Delft University of Technology

MSc Thesis Project

AN INFORMATION SECURITY CULTURAL FRAMEWORK

A case study for the Netherlands

Author:
Shifaiz Mohamed – 4180216
Engineering and policy analysis
Faculty of Technology Policy and Management

Graduation Committee:
Chairman: Prof.dr.ir. Jan van den Berg
First supervisor: Prof.dr.ir. Pieter van Gelder
Second supervisor: Dr.ir. Bert Enserink

PREFACE

This report is the result of my graduation research for my master study of Engineering and Policy analysis. The report is about information security, a subject I became fascinated on during a lecture I attended at the EWI faculty. I encountered many difficult times during this project, and it lasted a lot longer than I expected, but I have gained an experience I will never forget. Every accomplishment after a setback, makes you stronger to tackle the next problem.

This could not have been done without the help of others. My first gratitude goes out to Prof. Jan van den Berg, Prof. Pieter van Gelder, and Dr. Bert Enserink for their guidance and support during this journey.

I am also grateful to my girlfriend, and her parents for always being there for me in terms of support and motivation.

Last but definitely not least, my special thanks goes out to my parents who provided me with the opportunity to study and reach my goals. Words cannot describe how grateful I am for their support. Also thanks to my brother and sister for their support.

Above all, I would like to thank God for the strength, wisdom and blessings he provides.

SUMMARY

Information security is defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction" according to the US law (US Government Legal Information Institute, Subchapter 111). One of the important measures to ensure information security is the information security policy. The information security policy is a document issued by the organization management, that defines the need of information security, given the organization's objectives and scope. It contains the controls (i.e. measures), guidelines and responsibilities necessary to safeguard the organization's resources. Technology alone cannot guarantee the security of an organization; the human aspects needs to be considered as well. The state of information security is dependent on human behavior, since humans can either follow or break the policy rules of an organization, so they can either weaken or strengthen the information security. Organizations acknowledge that human behavior, namely lack of awareness and understanding of risks, is the biggest challenge in information security. Therefore, they strive to create a security culture and embed it in the organization's culture with the aim to encourage employees to comply with the security policy. There are many claims and researches that state that awareness programs and trainings are essential to change the human behavior towards the information systems, but they do not elaborate on how to do it. There is no specific procedure on how an information security culture should be embedded in the organization. Therefore, this thesis aims to provide a guideline for establishing an information security cultural framework by considering the effects of national culture on human compliant behavior.

National culture has been identified as the underlying determinant of human behavior, since each country has dominant cultural traits that distinguish them from other countries. Not every scholar believes that national and organizational culture are related, but Hofstede does. Therefore, for this research Hofstede's cultural model was used, since the model relates the values of a national culture to the values of an organizational culture. In order to verify whether this model is applicable in the context of this research, the relation between national and organizational culture was first verified through interviews. Then the main research question for this thesis was answered: *Which factors of culture and which risk management measures need to be considered for ensuring information security compliant behavior of organization employees?* The research method is based

on processing data obtained through interviews and through an online survey. Based on the results of this analysis, a model was formulated and recommendation were drawn.

The conclusion is that there is a relation between national culture and the way employees comply with the security rules. More specifically, based on Hofstede, the Netherlands is considered to be an individualistic society, in which individuals primarily take care of themselves and of their immediate families only. Individualism has implications on the compliance with security measures, as employees put their own interests above those of the organization, and by doing so may neglect security rules. People from individualistic might ignore and not act if they encounter a colleague not living up to the security rules, since an incident caused by a colleague may affect the organization as a whole and not the person himself. Further, the Dutch culture has an average score on uncertainty avoidance, that is the extent to which people feel safe in uncertain situations. Uncertainty avoiding societies typically introduce more rules and procedures to deal with these uncertainties. Contrary to these expectations, the results of this research show that in the context considered the Dutch culture is not very uncertainty avoidant, and Dutch employees do not like rules and procedures as they limit them in their creativity. Not having a guideline with the security standards and rules to follow, could lead to unnecessary incidents. That is why, information security is a topic that needs rules and procedures in the form of a written policy to act as a guideline and constant reminder for employees on maintaining aware behavior. Instead of having rules and procedures, employees in the Netherlands rely on cooperation which is stimulated mainly within the departments of an organization, where people are inclined to help each other, and so may prevent security risks. This characteristic corresponds with the feminist dimension of the Hofstede model and it is beneficial for ensuring safety in organizations.

Following the main conclusion that national culture influences the way people comply with security rules, the following recommendations have been made. A written security policy is an important element of an information security culture as it provides rules and procedures for employees to deal with the information systems. However, it is important to formulate the security policy in a manner that it does not offend or unnecessarily limit the employees. Rather than being written as rules and procedures, a security policy can be formulated as a set of guidelines that make employees aware of the dangers and risks of careless behavior. Employees can also be primed with security artefacts present in the organization, which can indirectly stimulate them to comply with

the rules. Furthermore, awareness training is of great importance and should be department specific as each department faces different risks.

The companies that participated in the interviews had a Dutch culture. But there are also foreign companies situated in the Netherlands with their own culture., Thus for future research, it would be interesting to see the security differences between foreign companies and local companies in the Netherlands, especially how the employees perceive and comply with the security policies. Another possible future research is to examine the extent that changes in scores of Hofstede's dimension, affect information security. The score for uncertainty avoidance in Germany is only 12 points higher than in the Netherlands, but this already had some noticeable changes on the rules and procedures that are implemented.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Chapter 1 Introduction

The number of users of the Internet keeps growing every year and its use has become a custom of our daily lives. At the beginning of 2014, the diffusion of the internet has reached 84 % in Germany, 87 % in the US, 95 % in Scandinavian countries and 96 % in the Netherlands (van Deursen & van Dijk). The Internet has changed the way people work, learn, play and communicate, since it can be used for making financial transactions, streaming of media, accessing social media and for many other purposes. It has opened many new business opportunities for firms, as many of them use this medium to sell or promote their products online and in this way reach a large audience with no geographical constraints.

However, as Pablo Picasso stated: "every positive value has its price in negative terms", and this holds also for the Internet. The increased use of the internet has led to an increased number of cyber-attacks on organizations' ICT infractructure. For instance, in the UK, 74 % of all organizations were attacked in 2004, compared to only 44 % in 2000, with the security breaches costing around $17 billion every year (Doherty, Anastasakis, & Fulford, 2009).

Cyber-attacks can be defined as the use of information technology to attack networks, computer systems and telecommunication infrastructures (Gorge, 2007). A cyber-attack is an intrusion, which is defined as any action taken by an adversary to gain access to a system to steal, monitor confidential information or to disrupt it from functioning properly (Day, 2013). Although security threats often originate outside the organization, their impact can be aggravated by inappriate behavior of employees inside the organization. This is referred to as insider threat, and detailed in the next section.

INSIDER THREAT

Intrusions are caused on purpose by outsiders who penetrate the network. Still, intrusions are not considered as the only problem: incidents caused by employees form an important threat for information security (Da Veiga & Martins, 2015b). According to a survey conducted by PricewaterhouseCoopers, 31 % of current employees and 27 % of former employees are responsible for these incidents ("Managing Cyber Risks in an Interconnected World", 2014). In the report of PWC was also noted that, even though 32% of the respondents claimed that insiders'

incidents are costlier and more damaging than outsider crimes, many of the organizations do not have programs to deal with them. According to PWC's, only 54% of organizations in South America, 63 % in Asia, 55 % in Europe have information security and awareness programs.

Many incidents caused by the employee occur due to the lack of compliance with security policies (Kolkowska & Dhillon, 2013). A rule of thumb used by professionals is the 20-60-20 rule (Moberly, 2014). It states that 20 % of the people we work with are honest and exhibit high levels of personal and professional integrity. The other 20 % is the opposite - people who possess little sense of professional and personal integrity. The large group of 60 % employees are those who do not demonstrate any particular dishonest, unethical or illegal behavior that would purposely put their employer's assets at risk. However, their future behavior can be influenced by their interpretation of the sanctions that the employer imposes on those who violate company information policies.

1.1 RESEARCH PROBLEM

Incidents caused by employees are a big concern in information security and since the purpose of information security is to protect the confidentiality, integrity and availability of information systems, these incidents should be minimized or eliminated (Koskosas, Kakoulidis, Siomos, 2011). However, this concern goes further than just having technical measures in place. One has to deal with the human aspect of information security, namely the attitude people have towards the information systems and the way they comply with the policies. Lack of compliance with the security policies can occur if employees do not know or understand the security policies, or by simply resisting to follow them (Kolkowska & Dhillon, 2013). There are different ways in which organizations try to achieve employees' compliant behavior. Some organizations try to enforce tighter information policies and technical obligations to enforce employee compliance. However, a survey conducted by Macromil Embrain (2014) indicated that this type of enforcement may have a negative effect on employees' compliance, as it induces stress on them, which in turn reduces their willingness to comply with the rules (C. Lee, Lee, & Kim, 2016).

Other studies emphasize that the cultivation of an information security culture can improve employees' compliance with the security policies (Da Veiga & Martins, 2015b). An organizational culture is defined as "a shared philosophy, ideology, value, assumption, beliefs, hope, behavior

and norms that bound an organization together" (Kilman, 1985). Thus, an information security culture is one were security is a value and norm within an organization, with the aim to cultivate information security values in employees their daily activities. Many researchers have called for the creation of an information security policy to influence the behavior of employees towards better information security and that this information security culture should be embedded in the organizational culture. The majority of organizations do have an organizational culture with certain rules, values and procedures that they share. Lim et al. state that the organizational culture influences the establishment of an information security culture, and thus employees' compliancy with the security rules (Lim, Chang, Maynard, & Ahmad, 2009). In turn, some scholars believe that organization culture is influenced by national culture, since the managers and majority of the employees have the same national cultural traits, which manifest in the organization (Geert Hofstede, 1994). This means that employees' compliance with the security policy may be related to the national culture.

