group B when comparing their uncertainty levels they have expressed about information security culture [63]. We can reject $H0_{GU}$ and we can accept $H1_{GU}$.

5 Results

In this chapter the author provides answers to the research questions presented in the first chapter. The answers to the research questions can also be found when reading the previous chapters, but in order to provide clarity and transparency the answers have also beeen explicitly described here.

The first research question was **“What characterises the state of risk management in Company A today?”**. The interviewees told that risk management as a topic is not very common in Company A. Risks are mostly handled by a few teams and by a few people across the company. At the same time attitude is very good and whenever there is a need to talk about risks or for handling risks, then this is done. According to the interviewees the general visibility on risks should be improved even further.

The survey results indicate that a decent part of IT risk management procedures relate to the employee’s daily tasks in Company A. The employees whose daily job tasks relate strongly to various IT risk management procedures are not just from engineering teams – they are also from non-engineering teams which indicates that IT risk management is equally the responsibility of engineers and non-engineers.

The second research question was **“How does information security culture in a young technology company compare to the results measured previously in other companies?”**. The information security assessment results of Company A were compared to a study conducted over 10 years ago in a more corporate company. To a large extent the top most favourable and least favourable information security statements were similar for both studies. It was seen from both assessments that people tend to show supportive attitude towards information security culture but are often unsure or less positively minded about the more detailed information security statements. The reason behind this can be that the employees do not have enough knowledge about the details of information security to form a confident favourable response.

Some of the interviewees mentioned that similar results speak for Company A's achievements in the field of information security culture. These interviewees did not perceive Company A as a corporate environment and felt that having similarities with a corporate organisation in terms of information security culture mean that something has been done right. Some interviewees mentioned that the businesses today focus more on information technology solutions and should therefore also focus more on information security than the businesses that existed 10 years ago – these interviewees expected more differences to be drawn out. One of the interviewees also mentioned that even though information technology has become an integral part for almost every business, the attitudes and opinions of people do not change that quickly. Therefore the similarities found between the studies can simply refer to the fact that cultural changes occur slowly.

The third research question was **"What has shaped the information security culture in Company A until this day?".** The opinion of the interviewees was that although the information security culture is not at its peak, it is about to get better as much of the focus has been put to making improvements. The general organisational culture in Company A foresees that people do the right thing if they feel that this is the right thing and this also has an influence on information security culture. In order to improve information security culture even further in Company A, the information security team should come up with innovative ways (that ideally could also entail joyful incentive) to improve employees' awareness and make the distance between security team and the rest of the employees smaller.

The fourth research question was **"Are engineers perceiving information security culture more positively than non-engineers and what could be the reasons for that?".** The author made an assumption that engineers could perceive information security culture more positively as due to their area of focus they should have a better understanding about information technology solutions and related risks in general. A similar idea was also supported by Da Veiga and Martins who saw that IT employees have more positive perception about information security culture [25]. The reason why the author decided to investigate engineers was also the assumption that due to their profession engineers might have more exposure to the IT risk management procedures.

Interestingly, it turned out that engineers seem to perceive information security culture slightly less positively than non-engineers. The t-test did not show that the differences between engineers and non-engineers would be meaningful. At the same time when asked about this, the interviewees felt that as engineers have more visibility and understanding on how the matters relating to information security could be which is why they may exhibit more critical way of thinking than non-engineers.

Also as the information security culture assessment brought out that there was a fair amount of uncertainty among the responses, the author also analysed whether engineers and non-engineers differ from the level of uncertainty they feel about information security culture. The t-test indicated that not meaningful differences exist. As a result it can be concluded that although engineers might have more relation to IT risk management procedures and more exposure to the information security aspects they do not perceive information security culture differently compared to non-engineers.

The author provides the answer to the fifth and sixth question together as these are interconnected. The fifth question was **"Are the employees who are more involved in risk management procedures (employee group A) more promotively minded towards information security than the employees who are less involved in risk management procedures (employee group B)?"** and the sixth question was **"What can possibly cause the differences in perception between employee group A and employee group B?"**. The author of this study assumed that there the employee group A is more positively minded about information security culture than employee group B. However it turned out that people who are more involved in risk management procedures on a daily basis, on average tend to grade information security culture with a slightly lower grade than employee group B. The interviewees thought that this might be because the employee group A has better visibility on risks in general and therefore knows what more to expect from information security culture.

The t-tests that the author conducted revealed that the differences in how the employee group A and employee group B perceive information security culture are not statistically meaningful. However when conducting t-test in order to understand whether employee group A and employee group B have exhibited different levels of uncertainty about information security culture, it turned out that this is true: there is a difference how much does group A feels uncertain about information security culture and how much uncertainty the respondents in group B feel. This aspect might be worth further investigation but the initial data comparison indicates that the people who are more involved in IT risk management procedures (group A) have lower uncertainty levels than group B.

6 Conclusion

The author of this thesis focused on finding out what are the implications of information security culture on IT risk management. The author conducted a study in a young technology company (less than 10 years old) which has operations in Estonia (Company A). The study combined qualitative and quantitative research methods: the author conducted a survey and several interviews with different employees in the company.