There are several frameworks focused on ensuring information security, from which ISO 27000, and the COBIT 5 are frequently used. These frameworks focus on risk management with the help of best practices, but do not include the effect of national culture. Therefore, this thesis will study the relationship between national culture and employees' compliance with information security policies.

1.2 RESEARCH OBJECTIVE

The objective of the thesis is to study the relation between national culture and organizational culture, and in turn with the employees' compliant behavior with security policies. Culture is considered important to the study of information technology, because national, organizational and group culture can influence the successful implementation of information technology (Leidner & Kayworth, 2006). Not everyone believes that there is a relation between national and organizational culture. Some scholars argue that organizations create their unique culture with values independent of the national cultural values {Lee, 2016 #153} These scholars believe, that thanks to the different values, organizations are able to be competitive towards each other. On the other hand, some scholars believe that there is a relation between national culture and organizational culture. These scholars claim that the organizations' founders and dominant elites create and shape an organization based on their national values and assumptions and that these

values are meaningful for their environment (Nelson & Gopalan, 2003). Hofstede is one of the scholars who believes that there is a relation between national and organizational culture. He developed a cultural model from which nations and groups could be distinguished based on their dominant cultural traits. As national culture influences organizational culture, it may in turn affect the establishment of an information security culture. These cultural traits may influence the way people perceive and behave towards the information systems. In this thesis, Hofstede's cultural model is used to study the relation between culture and employees' compliant behavior and to propose solutions to deal with the possible negative effect of this relation.

RESEARCH QUESTIONS

The main research question is: *Which factors of culture and which risk management measures need to be considered for ensuring information security compliant behavior of organization employees?*

The sub-question for this research are:

- *What is the importance of an information security culture?*
- *What are the key elements of an information security culture?*
- *What is the relation between national and organizational culture?*

1.3 RESEARCH METHOD

An organization can be considered as a secure one if the security policies and measures it has implemented are able to withstand security incidents in order to avoid costly business disruptions (Campbell, 2014). The security policies and measures that are implemented should be able to detect and prevent external and internal security incidents.

The methodological approach used in this thesis is a combination of a qualitative and a quantitative one. The qualitative part is based on collecting information via literature research and interviews with experts in order to grasp their knowledge. The quantitative approach is based on gathering data through questionnaires, and the subsequent statistical analysis of the data.

From the literature study, factors were identified that influence information security in organizations. This data originated from journals, scientific articles, white papers, websites and

other sources describing security-related measures. Another source of information is the ISO 27000 norm which describes risk management controls to ensure information security. From this framework, the controls written policy and compliance were focused on, as these are related to employee behavior.

To verify whether there is a relation between national and organization culture, interviews have been conducted in several companies in the Netherlands, based on Hofstede's cultural model. Hofstede's model distinguishes groups based on their dominant cultural traits, which he divided in five main dimensions. The interview topics were based on these dimensions, and the respondents gave their opinion on whether they consider Hofstede's model valid and elaborate on whether they believe that there is a relation between national and organizational culture. In addition, the interviews were also conducted to study the effect of national culture on information security and the effect of national culture on employees' compliancy with the security policies.

In addition to the interviews, an online survey was developed to further evaluate the relation between culture and information security. The selected companies were in the sectors: energy, accountancy, ICT, manufacturing, assurance, financial institutions, transportation and logistics and databases services. These sectors were chosen, since according to the global survey by PWC they are the most targeted sectors with respect to security threats ("Managing Cyber Risks in an Interconnected World", 2014). The size of the company was not chosen as a criterion, in order to be able to differentiate in the data between small, medium and large sized companies. An inherent limitation of this research method the low response rate - often lower than 20% (Shih & Fan, 2009). To maximize the response rate, a letter containing the survey link and a description of this project was sent to the postal address of each company, using official TU Delft envelopes. The data of the questionnaire was analyzed using the statistical analysis tool SPSS. The data was processed with descriptive test to analyze the extent of risk management measures implemented in the companies

1.4 RESEARCH FRAMEWORK

The goal of the research is to develop an information security framework that includes risk management controls as well as the effect of culture on employees' security-compliant behavior, as illustrated in Figure 1. First the relation between National and organizational culture is verified,

and the risk management controls. These risk management control include technical, and organizational controls related to employees' compliant behavior.

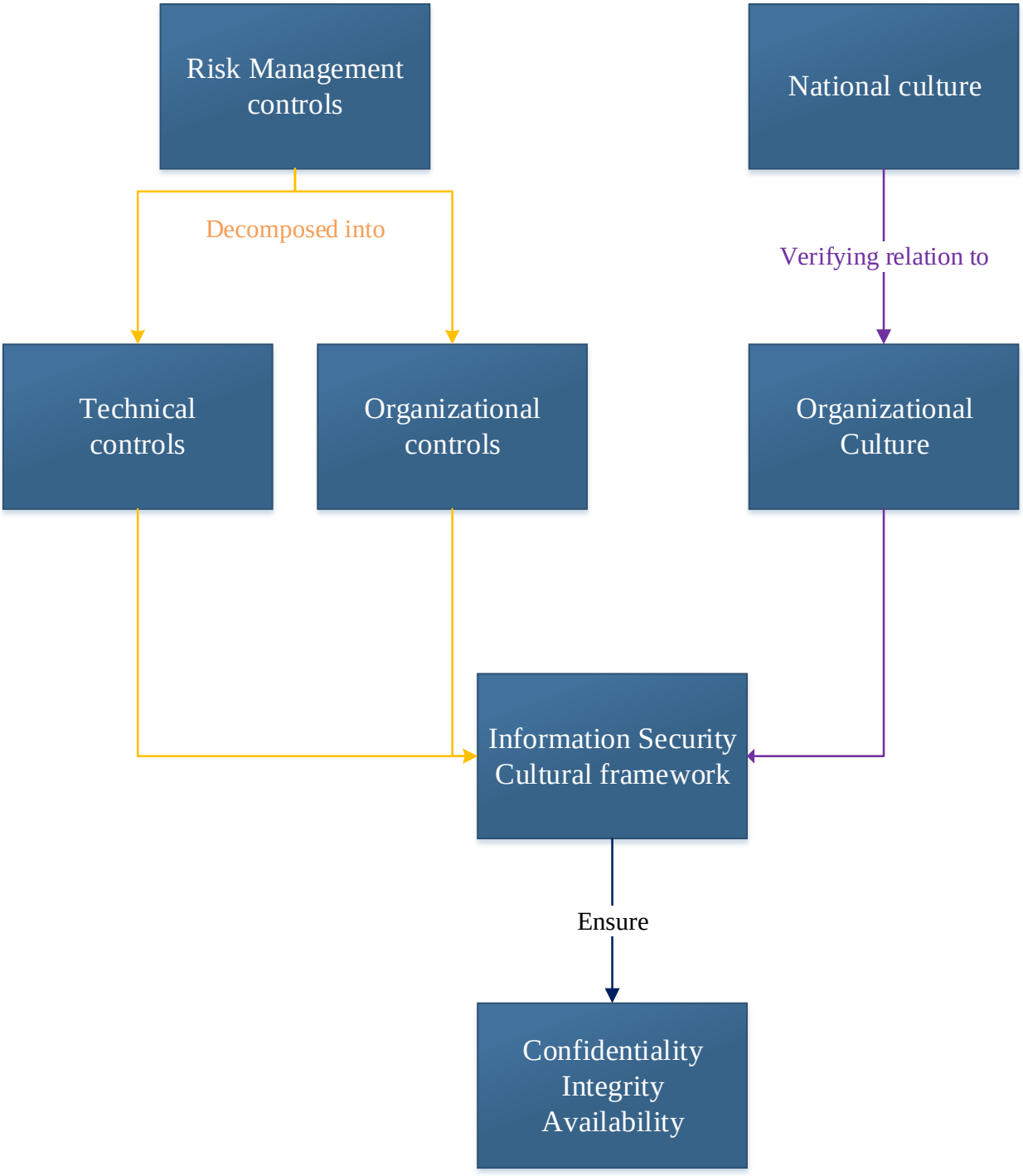

Figure 1: THEORETICAL FRAMEWORK OF the thesis.

1.5 OUTLINE OF THE THESIS

In Chapter 1, we have introduced the research problem and objective of the thesis, which is to propose an information security framework consisting of risk management controls and cultural effects on information security to improve employees' compliant behavior. In Chapter 2 the development of information security is elaborated on and the chapter also describes the risk management controls aimed at improving security compliant behavior. Chapter 4 presents the results and analyses of the interviews. In this chapter, the relation between national and organizational culture is also verified. In Chapter 5, the survey results are presented and analyzed. The proposed framework is presented and evaluated in Chapter 6. Finally, the conclusions and recommendations are presented in Chapters 7 and 8, respectively.

CHAPTER 2 INFORMATION SECURITY

2.1 DEFINITION OF INFORMATION SECURITY

Every major change in the existence of mankind is derived from a technological discovery related to communication (Rodríguez, Busco, & Flores, 2015). Language and writing were the first communication techniques, but later technologies such as the telephone, radio, TV, and the Internet arrived. During the years, information technology evolved and it has become widely used in organizations for carrying out their business activities. Information technology is defined as the use of any computer, networking, infrastructure and processes to create, process, store, secure and exchange electronic data (Burrows, 1993).

One of the big communication breakthroughs, is the Internet. The Internet has opened many new business opportunities for firms and entrepreneurs, as many of them use the internet to sell or promote their products online, and can therefore reach a bigger audience, without any geographical constraints. However, every technological change results in new exploitable possibilities for criminals. For example, as the mobile phone industry grew, the number of people that were scammed also increased (Ghosh, 2010). Many people received a call or a text in which a criminal presents him/herself as a banker or a representative of a government institution and asks bank information, which later can be used to steal money. These scams still occur, but the number of people tricked decreases, since scam methods became well known and general public has been made aware of them.

Besides individuals, organizations are often targeted by intruders who try to steal information or money or just to spy on the systems (Seebruck, 2015). An intrusion is defined as any action taken by an adversary to gain access to a system to steal and monitor confidential information or to disrupt it from functioning properly (Day, 2013).

If a system becomes compromised, classified information may be stolen, which may lead to million dollar losses. Therefore, the information systems need to be secure to deal with intrusions. So what is information security?

According to the US law (US Government Legal Information Institute, Subchapter 111), information security is defined as *"protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction"*. In practice this boils down to protecting the relevant assets, which can be physical items, software, source code or just any data.

However, this definition does not cover all aspects required in information security. It refers to unauthorized access, while it does not cover the situation in which intruders have authorized access to the information system. This is crucial as one of the concerns in information security are incidents caused by current and former employees (Da Veiga & Martins, 2015b). An incident is not the same as an intrusion, since the first may happen by accident or by careless behavior, while an intrusion is committed on purpose by the intruder. Therefore, information security should be defined as protecting information from unauthorized access and also from those who have authorized access, but have bad intentions or exhibit careless behavior.

2.2 DEVELOPMENT OF INFORMATION SECURITY

Information security has developed over the years in order to deal with the developing threats. Professor Basie von Solms, described the development of information security in three waves, the technical wave, the management wave, and the institutional wave (von Solms, 2000). Each wave can be defined as an incremental focus area for information security.

THE TECHNICAL WAVE

The technical wave, which dates back to the early eighties is characterized by a technical approach to information security. In this wave, information security was addressed as something that can be solved with the built in facilities on the operating systems, such as user IDs and passwords. These issues were left to be solved by technical experts.

THE MANAGEMENT WAVE

The management wave, which lasted from about the early eighties till the mid-nineties, was driven by the realization that information security has a management dimension oriented at security policies which are essential to be implemented (von Solms, 2000). In this wave information security managers were appointed and they started to develop policies and procedures, which they then reported to the top management.

THE INSTITUTIONAL WAVE

Finally, the third wave came, which focuses on the standardization of information security in a company. It covers aspects such as best practices, certification, measurement and monitoring of information security, and the need for a security culture.

In 2006, professor von Solms published the article "Information Security - the Fourth Wave" describing the wave of Information Security Governance (von Solms, 2006). It stresses that the drivers in this wave are related to Corporate Governance and regulatory areas. The board of members should have access to accurate, relevant and timely information, which can be ensured by having a security program in place. The board must realize that information security governance has an impact on the whole organizations and therefore it should be well managed.

However, the third wave, the establishment of a security culture to deal with the human factor, is still being explored, since human behavior is still considered as a big concern in information security (Ashenden, 2008). Especially since many organizations do not have an information security culture (Lim et al., 2009).

2.3 CONCEPTS OF INFORMATION SECURITY

What is the purpose of information security? What needs to be protected and what should be considered in an information security framework? The purpose of information security is to ensure the confidentiality, integrity and availability of information - the CIA triad (Andress, 2014), see also Figure 2. The CIA triad is a model designed to guide policies for information security within an organization.

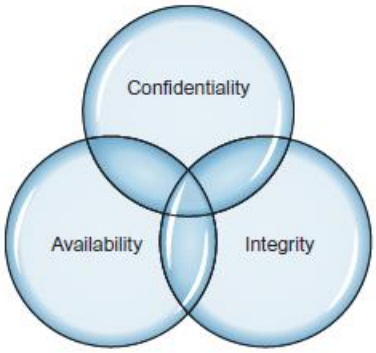

Figure 2: CIA Triad

CONFIDENTIALITY: BASIC INFORMATION SECURITY PRINCIPLES

Confidentiality defines the procedures and measures that need to be undertaken to ensure that sensitive information does not reach the wrong people. Access to data must therefore be restricted to those who have authorization (Cabric, 2015). These procedures include:

- Management of user profiles
- Data classification
- Clean desk policy
- Confidentiality and non-disclosure agreements with employees and contractors
- Password policy
- Rules and regulations for employee IT use
- Trainings for employees and implemented procedures aimed at preventing, detecting, and stopping social engineering attacks.

An extensive list of other measures that can be taken into account for maintaining confidentiality can be found in the Appendix I.

INTEGRITY

The aim of integrity is to make sure that the information remains intact and unaltered. It involves maintaining the consistency, accuracy, and trustworthiness of data during its whole life cycle (Cabric, 2015). An example of a compromised integrity is the one where a client information bank details are changed by a bank employee in order to commit fraud. In order to maintain integrity, unauthorized changes need to be prevented, but one also needs the ability to revert changes that have been made. Integrity is managed with controls consisting with several primary objectives (Andress, 2014):

- Prevention
- Detection of fraud or a reasonable indication that fraud has been committed
- Communication and reporting
- Reaction that includes investigation, disciplinary and legal proceedings and mitigation of damage
- Design and implementation of improvement actions aimed at closing detected gaps

AVAILABILITY

The aim of availability is to ensure business continuity by identifying and dealing with problems immediately. Availability should be ensured by processes that identify potential impacts of risks, and provide effective responses in order to safeguard the interests of its key stakeholders, reputation, brand and value creating activities. Loss of availability can refer to a variety of disruptions anywhere in the chain from where data can be accessed. These disruptions can be caused by power failure, operating system or application problems, and network attacks such as a Denial of service (DoS) attacks.

2.4 TYPES OF SECURITY ATTACKS

In this section intrusions are categorized based on the type of attack and the corresponding risk. Attacks are divided into four types: interception, interruption, modification and fabrication (Pawar & Anuradha, 2015).

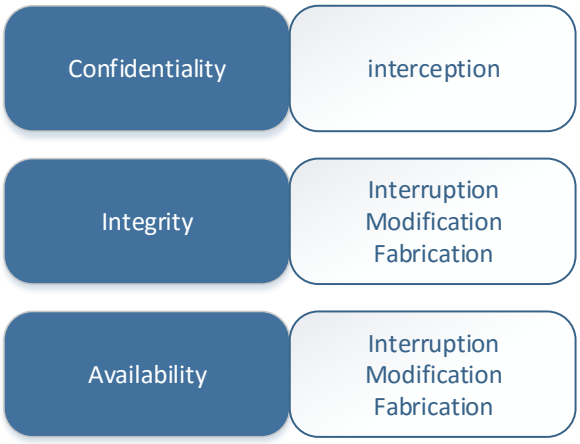

Figure 3: Types of attack and the corresponding risk.

INTERCEPTION

These attacks allow unauthorized users to access data, applications or a secure environment (Pandey, 2010). They usually are attacks against confidentiality and might take the form of unauthorized file viewing or copying, eavesdropping of conversations, reading emails.

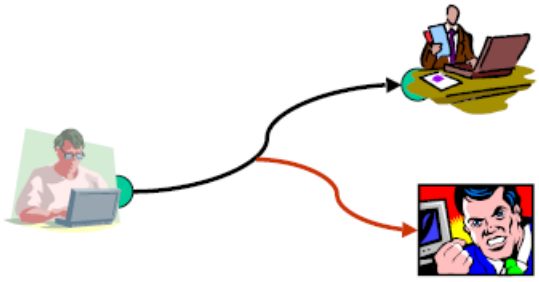

Figure 4: Interception attack (Andress, 2014)

INTERRUPTION

An interruption attack causes the assets to be unusable or unavailable on a temporary or permanent basis. These attacks affect availability as well as integrity depending on the type of attack. For example, a DoS attack on a server can be classified as an availability attack, since the server won't be available for a while. Another example of an interruption attack, is the one where an attacker manipulates processes on a database preventing access to the system. It can be considered as an integrity attack, since this attack may cause data loss and/or corruption.

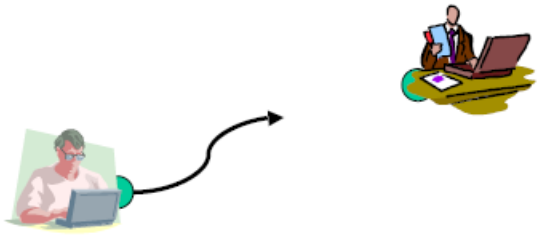

Figure 5: Interruption attack (Andress, 2014)

MODIFICATION

Modification attacks involve attacks where data is altered, and is usually considered as an integrity attack but can also be an availability attack. In some cases, where the altered data is a configuration file, the availability of the service may be affected.

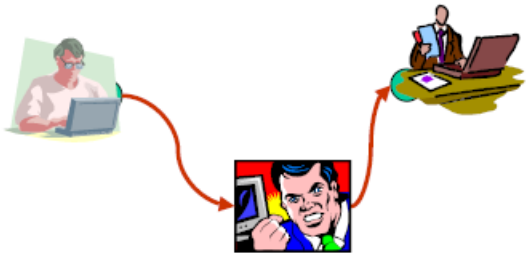

Figure 6: Modification attack (Andress, 2014)

FABRICATION

These attacks involve the generation of data, processes by an unauthorized user (Ahmad, Verma, Kumar and Shekhar, 2011). An example of a fabrication integrity attack is spoofing, where an email header is forged so that it appears that the message originated from somewhere or someone else with the goal that the recipient responds to the message. A fabrication availability attack is the one where enough traffic is generated to disrupt the system from operating properly.

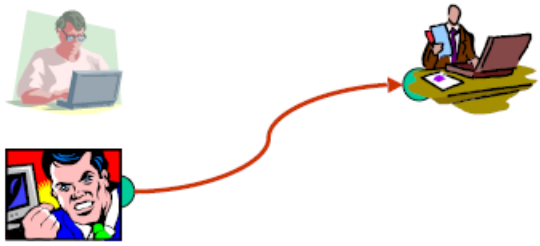

Figure 7: Fabrication attack (Andress, 2014)

2.5 ATTACK TOOLS

The threats mentioned in Section 2.2 are executed by technical tools either self-developed or readily available exploit kits. In this chapter the main tools that are used in online threats are mentioned.