The approach used in this study is one of the things that makes this study novel. Various literature reviews suggest that in order to evaluate information security culture properly, several research methods should be used. For example qualitative and quantitative methods. The author of this study has decided to do that by conducting a survey and several interviews with various stakeholders from Company A. Previous studies that have focused on information security culture do not deploy combined research methods or have deployed them insufficiently (e.g. by only interviewing the chief information security manager and leaving other stakeholders out of the picture).

The decision to focus on young technology companies can be explained by the point that there are a lot of new technology companies emerging lately. In addition, it is likely that the young companies do not have as mature risk management and information security management as older companies but they still have to address the risks. As much of the risks in the technology companies relate to the information security and people, the author decided to research the relationship between information security culture and IT risk management. The author noticed that previously no specific emphasis has put on researching information security culture in relation to young companies which is another aspect why this study is novel.

Information security culture is the values, norms, attitudes, expectations that employees have towards their company's information security culture and it works on different layers – organisational, group layer and individual layer. Information security culture is something that exists in every organization and is different for every organisation. There can even be different subcultures within one organisation.

Information security culture, when cultivated properly, can increase the promoting attitude people have towards information security controls and therefore determine the effectiveness of these controls. Strong information security culture might also extend its positive influence to IT risk management procedures and help shape employees security awareness.

The importance of taking advantage of information security culture in the case of young technology companies relies in the fact that the young companies tend to have most of their focus on innovation and business growth while struggling with establishing clear communication lines within the company. Information security culture helps to make it easier for a young company to manage IT risks with better coverage.

In order to analyse the implications information security culture might have on risk management procedures, the author designed a survey. Fortunately the author was able to use information security assessment created by another researcher (Da Veiga) which also had been tested for reliability. The author had to make adjustments to the existing assessment so that it would be relevant for the technology companies operating today. In addition the author added a separate survey section which would help to determine the employees who are more involved in IT risk management procedures (group A) and employees who are less involved in IT risk management procedures (group B).

At first the designed survey was used in Company B – another young technology company having operations in Estonia. The amount of respondents was low, but this experience helped the author to gather some feedback and improve the survey as per feedback. After that the survey was conducted in Company A. Before the survey was launched in Company A, it was also reviewed by the representative from Company A to make sure that the survey is usable in Company A.

Altogether 104 employees responded to the survey in Company A which met the minimum target set by the author. The author was able to carry on the data analysis and conduct 6 interviews with stakeholders from Company A. As the survey was modified by the author, the survey parts were tested for reliability. Cronbach's alpha value was calculated for each survey part – IT risk management part, security knowledge part, and information security culture part. The Cronbach's alpha showed that the IT risk management part and information security culture part are reliable. Security knowledge part turned out to be not reliable and the author decided not to build strong conclusions on data about security knowledge.

The main outcomes of the data analysis and the information obtained during interviews was that Company A seems to have organic culture which in the literature has been connected to having a positive effect on the way people in the company perceive risk management activities and programmes established within the company. This might have a relation to the fact that the respondents perceived that their work relates to on average over a third of IT risk management statements that were presented to them in the survey. This also might have a connection to the fact that the people who on average are more related to IT risk management procedures have equal amount of engineers and non-engineers. This indicates that IT risk management is a responsibility that has been shared in a wider manner. This outcome is expected as in a technology company majority of the business processes are supported with the usage of technological solutions which means more people are exposed to dealing with possible IT risks.

During the data analysis, the author tested four pairs of hypotheses by conducting the t-tests. It turned out that there is no significant difference in the way engineers and non-engineers perceive information security culture in Company A. This could indicate that across different groups of people the information security culture has been established evenly in Company A. There was a slight difference in the means but it was not meaningful.

The author expected to see that engineers have more positive perception towards information security culture than the non-engineers, but the difference was irrelevant and had opposite direction than assumed. The interviewees mentioned that in general engineers may give lower grade to information security culture as they tend to have more visibility and understanding about the information technology solutions in general which makes them be more critical about the information security culture too.

When comparing the employees whose daily job tasks are more related to IT risk management procedures (group A) to the employees whose daily job tasks are less related to IT risk management procedures (group B), it was noted that group A had on average given a lower grade to information security culture than group B. The interviewees explained that as group A has more visibility of IT risks, they might also be more critical about information security culture. The t-tests conducted did not confirm the significance of the difference group A and group B had in terms of their information security culture perception. This also could speak for the fact that information security culture has evolved evenly across the company.

There was one pair of hypotheses for which the results of the t-test allowed the author to reject the null-hypothesis and accept the alternative hypothesis. When comparing whether the levels of uncertainty group A and group B have exhibited about information security culture, the author was able to confirm that group A and group B have different levels of uncertainty about information security culture. Initial data analysis indicates that group A has been more confident in their responses and group B has been responding with “unsure” significantly more. This could mean that although based on the mean values the different groups of people perceive information security culture similarly, there is a difference in how confident the people are when asked to express an opinion or attitude about information security matters. In a way this associates with what the interviewees emphasised: people in group A should have better visibility about information security matters as they have more exposure to IT risk management procedures.