TROJANS

These are small programs that often look like useful programs. The purpose of a Trojan is to exploit security deficiencies in order to gain access to the user's information. A feature of a Trojan is that it is able to download and install other threats onto the compromised computer.

BOTNETS

Botnets are networks that are formed by machines compromised by malware. These networks have been created to conduct illegal activities and endanger the operation of private and public services. It is believed that 16-25 % of the computers connected to the internet are members of a botnet (Silva, Silva, Pinto, & Salles, 2013). The attacker takes control of the machines in the botnet to execute criminal activities such as information and identity theft.

PHISHING

Phishing are illegal activities where hackers pose as a legitimate organization or person to motivate people to open their messages (Sumner, 2016). They use these methods to acquire someone's credentials in order to gain access to a system.

MALWARE

These are software application that are meant to disrupt the operation of a system or to gather confidential information. Some examples of malware are:

VIRUSES

A virus is a program that is able to spread itself by initially infecting the executable files and then reproduce itself (Granova & Slaviero, 2013). The three main types of viruses based on the purpose they have are: a boot sector, a program, and macro viruses. A boot-sector virus attacks the boot sector and disables the whole system either temporary or permanently, while program type viruses come in an executable format and loads automatically. Finally, macro viruses are small applications in a file that automate the performance of some tasks.

WORMS

Worms have almost the same characteristics as viruses. In addition, they are programmed to penetrate every workstation on a network.

DENIAL OF SERVICE (DOS)

In a DoS attack the service to the rightful users, networks, systems or other resources is disrupted and/or denied (Eloff & Granova, 2009). The network becomes inaccessible due to the large amount of traffic that is generated, which causes servers to crash, routers to overload and prevent other network functions to work properly. To perform DoS attacks, no big set of skills are required by

the attacker, since all the necessary tools are available on the internet. These attackers gain access to an end user's machine through a communication channel such as IRC, PTTP or HTTP by covertly installing a program on their PC. When they have already compromised a number of workstations, they use these in a DoS attack against a specific network. The adoption of the Supervisory Control and Data Acquisition (SCADA) system for infrastructures in the US has made it attractive for DoS attacks, since SCADA interconnects different infrastructures such as power, water and utilities (Eloff & Granova, 2009). A DoS attack on this network would cause some real problems.

DISTRIBUTED DOS (DDOS)

A DDoS attack also involves flooding the target resource with external communication requests, which causes the system to overload and slows its response so that it becomes unavailable. The difference between DoS and DDoS attacks is that in DoS attacks one computer and one internet connection is used to flood a server with packets, while many devices and multiple internet connections are used in DDoS attack, making it more difficult to deflect since there is no single attacker to defend from. In order to execute a DDoS attack, a number of workstations need to be compromised by the attacker. To do this, he must gain unauthorized access to the system in order to install the software necessary to execute the attack. After this is done, he uses the compromised systems to send data to the network he wants to flood. Some well-known tools used in DDoS attacks are TribeFloodNet (TFN), Trinoo, and Stacheldraht, which can be used against UNIX and Windows systems.

These are the most common attacks that occur through the internet. However, an intrusion or data theft may also be caused by employees, either accidentally or on purpose. According a Ponemon Institute report released in September 2014, more than 80 percent of the breaches were caused by employee negligence. Some employees shared their password, other lost a USB or laptop, mishandled files or left the door to the network operations center open. Most of the insider incidents that occurred were not intentional, but happened due to lack of knowledge or careless behavior. This can be minimized by having a written policy defining rules and guidelines that employees can follow. Such a policy will help make employees more aware of the problems and make them more compliant with the security rules.

2.6 ACTORS INVOLVED WITH INFORMATION SECURITY

The actors who are a part of the information security landscape can be divided into malicious actors, which are those with an illegal intent, governmental bodies who develop policies and regulations regarding the information security, and finally the targets.

Table 1: Main actors in information security landscape (Sigholm, 2013)

Actor group	*Actor*
Malicious	Governments Cyber vandals Script kiddies Hacktivists Insiders Private organizations
Targets	Governments Insiders Private organizations
Regulatory bodies	Governments Regulatory agencies

CYBER VANDALS

These are people who create malware or use other tools to vandalize another computer, network or website by damaging data or leaving some kind of signature on it. These people often do it to prove a point and out of their own desire and pleasure. A DOS attack can be seen as cyber vandalism.

SCRIPT KIDDIES

They are not so skilled hackers or attackers who makes use of scripts or programs developed by more skilled hackers to penetrate a network ("Script Kiddies Rule The Internet," 2001). They are usually younger people who try to gain attention of their peers.

HACKTIVISTS

These are people who hack a network out of 'ethical' reasons. They usually take a network down with an DOS attack or leak sensitive and embarrassing information to promote their cause (Hiller & Russell, 2013). Information they leak could be from criminals who try to transfer funds, credit card information or trade secrets. A well-known platform for hacktivists is the WikiLeaks, which is a website where people can place information about governmental institutions and companies anonymously.

GOVERNMENTS

A intrusion in a governmental system of a state executed by another state (Lilienthal & Ahmad, 2015). However, it is not clear yet if this intrusion causes a breach of Article 2(4) of the UN Charter. It is considered a breach when an intrusion causes significant risk of public safety and national security. Cyber warfare is relatively new, there is no formal definition and also no laws on how to deal with it. The traditional definition of warfare as a military action using some kind of physical force on another state, cannot be used for cyber warfare. This definition was based on physical boundaries, but there are no geographical restraints on the internet. Cyber warfare can be defined as actions by a state to gain access to another state's network with the aim of causing damage or stealing information with a political motive.

INSIDERS

Human errors cause 52 % of the breaches in organizations (Korolov, 2015). These errors usually occur due to negligence or lack of training. Employees often take paper records home or download files to an unsecured personal hard drive. In a survey conducted by Forrester, 42 % of employees admitted that they used a personal computer or smartphone to get their work done, even if it is prohibited to do so (Khanna, 2013). These devices do not have the required encryption to withstand malicious attacks. Besides the breaches that are caused unintentionally, there are also intentional breaches. The Snowden leak, where an employee leaked classified information of his employer, is an example of an intentional employee data leak. Thus, an insider can also be considered as a malicious actor and a target.

PRIVATE ORGANIZATIONS

Besides intrusion with a political agenda on governmental systems, there are also intrusions caused by private organizations on other organizations (usually competitors) in order to steal trade secrets or to shut the network down to decrease revenue.

REGULATORY BODIES

Regulatory agencies are those who develop and define policies and best practices with the purpose to force organizations to protect their information systems (Williams, 2001). The best practices and policies are guidelines and minimal requirements that these organizations need to comply with. For example, the ISO/IEC 1799 security framework mentions that a written policy should be available to all employees (Schumacher, 2002).

2.7 RISK MANAGEMENT OF THE INSIDERS THREAT

A risk is measured by the probability of an event occurring and the impact it can have. The severity of the risk is determined by these two factors. The higher the probability and the bigger the impact of the risk, the more severe the risk will be. Information security risk management is the means by which organizations try to preserve the confidentiality, integrity and availability of information resources (Webb, Ahmad, Maynard, & Shanks, 2014). The ISO 27000 series is one of the information security best practices standards that suggest a range of managerial and technical controls to protect information resources. The objectives of information security risk management are risk identification, risk assessment, risk treatment, and risk review. The ISO 27000 defines the following control groups for risk management.

- Security Policies – An information security policy document for supporting information security in accordance with the organization business objectives and scope.
- Organization of information security – The management of information security in the organization by the managers through clear direction and demonstrated commitment.
- Human resource security – To ensure that employees, and contractors understand their responsibilities, and that they are suitable for their roles. This can be achieved by background checks on all candidates for employment.
- Asset management – To maintain and achieve appropriate protection of organizational assets such as inventory and acceptable use of assets.

- Access control – To control access to information with user registration, password management, privilege management, etc.
- Cryptography – Protect confidentiality, authenticity and integrity of information with the help of cryptography.
- Physical and environmental security – To prevent unauthorized physical access, damage and interference to the organization's premises and information.
- Operations and communications security – To ensure the protection of information in networks and the protection of the supporting infrastructure.
- System acquisition, development and maintenance – To ensure that security is an integral part of information systems.
- Information security incident management – To ensure that information security events and weaknesses associated with information systems are communicated in a manner that allows timely corrective actions to be taken.
- Information security aspects of business continuity management - To counteract interruptions to business activities and protect critical business processes from the effects of major failures of information systems.
- Compliance – To avoid breaches of any law, statuary, regulatory or contractual obligations, both by the employee and organization as a whole.

The security controls focus on the mitigation and/or prevention of the risks. Some security measures eliminate specific risks while others reduce the risk. Having security measures installed does not guarantee that an incident will not occur, but they can minimize the chance of it occurring or the impact it can have. The types of security measures based on their function are divided into the following categories:

- Preventive: These are measures that can be taken before the incident takes place.

- Reductive: These are measures that are aimed at minimizing the damage in case an intrusion occurs. They focus on reduction of the impact of an incident for example by creating backups.

- Detective: These are measures with the function of detecting a security intrusion in an early stage.

- Repressive: These are measures that minimize the damage in case an incident occurred and focus on counteracting the continuation of an incident. Examples of these measures are automatic locking of user accounts after specified number of unsuccessful log-on attempts or blocking of the network.

- Corrective measures: These are measures that are aimed at repairing damage and restoring the status as before the incident.

2.7.1 SECURITY POLICY

There are various controls and measures that need to be implemented in an organization to ensure an effective information security. One of the important information security controls is an information security policy (Höne & Eloff, 2002). The objective of an information security policy is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations (Dalziel, 2015). A security policy document consists of all the regulations and mechanisms needed to make the organization less susceptible to attacks. It guides the behaviour of the employees by stating what their restrictions and possibilities are. The security policy document should contain the organization's approach to managing information security and it should include (Sennewald & Baillie, 2016) :

a) A definition of information security, its overall objectives and scope.
b) A statement supporting the goals and principles of information security in line with the business strategy and objectives.
c) Control objectives for risk management, which are required to address the risk of a network by identifying vulnerabilities and information on what elements are in place to mitigate risks.
d) A definition and specific responsibilities for information security management including reporting information security incidents.
e) Explanation of the security policies, standards and principles important to the organization's goal.
f) Security roles and responsibilities agreement that needs to be signed by employees, contractors and third party users to reduce the risk of theft, fraud or misuse of facilities.
g) Information security policy violations and disciplinary actions.

A security policy should cover the following areas:

PEOPLE

- Roles
- Responsibilities
- Guidelines

ORGANIZATION

- Strategies & Objectives
- Structure & culture

TECHNOLOGY

- Physical Infrastructure
- Applications
- Communications architecture

2.7.2 EMPLOYEES COMPLIANCE WITH SECURITY POLICIES

The ISO 27000 consist of many technical controls, and according to this framework, employees' compliance to the security policies is considered very important. That is why there is a separate control for compliance, with one of the objectives to ensure compliance to the security policies, rules and standards of the organization. A written security policy is required to state the objectives of the organization and the guidelines for employees. However, these guidelines mean nothing if people are not encouraged to abide by the rules. The ISO 27000 standard aims at improving compliance and awareness by incorporating information security values in employees' daily work activities.

Employee behavior is one of the root causes for information incidents and privacy breaches as a result of negligence, error or a deliberate malicious attack (Herold, 2010). Employees often have access to sensitive information such as social security numbers, financial information, and health information of customers or other employees. Therefore, it is important that employees process and treat the information in a secure way to prevent mistakes and damage. Employee behavior can

be classified in the categories: security-assuring behavior, security-compliant behavior, security-risk taking behavior, and security-damaging behavior (Guo, 2013).

SECURITY-ASSURING BEHAVIOR

Security-assuring behavior is an active, intentional behavior by an individual to protect the organization's information system. This is the most desirable behavior from the security perspective, with examples such as reporting security incidents and taking precautions to prevent them.

SECURITY-COMPLIANT BEHAVIOR

This is a behavior that is in line with the organizational security policies. People tend to refrain from prohibited behavior. This refers to intentional or unintentional behavior by employees that do not violate security policies. Employees who do this intentionally, may consciously try to avoid violating security policies or causing security problems. In the unintentional case, employees may do something without security issues in mind, but still in line with the organization's security policies.

SECURITY RISK-TAKING BEHAVIOR

This is an intentional behavior that may put the organization information system at risk, for instance by copying sensitive data to mobile devices, etc. This behavior may put the organization at risk and can be viewed as employees doing what is not expected of them.

SECURITY-DAMAGING BEHAVIOR

This is a behavior that will cause direct damage to the organization's information system such as data theft and cracking of passwords. Security damaging behavior is malicious and can be punished because it violates the laws and regulations of the society in general (Guo, 2013). These are offenses committed by the malicious actors mentioned in the previous chapter.

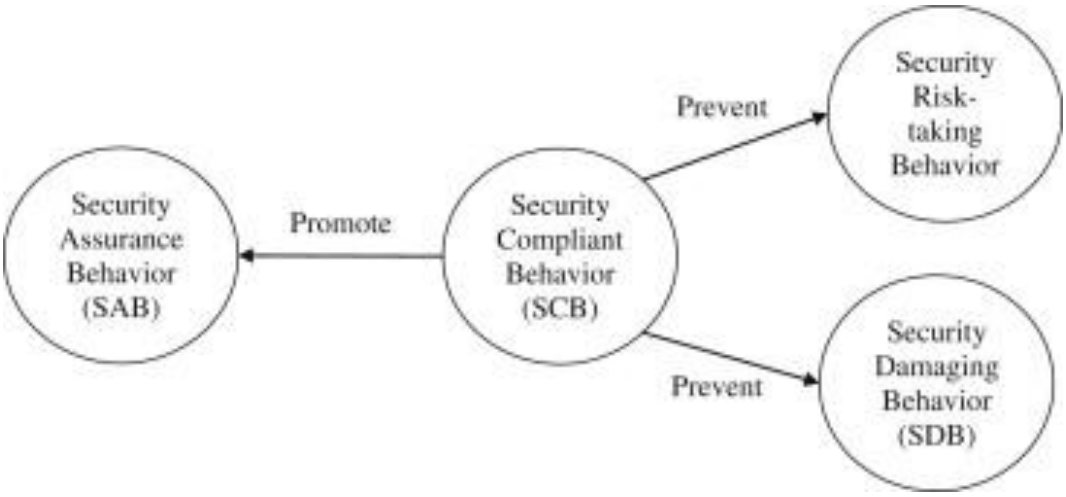

Figure 8: Security related behaviors. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404812001666

UNDESIRABLE BEHAVIOR

The security-risk-taking and security-damaging behaviors pose a risk for the protection of the information systems and are considered as undesirable behaviors. Some of these undesirable behaviors may be intentional and others unintentional. One can distinguish between the following types of undesired behavior.

UNETHICAL USE

This refers to inappropriate use of the information systems. Unauthorized, deliberate, and internally recognizable misuse of IS assets such as data theft, software piracy, stealing information, cracking passwords, etc.

CARELESS SECURITY BEHAVIOR

The act by people who are aware of but choose to neglect information security threats and countermeasures. These are often people who do not change their passwords or update security patches.

VIOLATION OF POLICY

This refers to employees' ignorance or negligence of organizational security policies. Examples are copying of sensitive data to USB drives and revealing confidential information to outsiders.

2.8 SUMMARY

From this chapter it can be concluded that the purpose of information security is to ensure the confidentiality, integrity and availability of information systems. This goes beyond implementing only technical measures, as human behaviour is unpredictable and needs to be explicitly considered in security policies. Based on the ISO 27000 framework, one of the important controls to ensure confidentiality, integrity, and availability, is a written policy. The policy document should cover the people, the organization and its infrastructures. The organizational goals, structure and objectives should be made clear in the policy document, as well as the role that employees have in achieving these goals. It should contain the guidelines and the description of the expected behaviour of employees with respect to the infrastructure. The infrastructure can further be divided into the physical infrastructure and the communication architecture.

The other ISO control considered in this research is the human compliance with the information security policies. Compliance can be ensured with the help of awareness programs and by managers who monitor the employees' behaviour. The written policy provides the guidelines and rules that the employees should follow. At the same time, there should also be compliancy controls in place to monitor if employees follow the rules. The summary of Chapter 2 is illustrated in Figure 10.

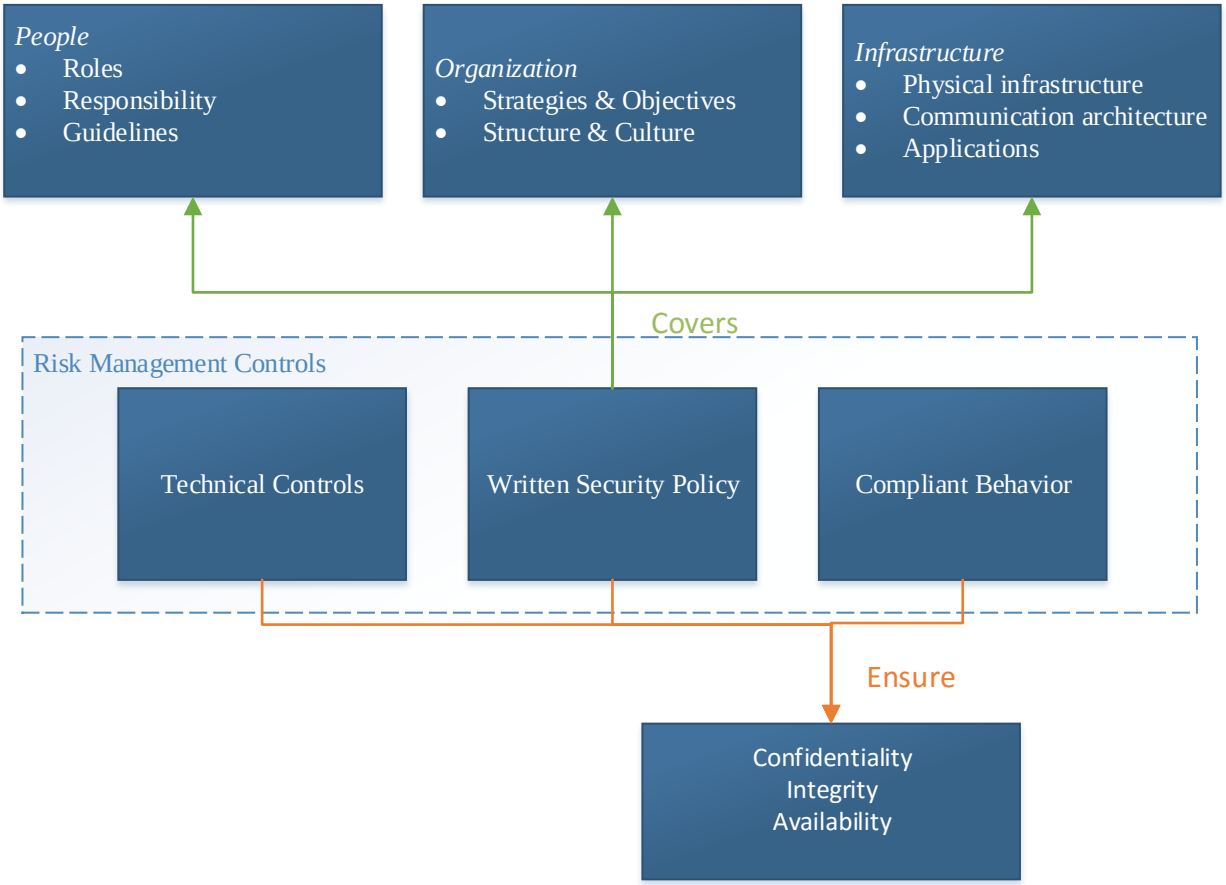

Figure 9: Summary of the concepts presented in Chapter 2.