It is difficult to determine the direction of the implication here. The current analysis did not reveal strong differences in the information security culture means calculated for different groups of employees. Additional studies should be conducted in the future to assess whether information security culture dependent on risk management or *vice versa*. It is also currently not possible to determine whether risk management is dependent on the level of uncertainty people have about information security culture or perhaps the uncertainty depends on whether the employee belongs to group A or group B. Further studies including regression analysis could clarify that.

As the study was conducted in one young technology company it is difficult to extend the previously listed conclusions to other similar companies because young technology companies can differ from many other aspects that can influence the way people perceive information security culture or handle IT risks. For example the composition of different nationalities among staff members could have an unexpected influence. This is one of the possible reasons why the results of a multi-location company cannot be applied to for example local single-location technology companies. Another possible reason that can have impact is the industry the business operates in – some industries are more regulated than others which also influences the shape of information security culture.

The author believes that in the future it would be beneficial to also analyse how does employee’s nationality influence information security culture or how do the values in the organisational culture relate to the information security culture. On a slightly more ambitious note: Estonian citizens have exposure to various e-services that the government provides to them and therefore they also have exposure to the usage of information technology solutions. It would be interesting to measure information security culture among the citizens of Estonia (or any other country that deploys digital solutions). This would of course require the development of yet another information security culture assessment.

References

[1] E. Schulze, “State of European Tech 2018: Record year for start-ups,” *CNBC*, 2018. [Online]. Available: https://www.cnbc.com/2018/12/04/state-of-european-tech-2018-record-year-for-start-ups.html. [Accessed: 21-Apr-2019].

[2] R. Florida and C. Mellander, “How the Geography of Startups and Innovation is Changing,” *Harvard Business Review*, 27-Nov-2018. [Online]. Available: https://hbr.org/2018/11/how-the-geography-of-startups-and-innovation-is-changing. [Accessed: 21-Apr-2019].

[3] D. Prosser, “UK Technology Startups Hit All-Time High,” *Forbes*, 2018. [Online]. Available: https://www.forbes.com/sites/davidprosser/2018/04/06/uk-technology-start-ups-hit-all-time-high/#3a07854e5d85. [Accessed: 22-Apr-2019].

[4] L. Morgan, “Hacker Puts Code Spaces Out of Business,” *IT Governance Blog*, 2014. [Online]. Available: https://www.itgovernance.co.uk/blog/hacker-puts-code-spaces-out-of-business. [Accessed: 07-May-2019].

[5] “Code Spaces,” *Crunchbase*. [Online]. Available: https://www.crunchbase.com/organization/code-spaces#section-overview. [Accessed: 07-May-2019].

[6] A. Martins and J. Elofe, “Information Security Culture,” in *Security in the Information Society*, M. A. Ghonaimy, M. T. El-Hadidi, and H. K. Aslan, Eds. Boston, MA: Springer, 2002, pp. 203–214.

[7] C. T. Cybersecurity Insiders, “2018 Insider Threat Report,” 2018.

[8] Hall John, “12 Challenges Faced By The Fastest-Growing Companies,” *Forbes*, 2013. [Online]. Available: https://www.forbes.com/sites/johnhall/2013/11/03/12-challenges-faced-by-the-fastest-growing-companies/#3109e7e4657e. [Accessed: 24-Mar-2019].

[9] Barrett Keith, “Global challenges facing tech startups,” *Bite.tech*, 2018. [Online]. Available: http://www.bite.tech/news/global-challenges-facing-tech-startups. [Accessed: 24-Mar-2019].

[10] Hunckler Matt, “12 Challenges Startup Culture Must Overcome In Order To Thrive in 2017,” *Forbes*, 2017. [Online]. Available: https://www.forbes.com/sites/matthunckler/2017/03/22/12-challenges-startup-culture-must-overcome-in-order-to-thrive-in-2017/#4adfa9847592. [Accessed: 24-Mar-2019].

[11] T. Bailetti, “What Technology Startups Must Get Right to Globalize Early and Rapidly,” *Technol. Innov. Manag. Rev.*, no. October, pp. 5–16, 2012.

[12] Nair Praseeda, “Why you need a strong information security culture in business,” *Growthbusiness.co.uk*, 2017. [Online]. Available: https://www.growthbusiness.co.uk/need-strong-information-security-culture-business-2550058/. [Accessed: 24-Mar-2019].

[13] Roer Kai, “Building a Security Culture Has Its Benefits,” *ISACA Now Blog*. [Online]. Available: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?List=ef7cbc6d-9997-4b62-96a4-a36fb7e171af&ID=665. [Accessed: 24-Mar-2019].

[14] A. AlHogail and A. Mirza, “Information security culture: A definition and a literature review,” in *2014 World Congress on Computer Applications and Information Systems, WCCAIS 2014*, 2014, no. October 2014.

[15] K. Roer, “How Measuring Security Culture Is Different from Counting Employees,” in *RSA Conference 2017*, 2017.