CHAPTER 3 CULTURE

3.1 INTRODUCTION

The influence of humans and their culture needs to be explicitly considered in the context of information security, since current and former employees are regarded as one of the root causes of information security incidents (Da Veiga & Martins, 2015b). Therefore, employees need to be made aware of the rules and risks associated with the use of information systems, in order to minimize the risk of incidents.

The definition of a culture found in the Oxford dictionary is: a particular group or society who share the same ideas, customs, and social behavior (OED, 2015). Culture distinguishes members of one category from members of another. The category of people can be a nation, region, or ethnic group, a social class, a work organization, or even a family (Geert Hofstede, 1994). Thus, culture can be defined at national level, or at organizational and group level. National culture differs mostly on the values level, compared to organizational culture where culture is expressed in terms of symbols and rituals.

Culture is considered important in the study of information technology, because national, organizational and group culture can influence the successful implementation of information technology (Leidner & Kayworth, 2006). Hofstede also mentions that the values of a national culture determine the values of an organizational culture (Geert Hofstede, 1994). However, not everyone agrees with Hofstede's statement, and some argue that organizations are able to create unique cultures with their own values independent from the national culture values (Y. Lee & Kramer).

This chapter will elaborate on the notions of national, organizational and information security culture. As this research is conducted in the Netherlands, the Dutch culture is further elaborated on in more detail.

3.2 NATIONAL CULTURE

For a long time, there has been an argument among scholars whether national culture and organizational culture are related. Some scholars argue that organizations develop their own culture that is different from the national culture, in order to make the organization more competitive (Y. Lee & Kramer).

Other scholars state that the organization's culture becomes similar to the national one, in which they are embedded (Nelson & Gopalan, 2003). They claim that the organization founders and dominant elites create and shape an organization based on their national values and assumptions, and that these values are meaningful for their environment. Hofstede's cultural framework is often used to describe the cultural differences between nations and groups. Therefore, this framework will also be used for this research. Hofstede defined five dimensions to distinguish cultures (G. Hofstede, 1983).

POWER DISTANCE

This represents the extent to which less powerful members of a group accept and expect that power is not distributed equally. It represents inequality in societies and that some societies are more unequal than others. Countries with a large power distance, are usually more unequal and there is a hierarchical order that defines a role for everybody. This hierarchical order is often accepted without opposition. On the other hand, countries with a low power distance are characterized by equal distribution of power, where it is also necessary to justify the inequalities of power.

INDIVIDUALISM VS COLLECTIVISM

This is the degree to which individuals are integrated into groups. In countries that are very individualistic, people tend to look after themselves and their immediate family. Countries that are collectivistic are characterized by strong, cohesive groups who continue to protect each other in exchange for unquestioning loyalty.

MASCULINITY VS FEMININITY

A masculine culture is one that is competitive and that strives for achievements, heroism and material rewards for success. A country with a high feminism index is one that prefers cooperation, modesty, caring for the weak and quality of life.

UNCERTAINTY AVOIDANCE

This dimension represents how a society deals with uncertainty and ambiguity; how uncomfortable or comfortable members of a culture feel in unstructured situations. These unstructured situations are unknown, new, surprising and different from the usual situations. Uncertainty avoiding cultures are usually more emotional and try to minimize and avoid uncertain situations. While uncertainty accepting countries try to have few rules as possible and are tolerant to opinions different from their own.

LONG TERM VS SHORT TERM ORIENTATION

Cultures that are long term oriented, focus on the future and value persistence, perseverance, saving and being able to adapt. Short term orientation cultures are focused on the present or past and consider them more important than the future. These cultures value tradition, fulfilling social obligations and the current hierarchy. This dimension illustrates how the different cultures view time and the importance of the past, present and future.

HOFSTEDE'S SCORE FOR THE NETHERLANDS

Each of the five dimensions can be scored from 0 to 100. If a score is under 50, it is considered to be relatively low, while a score above 50 is relatively high. These dimensions distinguish countries and organization from each other. The score for the Netherlands based on Hofstede's cultural model is listed in table 2. From table 2, can be concluded that the Netherlands scores high on individualism and low on masculinity. Individualism and femininity are the key characteristics of the Dutch culture. China, with a score of 20 is a country with low individualism, where people are more trusting towards each other. China does have a high score on power distance of 80 compared to 38 of the Netherlands. The high power distance of China reflects in hierarchies they have in the society and organizations. The Netherlands on the other hand does not have a high power distance where people mostly are able to address each other at their first name independent of the status. Even though each dimension has a score, the outliers define the key characteristic of a countries' culture.

Table 2: Hofstede's score for the Netherlands

Dimension	**Score**
Power Distance	38
Individualism	80
Masculinity	14
Uncertainty avoidance	53
Long term Orientation	67

POWER DISTANCE

The Netherlands scores low on Power distance, which means that the culture is characterized by being independent, equal rights, coaching leader, hierarchy only when necessary, power that is decentralized. In an organization, managers rely on the experience of their team members, and control in organizations is disliked. Employees have an informal attitude towards managers (on first name basis) and the communication between them is direct.

Power distance (PD) also influences the way information security is managed. In a high power-distance country, employees rely on managers to solve work issues because they often have the role of problem-solvers (Shaaban & Conrad, 2013). In these countries employees have less freedom to do what they want, since they have to report almost everything and they are also monitored more than people in lower-power distance countries. In countries with lower power distance, where employees have more freedom, such as the Netherlands, people can make decision or take actions without consulting superiors, which in turn can cause a security violation. In countries with a high PD score detailed instructions on tasks are expected from managers, who also expect that these instructions are followed without questions asked. In the Netherlands, that has a low PD score, employees don not expect detailed instructions, which in turn can lead to knowledge gap on how to deal with certain situations.

INDIVIDUALISM

Based on the high score for this dimension, the Netherlands is considered to be an individualistic society. Individuals are expected to take care of themselves and their immediate families only. In an organization, management is considered as management of individuals and the employer/employee relationship is a contract based on mutual advantage. Hiring and promotion is based on quality of performance only.

Collectivist societies are more trusting towards each other and are therefore more likely to commit information security violations such as password sharing and illegal sharing of copyrighted material (Al-Mukahal & Alshare, 2015). People in individualistic societies are not relying on others and trust their own selves to get things done and solve their own problems rather than relying on others. This can also cause security violations if the individual does not have the required knowledge to solve the problem. However, it could also be said that employees will not execute orders if these are in conflict with the existing security policies. Therefore, it is important to share these policies.

MASCULINITY

As mentioned before, a high score means that the society is competitive and it is driven by achievement and success. A lower scores means that the dominant values are caring for others and for quality of life. In a feminine society quality of life is a sign of success and standing out from the crowd. The Netherlands who has a low score of 14, is a feminine society, here individuals try to have a healthy balance between life and work. A feminine organization is one where a manager tries to support his employees and tries to involve them in decision-making, and where conflicts are resolved by compromise and negotiation. People in masculine culture emphasize goal-achievement attributes more than in feminine societies. Individuals from masculine societies tend to accept activities or support policies that maximize their personal gains and to some degree those of the organization as well (Nemati, 2010). Therefore, it could be argued that masculine countries would be positive towards implementing information and communication technologies and new ideas related to IS security, if these would increase the chance of success (Ifinedo, 2009). However, some authors argue that information technologies promote cooperation at work and better quality of life (characteristics of feminine societies), while countries with high masculinity would also be positive towards implementing new ICT technologies if these would improve chance of success

and support competition (Halpin, 2013). Based on the literature, both feminine and masculine cultures could have a positive impact on information security as one supports cooperation and the other the implementation of new policies and technologies. For an information security culture a combination of both would be ideal, since cooperation between employees is essential as is the willingness to implement and abide to new policies and rules.

UNCERTAINTY AVOIDANCE

A score of 53 for the Netherlands, means that slightly they lean towards uncertainty avoidance. Uncertainty avoidance societies are characterized by precision and punctuality, security is considered important, time is money, and people have an inner urge to be busy and work hard.

This dimension represents the extent to which members of a culture feel threatened to unknown or uncertain situations. Research showed that the Dutch ignore rules if they do not make sense to them (Al-Mukahal & Alshare, 2015). The chance is higher that people from the Netherlands resist change and rules related to the change if they do not feel comfortable with them, which in turn can lead to security violations. Knowledge can be used as a means for controlling and avoiding risks.

In Countries with a high uncertainty-avoidance index, strict polices and regulations are adopted and implemented, in order to avoid unexpected situations. In the US for example, information security managers will tend to not include their people in their security-related decisions, while Swedish managers may care for how their implemented decisions affect their people, and thus involve them in decisions on potential changes in the organizational environment, so favoring local participation.

LONG TERM ORIENTATION

Characteristics of this dimension are persistence, ordering relationships by status, thrift and having a sense of shame. The Netherlands scores above average on this dimension. A lack of long-term orientation can have negative influence on the development and implementation of information security or knowledge management concepts. Employees will not comply with the measures and policies of their organization if they do not feel that the management is convinced that these policies will benefit the organization in the long term (Glaser & Pallas, 2007).In the context of long term orientation sense of shame, and persistence play an important role. Sense of shame is defined as a motivating awareness of ethical responsibility. This attribute is essential for

information security, since if people have a self-motivation to be aware towards the information systems, not much has to be done to change their behavior to comply with the security rules. Persistence can have a positive effect on information security. Being persistent towards the information policies independent of the circumstances, can lead to not overruling policies and in turn prevent unnecessary incidents from happening.

3.3 ORGANIZATIONAL CULTURE

The previous section elaborated on culture at national level, while this section elaborates on organizational culture. Mohelska et al present the following definition, "*an organizational culture is an elusive phenomenon characterizing the quality of the social climate within the organization and determining the dominant work positions of all workers. The status of organizational culture is relatively easy punishable immediately after joining the organization, but the definition of the term is difficult because it represents a phenomenon that appeals more to emotions that rational considerations of an observer"* (Mohelska & Sokolova, 2015). Kilman et al. define organizational culture as "a shared philosophy, ideology, value, assumption, beliefs, hope, behavior and norms that bound an organization together" (Kilman, 1985).

Edgar Schein developed an organizational culture model to make culture more visible within an organization and also to highlight the steps that need to be followed to bring a cultural change. He stated that there are direct and indirect mechanisms within organizations and that the organizational culture model is influenced by direct mechanisms such as behavior, opinions, status and appointments. On the other hand, indirect mechanism such as mission of a company, formal guidelines, corporate identity, rituals and design do not influence organizational culture (Schein, 2006). He divided an organizational culture into three levels artefacts and symbols, espoused values, and assumptions.

ARTEFACTS

These are the visible elements in the organization such as logos, architecture, structure, processes and clothing. It includes everything that one hears, sees, and feels when encountering a group with an unfamiliar culture (Schein, 2006).

ESPOUSED BELIEFS

This category includes standards, values, and rules of conduct. These are values that an organization has that gets a group moving in dealing with internal and external problems. For example, if what a leader proposes works, and continues to work, this method will gradually become a shared standard.

ASSUMPTIONS

This is the deeply embedded behavior that unconsciously constitutes to the organizational culture.

3.4 INFORMATION SECURITY CULTURE

Does organizational culture have an effect on the use of information technology? Studies have proven that an organization's culture can improve the quality and value of information and information services (Sundqvist & Svärd, 2016). This information culture is embedded in the organization's culture, and can be nurtured with training and communication. Another study proved that the values and attitudes towards the information system depend on the organization's culture and that personal attitudes and awareness play a crucial role on how employees perceive information systems (Widén-Wulff, Gunilla, 2000).

Since the major threats to information security are caused by current and previous employees who do not comply with the organizational policies and procedures, an established information security culture can help prevent this from happening. In the previous chapter, we defined an organizational culture as a set of shared values, beliefs, assumptions and practices that guide the employees' attitude and behavior within an organization. Dhillon et al. (1997) define an information security culture as the behavior, values and assumptions that ensure information security. Another definition is, a system in which attitude, motivation, knowledge, and mental models about information security all interact together (Dhillon, Syed, & Pedron, 2016). Thus, an information security culture not only focusses on technical and formal controls, but also on guiding the behavior of employees. A security culture should support all daily activities in such a way that security becomes natural to all employees (Lim, Chang, Maynard, Ahmad, 2009).

SECURITY CULTURE, AWARENESS AND TRAINING

Researchers claim that an information security culture can contribute to minimizing the undesirable behavior of employees (Da Veiga & Martins, 2015b). It can help minimize risks from

employees such as wrongful disclosure of confidential information, unauthorized transfer of information to third parties, and saving sensitive information to unencrypted devices. An information security culture is considered as an effective solution to dealing with the human aspect, since it consist of various information security controls (e.g. awareness, training and monitoring) that must be implemented to change employees behavior (da Veiga & Martins, 2015a)

Information security awareness and training are important elements of an information security culture (Taylor, 2013). By making security mandatory for all employees, they get the message that the organization is serious about security. Security awareness and training are not the same thing. Security awareness refers to the marketing and promotion of security inside the organization such posters, e-mail reminders which are motivational by nature. Security training is an actual security course that takes place in a classroom or online with the purpose to teach the employees how the systems are used and should be operated in a secure way. The training of employees empowers them to demonstrate security compliant behavior (Taylor, 2013).

3.5 SUMMARY

Culture is defined as a group with shared beliefs, and values either on a national or group level. Some scholars believe that organizational culture is related to national culture, while others claim the opposite. This relation between these two will be verified in the next chapter. However, there is an agreement on the fact that information security culture is important for ensuring security in the organization. A good information security culture not only focusses on technical and formal controls, but also on guiding the behavior of employees and supporting all daily activities in such a way, that security becomes natural to all employees.

CHAPTER 4 INTERVIEWS: RESULTS & ANALYSIS

4.1 INTRODUCTION

To obtain a richer understanding of the effect of culture on information security, five interviews were conducted with five experts of IT companies. They were all experienced individuals working with information technologies on a regular basis over a period 3-15 years. Of the five respondents, one was a security specialist, two were information consultants, one worked as the head of a department of industrial systems, and one was the director of an industrial company. Four of these respondents had the Dutch nationality, while one had a Surinamese nationality, but has been living in the Netherlands for almost 15 years. All of the companies were located in the Netherlands, and were chosen based on the criteria that they supply services to clients and have information systems on which confidential information in stored. Four of the interviews were carried out face-to-face, while one was carried out over Skype. The interviews lasted for approximately 45 minutes and were audio-recorded. The main objective of the interviews was to understand the effect of national culture on information security, but also to identify what measures these companies have implemented.

To measure the effect of culture on information security, a set of questions were formulated that form the basis for the interview. Hofstede's dimensions overlap each other, so one question can be linked to multiple dimensions. For example, as stated in Chapter 4, people in masculine countries are willing to follow rules if they make them more competitive and give them an advantage. This is also a characteristic of collectivism, as people consider the organization as a home, which they want to protect. Also the decision-making process regarding the implementation of policies can provide information for two dimensions. In feminine societies new policies are implemented with the consensus of employees. Employees' opinions are considered in the decision-making process. This is also a characteristic of countries with a low power distance, as in such societies opinions are considered. However, in societies with a high power distance, the employees have to accept the decisions made by their superiors. Table 3 lists all the metrics used to assess the dimensions of the Hofstede model.

Table 3: Dimension and relevant metric

Dimension	**Metric**
Power distance	Hierarchy Manager uses authority to implement policies Employees take part in decision-making process
Individualism – Collectivism	Willingness to help each other Willingness to follow rules What violations occur most
Masculinity – Femininity	Policies implemented through consensus How actively are rules followed Cooperation for maintaining security
Uncertainty avoidance	Written Policy Strict policies and procedures Awareness programs
Long term Orientation	Sense of shame Persistence

4.2 SUMMARY OF INTERVIEWS

COMPANY 1

The company provides software solutions, IT and business outsourcing services and has around 5000 employees distributed in Europe. The company, which was founded in the Netherlands, consist of a formal hierarchy with clearly defined roles. Each team has a team leader, who has to

report to the respective manager. Even though, there is a formal hierarchy defined for the departments in the Netherlands, the employees have a personal relationship with the team leaders and managers. It is possible to speak to them on a daily basis and is not necessary to address them in a formal way. Furthermore, it is also possible to disagree with a solution proposed by the team leader or manager.

The company has a security team, which is divided into two divisions. One is responsible for securing the data of the products they deliver to clients, while the other is responsible for handling internal security. The internal security team handles the password and username requirements and change policy, monitoring of the network, access within the organization to specific rooms and guest access. The password policy requires employees to change their passwords every month. Furthermore, it is prohibited to connect personal devices such as phones and laptops to the company's network.

The respondent has been working for three years at the organization and develops software solution for the clients of his employer. Security standards are defined for the software solutions they deliver. In the organization, the respondent only received a security training about the security standards and other standards for the products they deliver. The organization does not provide security training for dealing with the internal information systems.

The question was asked if there are written rules and security policies. The respondent answered that there probably is one, but that he has not read it. Most of the policies are transferred by word of mouth from the team leaders. However, there are some unwritten rules and procedures that they must follow. For example, they always have to logout of the system before they leave their workspace and it is not allowed to bring guests in the organization without notifying the receptionist.

In the organization, it often occurs that employees, especially new ones, leave their workstation open without logging out. Even though, there is an automatic logout after a few minutes, the colleagues turn the monitor so that the employee in question knows that he did not log out. These are not rules from the top of the organization, but rather the employees looking after each other.

COMPANY 2

Company 2 designs and provides specialized imaging technology products for their clients and is located in different countries in Europe with a staff of more than 250 people. The headquarters is in Germany. The respondent is working in the sales department which consists of 7 people. It is a small department where everyone reports to the director. Several servers located onsite contain clients' information. There is no local security team available and the rules and security controls are managed from Germany. The respondent believes that national culture influences information security and states that the information security is stricter in Germany than in the Netherlands. He believes that Germans follow more procedures and rules without any problems. On the other hand, Dutch are more open and do not like following rules if they are not perceived as necessary.

There is no dedicated security team, since it is a small department and there are also no security rules and policies within the organization. Some employees within the company sign NDAs with their specific clients, but the information often is still shared with other employees. It is perceived that people have their own responsibility and should know what is good and what they are allowed to do. He states that there is no strict control such as monitoring of employees, but that there is an informal social control on each other. The company also has a password policy, but contrary to Company 1, employees are required to change the password on a yearly basis.

COMPANY 3

This company is active in the IT sector, and delivers IT solutions for their clients' specific business cases. The company is only active in the Netherlands and has 180 employees. There is a hierarchy on paper, but just as with the previous companies, it is just a formal hierarchy and everybody has the same relationship with each other, independent of the status.

The company has a security department consisting of two persons, who are responsible for transferring the standards and policy rules to the employees regarding the clients' products and also regarding the internal security. They have servers on site on which the clients' information is stored. They also provide services to the military defense in the Netherlands. Only people who are working on projects for the military defense, undergo extensive screening by the organization and are required to sign NDA's among other official documents. People entering the server rooms also must be accompanied by someone else. Other employees are not screened before they are hired.

The company tries to avoid having too many rules and too much monitoring of employees. Just as the previous companies, the respondent said that the Dutch do not like rules, especially if they do not see the purpose behind them. Furthermore, monitoring of employees would irritate them and would not urge them to be more secure with the information systems. The respondent states that the best way to change behavior is not by having rules, but rather by motivating the employees and giving them a certain responsibility towards the information systems.