[16] K. M. Karlsson Fredrik, Aström Joachim, “Information security culture - state-of-the-art review between 2000 and 2013,” *Inf. Comput. Secur.*, vol. 23, no. 3, pp. 246–285, 2014.

[17] Startup Estonia, “Estonian Startup Explorer.” [Online]. Available: https://www.startupestonia.ee/startups. [Accessed: 12-Feb-2019].

[18] J. Kennedy, “12 terrific Tallinn start-ups to watch in 2018,” *Siliconrepublic*, 2017. [Online]. Available: https://www.siliconrepublic.com/start-ups/tallinn-startups-estonia-2018. [Accessed: 22-Apr-2019].

[19] A. Da Veiga, “Cultivating and assessing information security culture,” 2008.

[20] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies,” *Comput. Secur.*, vol. 66, pp. 40–51, 2017.

[21] ENISA, “Cyber Security Culture in organisations,” 2017.

[22] A. Da Veiga and J. H. P. Eloff, “A framework and assessment instrument for information security culture,” *Comput. Secur.*, vol. 29, no. 2, pp. 196–207, 2010.

[23] K. Roer and G. Petric, “To measure security culture,” 2018.

[24] A. B. Ruighaver, S. B. Maynard, and S. Chang, “Organisational security culture: Extending the end-user perspective,” *Comput. Secur.*, vol. 26, no. 1, pp. 56–62, 2007.

[25] A. Da Veiga and N. Martins, “Defining and identifying dominant information security cultures and subcultures,” *Comput. Secur.*, vol. 70, pp. 72–94, 2017.

[26] A. Da Veiga, “An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture,” *Inf. Comput. Secur.*, vol. 26, no. 5, pp. 584–612, 2018.

[27] M. Shifaiz, “An Information Security Cultural Framework: A case study for the Netherlands,” Delft University of Technology, 2017.

[28] N. H. Hassan, Z. Ismail, and N. Maarop, “Information Security Culture: A Systematic Literature Review,” in *Proceedings of the 5th International Conference on Computing and Informatics*, 2015, no. 205, pp. 456–463.

[29] I. Okere, J. Van Niekerk, and M. Carroll, “Assessing information security culture: A critical analysis of current approaches,” in *2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference*, 2012, no. August, pp. 136–143.

[30] A. Da Veiga, “Comparing the information security culture of employees who had read the information security policy and those who had not: Illustrated through an empirical study,” *Inf. Comput. Secur.*, vol. 24, no. 2, pp. 139–151, 2016.

[31] A. Da Veiga and N. Martins, “Improving the information security culture through monitoring and implementation actions illustrated through a case study,” *Comput. Secur.*, vol. 49, pp. 162–176, 2015.

[32] A. Alhogail, “Design and validation of information security culture framework,” *Comput. Human Behav.*, vol. 49, pp. 567–575, 2015.

[33] K. M. Parsons, E. Young, M. A. Butavicius, A. McCormac, M. R. Pattinson, and C. Jerram, “The influence of organizational information security culture on information security decision making,” *J. Cogn. Eng. Decis. Mak.*, vol. 9, no. 2, pp. 117–129, 2015.

[34] T. Schlienger and S. Teufel, “Information Security Culture - from Analysis to Ahange,” in *Information Security South Africa - Proceedings of ISSA 2003*, 2003, pp. 183–195.

[35] A. da Veiga, N. Martins, and J. H. P. Eloff, “Information security culture – validation of an assessment instrument,” *South African Bus. Rev.*, vol. 11, no. 1, pp. 147–166, 2007.

[36] I. O. for Standardization, “ISO/IEC 17799:2005 - Information technology -- Security techniques -- Code of practice for information security management.” [Online]. Available: https://www.iso.org/standard/39612.html. [Accessed: 10-Feb-2019].

[37] E. H. Schein, *The Corporate Culture Survival Guide*, 2009th ed. San Francisco, CA: Jossey-Bass, 1999.

[38] D. W. Hubbard, *The Failure of Risk Management - Why It’s Broken and How to Fix It*. Hoboken, New Jersey: John Wiley & Sons, Inc., 2009.

[39] R. K. Mobley, “What is Risk Management? — Life Cycle Engineering,” *Life cycle Engineering*. [Online]. Available: https://www.lce.com/What-is-Risk-Management-1263.html. [Accessed: 17-Feb-2019].

[40] “Open Group Standard: Risk Taxonomy (O-RT), Version 2.0.”

[41] B. W. Nocco *et al.*, “Applied corporate finance,” *J. Appl. Corp. Financ. - A Morgan Stanley Publ.*, vol. 18, no. 4, pp. 8–20, 2006.

[42] M. S. Beasley, “What is Enterprise risk management ?,” 2016.

[43] J. Deloach, “Key Elements of the Risk Management Process,” *Corporate Compliance Insights*, 2018. [Online]. Available: https://www.corporatecomplianceinsights.com/key-elements-of-the-risk-management-process/. [Accessed: 21-Apr-2019].

[44] F. S. Board, “Guidance on Supervisory Interaction with Financial Institutions on Risk Culture,” 2014.

[45] R. L. Kimbrough and P. J. Componation, “The relationship between organizational culture and enterprise risk management,” *EMJ - Eng. Manag. J.*, vol. 21, no. 2, pp. 18–26, 2009.

[46] R. F. Reigle, “Organizational Culture Assessment: Development of a Descriptive Test Instrument,” University of Alabama in Huntsville, 2003.

[47] G. Hofstede and M. H. Bond, “Hofstede’s Culture Dimensions: An Independent Validation Using Rokeach’s Value Survey,” *J. Cross - Cult. Psychol.*, vol. 15, no. 4, pp. 417–433, 1984.

[48] Y. Hancıoğlu, Ü. B. Doğan, and Ş. S. Yıldırım, “Relationship between Uncertainty Avoidance Culture, Entrepreneurial Activity and Economic Development,” *Procedia - Soc. Behav. Sci.*, vol. 150, pp. 908–916, 2014.

[49] North Carolina State Poole College of Management, “Risk Culture of Companies,” *Enterprise Risk Management Initiative*, 2009. [Online]. Available: https://erm.ncsu.edu/library/article/risk-culture-companies. [Accessed: 21-Apr-2019].

[50] A. Krivkovich and C. Levy, “Managing the people side of risk,” *McKinsey and Company*, 2015. [Online]. Available: https://www.mckinsey.com/business-functions/risk/our-insights/managing-the-people-side-of-risk. [Accessed: 21-Apr-2019].

[51] The Institute of International Finance, “Risk Governance and Compliance.” [Online]. Available: https://www.iif.com/advocacy/risk-governance-and-compliance. [Accessed: 21-Apr-2019].

[52] IT Governance UK, “Cyber Risk Management,” *IT Governance UK*. [Online]. Available: https://www.itgovernance.co.uk/cyber-security-risk-management. [Accessed: 21-Apr-2019].

[53] National Institute of Standard and Technology (NIST), “NIST Special Publication 800-37 Revision 2. Risk Management Framework for Information Systems and Organizations. A System Life Cycle Approach for Security and Privacy,” p. 183, 2018.

[54] IsecT, “ISO/IEC 27005 risk management standard,” *IsecT*. [Online]. Available:

https://www.iso27001security.com/html/27005.html. [Accessed: 21-Apr-2019].

[55] C. Giardino, X. Wang, and P. Abrahamsson, “Why early-stage software startups fail: A behavioral framework,” *Lect. Notes Bus. Inf. Process.*, vol. 182 LNBIP, pp. 27–41, 2014.

[56] S. Ragan, “Code Spaces Forced to Close Its Doors After Security Incident,” *CSO Online*, 2014. [Online]. Available: https://www.csoonline.com/article/2365062/code-spaces-forced-to-close-its-doors-after-security-incident.html. [Accessed: 07-May-2019].

[57] M. Mimoso, “Hacker Puts Hosting Service Code Spaces Out of Business,” *Threatpost*, 2014. [Online]. Available: https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/. [Accessed: 07-May-2019].

[58] D. Cohen and B. Crabtree, “Semi-structured Interviews,” *Qualitative Research Guidelines Project*. [Online]. Available: http://www.qualres.org/HomeSemi-3629.html. [Accessed: 20-Mar-2019].

[59] IsecT, “ISO/IEC 27002 code of practice,” *IsecT*. [Online]. Available: https://www.iso27001security.com/html/27002.html?fbclid=IwAR1K9pTikNueAmr_mfA860db3EbYkn-40BSuHRViQTQOY8sos0jx9j8AS0M#Section5. [Accessed: 10-Feb-2019].

[60] Creative Research Systems, “Sample Size Calculator.” [Online]. Available: https://www.surveysystem.com/sscalc.htm. [Accessed: 12-Feb-2019].

[61] Statistics Solutions, “Cronbach’s Alpha.” [Online]. Available: https://www.statisticssolutions.com/cronbachs-alpha/. [Accessed: 09-May-2019].

[62] “Using and Interpreting Cronbach’s Alpha,” *University of Virginia Library*. [Online]. Available: https://data.library.virginia.edu/using-and-interpreting-cronbachs-alpha/. [Accessed: 10-May-2019].

[63] “t-Test in Excel - Easy Excel Tutorial,” *Excel Easy*. [Online]. Available: https://www.excel-easy.com/examples/t-test.html. [Accessed: 01-May-2019].

Appendix 1 – Final survey with remarks by the author (complied by the author based on [19][20])

Please note that the statements where the sequence number is marked with an asterisk (*) are reverse statements meaning that the scale for responses is reversed.

No.	Question	Question type	Options	Section	Remarks by the author
	Please provide basic information about your current job position. This helps to put your answers into wider context.				
1	How long have you worked for your current employer?	Mandatory, categorical choice	* Less than 1 year * 1 - 3 years * 4 - 6 years * Over 6 years	1 - Background information	
2	Which office are you from?	Mandatory, categorical choice	choice of respective office locations	1 - Background information	Answer options obfuscated by the author for confidentiality reasons.
3	Your current role in the company (choose the most applicable)	Mandatory, categorical choice	choice of respective roles in the company	1 - Background information	Answer options obfuscated by the author for confidentiality reasons.

No.	Question	Question type	Options	Section	Remarks by the author
4	Your current field of focus (choose the most applicable)	Mandatory, categorical choice	choice of respective business units in the company	1 - Background information	Answer options obfuscated by the author for confidentiality reasons.
	The following statements help to determine how your work tasks relate to the risk management procedures concerning the usage of information technology solutions. You might want to think about your daily tasks relating to (but not limited to) user access management, software deployment, onboarding/managing software vendors, company risk management in general, data quality (accuracy, completeness, etc), processing of personal data, designing marketing campaigns, information security, privacy, etc.				
5	I'm the owner of at least one information asset (e.g. information systems, online collaboration spaces, data) in our company.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
6	I'm the owner of at least one business process (i.e. a set of tasks and activities that will contribute to achieving company's goals).	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
7	I know where to find our company's risk register.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	

No.	Question	Question type	Options	Section	Remarks by the author
8	I know how to classify the information assets (e.g. information systems, data, files) based on their level of sensitivity.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
9	My work includes detecting risks around the usage of information technology solutions.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
10	My work includes evaluating risks around the usage of information technology solutions.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
11	My work includes making decisions on how to treat risks related to the usage of information technology solutions.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
12	My work includes allocating resources to mitigate risks related to the usage of information technology solutions.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
13	My work includes handling incidents related to the usage of information technology solutions.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
14	My work includes managing access rights to information assets (e.g. information systems, online collaboration spaces, data)	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	

No.	Question	Question type	Options	Section	Remarks by the author
15	My work includes conducting due diligence procedures when onboarding new software vendors (e.g. running background checks, verifying certifications).	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
16	My work includes ensuring physical security of our company's data (e.g. protection from fire, flood, burglary, etc).	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
17	My work includes managing company's policies.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
18	My work includes managing when our information assets (e.g. data, files) should be archived or deleted/destroyed.	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
19	My work includes collaborating with external auditors (e.g. finance auditors, IT auditors).	Mandatory, categorical scale	* yes * no * unsure	2 - Exposure to risk decision making process	
	The aim is to identify your general knowledge about information security. Please use your knowledge as it is. Remember that we are not assessing specifically your knowledge here but trying to measure the information security culture temperature in the				

No.	Question	Question type	Options	Section	Remarks by the author
	company as a whole. Getting your honest feedback is essential.				
20	Our company has a written information security policy.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Souce: Da Veiga 2008
21	I have read the information security policy sections relevant to my job.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Souce: Da Veiga 2008
22	I know where to get a copy of the information security policy.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Souce: Da Veiga 2008
23	I know what my responsibilities are regarding information security.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Souce: Da Veiga 2008
24	I know what the risk is when opening e-mails from unknown senders.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Souce: Da Veiga 2008 Comment: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
25*	I am allowed to download any files onto my work computer if they help me to do my job.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Source: Parsons HAIS-Q 2017, replacing one item from Da Veiga 2008 as the original statement seems to be outdated.
26*	I am allowed to use any online tools on my work computer if they help me to do my job.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Additional statement added by the author. Followed the logic the previous statement has Comment: Added the statement in order to also target the online tools (no download needed) that employees in young companies might use.
27	When working on a sensitive document, I must ensure that strangers can't see my laptop screen.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Source: Parsons HAIS-Q 2017, replacing one item from Da Veiga 2008 as the original statement represented behaviour not knowledge.
28	I can be fired for something I post on social media.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Source: Parsons HAIS-Q 2017, replacing one item from Da Veiga 2008 as the original statement had multiple choice answer and the "correct" answer could easily be presumed by the respondent. Modified the question presented by Parsons - switched from negation to

No.	Question	Question type	Options	Section	Remarks by the author
					affirmative tone of speech to make answering to the statement clearer.
29	I know how to report security incidents.	Mandatory, categorical scale	* yes * no * unsure	3a - Security culture - knowledge statements	Source: Parsons HAIS-Q 2017, replacing one item from Da Veiga 2008 as the original statement had multiple choice answer. Comment: adjusted the language to directly represent clear knowledge.
	The following statements aim to identify your current values and perception towards information security, i.e. what you feel and think about information security in your company. Please use your independent opinion. Remember that we are not assessing specifically your knowledge here but trying to measure the information security culture temperature in the company as a whole. Usually the first answer that comes to your mind, is the most accurate one. Getting your honest feedback is also essential in this section.				
30	Management (i.e. team leads and leads of leads) in my business unit adheres to the information security policy.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements	Source: Da Veiga 2008

No.	Question	Question type	Options	Section	Remarks by the author
				Leadership and Governance - Sponsorship	
31	The protection of information is perceived as important in my business unit.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Leadership and Governance - Sponsorship	Source: Da Veiga 2008
32	I think that top-level managers in our company are committed to protect information.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Leadership and Governance - Sponsorship	Source: Da Veiga 2008 Remark: adjusted language
33	It is necessary to protect information to achieve our company's business strategy.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
				Leadership and Governance - Strategy	
34	I believe the information security controls implemented in our company support the business strategy.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Leadership and Governance - Strategy	Source: Da Veiga 2008 Remark: adjusted language
35	I feel that information security controls in our company are adequately implemented.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Leadership and Governance - Governance	Source: Da Veiga 2008 Remark: adjusted language
36	I understand how information security is managed in our company.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
				Leadership and Governance - Governance	
37	It is important to understand what the threats to information assets (e.g. data, files) are in my business unit.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Leadership and Governance - Risk Management	Source: Da Veiga 2008 Comment: original was a conjunction, removed "vulnerabilities", also adjusted language
38	Our company's risk management processes allow adequate identification of risks related to our information assets (e.g. data, files).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Leadership and Governance - Risk Management	Source: Da Veiga 2008 Comment: adjusted language
39	I believe our company commits enough resources to protect information.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
				Leadership and Governance - Return on Investement	
40	Investing into information security should be seen as a necessary future investment.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Leadership and Governance - Return on Investement	Source: Da Veiga 2008
41	I think our company complies with applicable regulatory requirements relating to information security (e.g. the General Data Protection Regulation).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Leadership and Governance - Legal and Regulatory	Source: Da Veiga 2008 Remark: adjusted language and examples.

No.	Question	Question type	Options	Section	Remarks by the author
42	The information security policy is applicable to the information I use in my daily duties.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Security Policies - Policies, Procedures, Standards and Guidelines	Source: Da Veiga 2008 Remark: adjusted language
43	The contents of the information security policy are easy to understand.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Security Policies - Policies, Procedures, Standards and Guidelines	Source: Da Veiga 2008
44	I feel that our Security Team has adequate authority to ensure the implementation of information security controls.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure	3b - Security culture - perception statements	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
			4 - Agree 5 - Strongly agree	Security Management and Organisation - Program Organisation	
45	There are adequate information security specialists throughout our company to ensure the implementation of information security controls.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Security Management and Organisation - Program Organisation	Source: Da Veiga 2008 Remark: adjusted language
46	I feel that Security Team adequately assists on the implementation of information security controls.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Security Management and Organisation -	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
				Program Organisation	
47	Employees' key performance indicators (KPIs) should also reflect information security objectives (e.g. regular participation in security trainings).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Security Program Management - Monitor and Audit	Source: Da Veiga 2008 Remark: adjusted language
48	Employees should be monitored on their compliance to information security policies (e.g. measuring the use of e-mail, monitoring what software is installed on computers).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Security Program Management - Monitor and Audit	Source: Da Veiga 2008 Comment: removed the conjunction.
49	I feel comfortable that our company makes use of electronic monitoring techniques to monitor if I comply with the information security policy (e.g.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure	3b - Security culture - perception statements	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
	Internet sites visited, detection of programs executed).		4 - Agree 5 - Strongly agree	Security Program Management - Monitor and Audit	
50	Employees in our business unit adhere to the information security policy.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Security Program Management - Compliance	Source: Da Veiga 2008
51	I feel that action should be taken against anyone who does not adhere to the information security policy (e.g. if they share passwords or visit prohibited Internet sites).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Security Program Management - Compliance	Source: Da Veiga 2008
52	The contents of the information security policy were effectively explained to me.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure	3b - Security culture - perception	Source: Da Veiga 2008

No.	Question	Question type	Options	Section	Remarks by the author
			4 - Agree 5 - Strongly agree	statements User Security Management - Education and Training	
53*	Our employees need additional information security training to protect information.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security Management - Education and Training	Source: Da Veiga 2008 Remark: clarified the statement
54	Management (i.e. team leads and leads of leads) communicates relevant information security requirements to me (e.g. which data storing and sharing methods are permitted).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security Management - Trust	Source: Da Veiga 2008 Remark: adjusted language, clarified company Comment: updated the examples

No.	Question	Question type	Options	Section	Remarks by the author
55	I believe the internal IT Team implements information security controls (e.g. controlling access to computer systems).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security Management - Trust	Source: Da Veiga 2008 Remark: adjusted language
56	I am aware of the information security aspects related to my job (e.g. when to change my password or which work information is confidential).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security Management - Employee Awareness	Source: Da Veiga 2008
57	I accept my responsibility towards the protection of information.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security	Source: Da Veiga 2008 Remark: clarified the statement

No.	Question	Question type	Options	Section	Remarks by the author
				Management - Ethical Conduct	
58	It is important to be careful when talking about confidential information in public places.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security Management - Ethical Conduct	Source: Da Veiga 2008 Remark: adjusted language
59*	I feel that password sharing should be allowed to make access to information easier.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security Management - Ethical Conduct	Source: Da Veiga 2008 Comment: adjusted language
60	I believe that third parties (e.g. business partners, software vendors) who have access to confidential information preserve the confidentiality.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security	Source: Da Veiga 2008

No.	Question	Question type	Options	Section	Remarks by the author
				Management - Privacy	
61	There are clear instructions in our company on how to protect sensitive (confidential) customer information.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security Management - Privacy	Source: Da Veiga 2008 Remark: adjusted language
62	There are clear instructions in our company on how to protect sensitive (confidential) employee information.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security Management - Privacy	Source: Da Veiga 2008 Remark: adjusted language
63	Management keeps my private information (e.g. contact information or performance evaluation information) confidential.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements User Security	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
				Management - Privacy	
64	My business unit is protecting its information assets adequately (e.g. locking away confidential documents or encrypting data).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology Protection - Asset Management	Source: Da Veiga 2008 Remark: adjusted examples
65	I feel that the information I work with is protected adequately.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology Protection - Asset Management	Source: Da Veiga 2008
66	I think the software development processes followed in our company are adequate to ensure information security.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
				Protection - System Development	
67	I believe the information security controls I use in my daily job are adequate (e.g. VPN, multi-factor authentication).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology Protection - System Development	Source: Da Veiga 2008 Remark: clarified the examples
68	I think that the internal IT Team believes information security is important.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology Protection - Technical Operations	Source: Da Veiga 2008 Remark: adjusted language Comment: Da Veiga refers to Information Technology Services business unit. Decided to use internal IT team instead. Also adjusted language
69*	I think that the protection of information is mainly the responsibility of our Security Team.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure	3b - Security culture - perception	Source: Da Veiga 2008 Remark: adjusted language Comment: Da Veiga refers to Information

No.	Question	Question type	Options	Section	Remarks by the author
			4 - Agree 5 - Strongly agree	statements Technology Protection - Technical Operations	Technology Services business unit. Decided to use information security team instead.
70	I believe our incident management process is effective in resolving information security incidents.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology Protection - Incident Management	Source: Da Veiga 2008 Remark: adjusted language
71	The information assets (e.g. data, files) I work with need to be protected.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology Protection - Physical Environment	Source: Da Veiga 2008 Comment: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
72	I think that the office building I work from is safeguarded adequately to protect information assets (e.g. systems, data, files).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology Protection - Physical Environment	Source: Da Veiga 2008 Comment: adjusted language
73	I believe my business unit will be able to continue its daily operations in case of a disaster resulting in the loss of systems, people and/or premises (e.g. fire, explosion or flood).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Technology Protection - Business Continuity Management	Source: Da Veiga 2008
74	I know what to do in the event of a disaster resulting in the loss of systems, people and/or premises.	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements	Source: Da Veiga 2008 Remark: adjusted language

No.	Question	Question type	Options	Section	Remarks by the author
				Technology Protection - Business Continuity Management	
75	I accept that some inconvenience is necessary to protect information assets (e.g. locking away confidential documents, making back ups or changing my password regularly) .	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Change - Change	Source: Da Veiga 2008 Comment: adjusted language
76	Changes made to protect our information assets (e.g. systems, data, files) are accepted positively in our business unit (e.g. adopting multi-factor authentication methods).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Change - Change	Source: Da Veiga 2008 Remark: clarified the examples and adjusted language.
77	I am informed in a timely manner as to how information security changes will affect me (e.g. policy changes, changes in procedures, updates to computer software).	Mandatory, categorical scale	1 - Strongly disagree 2 - Disagree 3 - Unsure 4 - Agree 5 - Strongly agree	3b - Security culture - perception statements Change - Change	Source: Da Veiga 2008 Remark: clarified the examples and adjusted language.

Appendix 2 – Organisational culture characteristics perceived by the interviewees (complied by the author based on [45][46])

Culture element	Characteristic	Count of times the interviewees selected the characteristic	Culture type (this column was not shown to the interviewees)
Language	Heroes/heroines, storytellers	3	Organic Culture
Language	Acronyms and jargon	4	Mechanistic Culture
Language	Negative comments	1	Mechanistic Culture
Language	Positive myths and legends	3	Organic Culture
Artifacts and Symbols	Symbols represent integration and support	2	Organic Culture
Artifacts and Symbols	Open door policy	3	Organic Culture
Artifacts and Symbols	Symbols enforce segregation (suits and ties for managers)	1	Mechanistic Culture
Artifacts and Symbols	Closely monitored work hours	0	Mechanistic Culture
Patterns of Behavior	Reward is paycheck	0	Mechanistic Culture
Patterns of Behavior	Micromanagement	0	Mechanistic Culture
Patterns of Behavior	Celebrate work accomplishments	1	Organic Culture
Patterns of Behavior	Look for ways to do job better	4	Organic Culture

Culture element	**Characteristic**	**Count of times the interviewees selected the characteristic**	**Culture type (this column was not shown to the interviewees)**
Espoused Values	Carrot and stick reward system	0	Mechanistic Culture
Espoused Values	Collaboration	5	Organic Culture
Espoused Values	Innovation	3	Organic Culture
Espoused Values	Push away responsibility	0	Mechanistic Culture
Basic Underlying Assumptions	Employees are important assets	4	Organic Culture
Basic Underlying Assumptions	Employees must be coerced to work	0	Mechanistic Culture
Basic Underlying Assumptions	Employees need little direction	4	Organic Culture
Basic Underlying Assumptions	Employees need detailed direction	1	Mechanistic Culture