The respondent said that even though everyone knows that security is important, no one really considers following all the rules and guidelines of the organization. He stated that sometimes, people send sensitive information via email even though it is forbidden to do so. He explains that people have a huge responsibility and freedom in the company, without being monitored the whole time, so they should decide what is acceptable to send via email. Employees misuse the freedom they have and not always choose the safest solution to prevent a problem. On the other hand, he believes that not everyone may know what is acceptable to be sent via email.

The company also has a password change policy of 6 months, but there is no measure to prevent employees from using passwords with a sequence (for example, employees sometimes have a fixed part in their password and only change the month/year after he fixed part). Employees are reminded to change their username and password as the deadline arrives.

COMPANY 4

The organization develops and provides intelligent automation technology for their clients. It is a company that originated from Germany and later expanded to the Netherlands and other countries in Europe. Just like the previous companies, there is a hierarchy in the company, but everyone is considered important. The company does not have a security team and information restriction is organized by the human resource department. Furthermore, they receive their rather strict policies and rules from the headquarters in Germany. The interviewee stated the Dutch take actions and later think about the consequences, while the Germans follow a procedure, in which the manager has to agree before a decision can be taken. The managers and team leaders in the Netherlands function more as a coach rather than as a boss. Their aim is to make the employees independent and coach them to make the right decisions on their own.

There is a password policy that requires employees to change their password and username once a month, which is maintained by the headquarters in Germany. Furthermore, a 2-factor authentication is required to access the computers.

The employees do not receive information from clients whom they are not working with. If the clients' requires it, NDA's are signed. There are no written policy rules, but employees receive an instruction video with rules that they are expected to observe. As in the previous companies, employees verbally receive rules that are expected from them and they get a certain responsibility. The company expects and hopes that the employees will not misuse this responsibility and leak information.

COMPANY 5

The company develops and supplies IT services for other organizations in, e.g., healthcare. At this moment, around 10 employees are working at the company, but it has many subsidiaries in the Netherlands. People are trained at the company and when they reach a certain level of skills, they are transferred to one of the subsidiaries. The company has a management team consisting of CEO, CTO, CFO, operation manager and the lower level consisting of the employees. Just as the previous organizations, the structure is informal and everyone has daily contact with each other. Neither the company nor their subsidiaries have a dedicated security team.

Important decisions are taken by the management team and then delivered to the employees. If the majority of the employees disagree with the decision, the management team considers it, and revises the decision, if possible.

In each of the subsidiaries, there are servers located, but one person manages them. Except encryption on the servers, no other security measures are implemented. The respondent stated that it is possible that someone might walk in and delete some services or data. Employees are also not screened before they are hired, but the respondent beliefs that this is important. He was not satisfied with the security in the organization, but believes that it is not yet perceived as necessary. He believes that when the number of clients increases and more data is stored, more measures will be implemented to protect the data.

The respondent thinks that there is a relation between culture and the way people interact with information systems. He stated that when working on an international project, he noticed that

people from the southern part of Europe followed more procedures, while people in the Netherlands like to think out of the box.

There is no device policy concerning connection to the wireless network, meaning that employees are allowed to connect with their own device on the wireless network and employees are also allowed to store sensitive data on their laptops, which they can take home.

There is a written policy stating the terms and conditions of the services the company delivers to their clients. This is a policy between the company as a whole and their clients, not a policy for its employees. The company does not have a business continuity plan and believes that an incident can cause a serious damage to the services they deliver and to the organization's image. He states that there is no policy and does not know what to do if an incident occurs.

The respondent also said that the security is lacking and that it can be improved by having policies with guidelines to improve employee awareness towards the information systems. However, the policy should not be framed as procedures and rules for employees that restrict them from thinking out of the box. The respondent said: *"You don't want to formulate it as do this or do that, but rather as look out for this and look out for that".*

4.3 RISK MANAGEMENT MEASURES IMPLEMENTED IN THE COMPANIES

PEOPLE & ORGANIZATION MANAGEMENT

Companies implement these measures to help their employees. One such measure is a written policy. Although the respondents believe that a written policy consisting of the rules and regulations is available at their company, they do not know what it contains and never speak about it or consider it.

Another crucial factor in information security, is security awareness training. However, in none of the companies the respondent received a security training. They merely received a training on how to fulfil their tasks and within this training, a security rule was mentioned.

Furthermore, it is also important to screen the employees who are hired in the organization, especially in organizations where sensitive information is stored. However, the companies interviewed do not screen their employees; only in Company 2 employees who work for the military defense department were screened. When the respondents were asked why they did not

screen their future employees, they stated that they did not know, but they thought that it should be considered in the future

COMMUNICATION INFRASTRUCTURE

Network security consist of the measures that are implemented to secure the network. Based on the interview, each of the companies' network was protected with an anti-virus and firewall. Company 1, 3, 4 and 5 also had a separated guest network, while company 2 did not. However, it is part of a larger organization and not having a separate guest network makes it easier to access the parent organization, since they have a common network. The employees at that location were also allowed to access the network with their private devices, while this was forbidden in the other companies. It is important that private devices are separated from the main network, because these devices usually do not have the same protection as the companies' workstations and servers. Consequently, if such a device is compromised and connects to the main network, it can also compromise the organization's network.

In all of the five companies, employees received a work laptop and phone, which they were allowed to take home. However, in Company 1 and 4 it was forbidden to store companies' sensitive data on the laptop. If they wanted to access the data from outside the company, they needed to connect through a VPN to access the data. In Company 3, the employees were allowed to store on the device data from the project they are working on. Thus if the device was stolen the data would also be compromised.

Furthermore, in each of the companies, no data was stored on the computers there. Instead, they had to sign in and their respective virtual workspace was loaded on their computer

Finally, no websites are blocked from visiting. In Suriname for example, employees at work are not able to access some websites such as torrent sites or Facebook, among others. These sites are blocked. However, none of the companies interviewed prevents their employees from visiting certain websites. The respondents were asked if it is not safer to do so, and they replied that it is, but the Dutch don't like to be controlled and monitored. Again, it is perceived as a better solution to give the employees the responsibility to decide what is good and what is not.

PHYSICAL SECURITY

Beside network security, it is also important to monitor who enters the building and especially the server rooms. People should be prevented from causing damage to the building, employees and also to the information systems. Except Company 3, the companies had physical measures implemented. Guest are restricted to the waiting rooms until they are picked up. The employees have a visible identification card that grants them access to certain areas. Each guest also receives a visible card with limited access. The buildings have cameras and alarms installed.

4.4 ANALYZING THE RELATION BETWEEN NATIONAL AND ORGANIZATIONAL CULTURE

The scholars who claim that national culture does have an impact on organizational culture, explain this by the fact that individuals are exposed to the social values and norms from their birth. The individuals learn these values and norms, which are then reinforced in the organization where they work (Y. Lee & Kramer). They are also enforced by the managers through training, monitoring, and other socialization processes. Another empirical study proved that people from different nations have different work-related cultures and different attitudes, or reaction to the same situation or set of controls (Chow, Kato, & Merchant, 1996). In this section the relation between national and organizational culture is verified based on the interviews.

POWER DISTANCE

The Dutch culture scores low on power distance, which is characterized by the lack of hierarchy. This was also concluded from the interviews. Each of the companies has a hierarchical structure consisting of a director, manager, team leader and employees. However, this hierarchical structure can be considered as a job description, since everyone has their own responsibility and freedom and can make certain decisions without consulting with their superiors. Almost all of the respondents compared the Dutch culture with the German culture, where the hierarchy is not just used to define roles. Based on the responses of the interviewees, in Germany it is required to consult the superior before taking decisions. The superiors in the Netherlands are considered as coaches, who teach their employees to be independent, self-conscious and give them a lot of responsibility and freedom for performing their tasks.

INDIVIDUALISM

Based on the interviews, the conclusion concerning the individualism and uncertainty avoidance was different from Hofstede's model. Consider first the individualism dimension, which ranks the Netherlands as an individualistic culture. This dimensions states that an organization management is considered as management of individuals and the employer/employee relationship is a contract based on mutual advantage. However, from the interviews it can be concluded that the management is not merely management of individuals, but rather of a team whose members are mutual dependent on each other. Many of the respondent also claim that there really is a family-like culture in their organization, where the employees look after each other. An example to illustrate this is when employees leave their workstation signed on to have a coffee break, the other employees close their desktop and turn it around to prevent others from misusing it and to create aware behavior from the respective employee. They do this to protect their colleagues, even though they are not obliged to do so. It was expected that within the organizations everyone would look after themselves and thus not really be concerned with other employees. However, a family like culture was visible within the organizations.

FEMINISM

This dimension has different interpretations, one of which is the role distribution between men and woman in the culture. The Netherlands scores low on this dimension, which means that men and woman share equal roles. The other interpretation is that a feminine organization is one where the managers support their employees and strive to involve them in decision-making, and where conflicts are resolved by compromise and negotiation. This can be concluded as valid from the interviews, since everyone's opinion is considered when new methods are going to be implemented.

UNCERTAINTY AVOIDANCE

The Netherlands scores just above average on this dimension, which is characterized by having written rules and regulations to which people must comply. By having written rules and procedures, people know how to act in uncertain situations. However, from the interviews it can be concluded that the Dutch culture does not prefer written rules and procedures if people do not see the benefit of them. One of the respondent stated that rules are necessary, but it is not necessary to have rules and procedures for everything. Another respondent stated that having to many rules

within an organization creates an atmosphere like a police state within the organization, which works in Germany but not in the Netherlands. There are some verbal rules and instructions provided in the organizations, especially when one starts working. However, the employees are coached and given a lot of responsibility towards their clients, information systems and in making decisions. They only sign NDA's in exceptional cases and it is expected that everyone has a moral responsibility and knows the difference between right and wrong and thus makes correct decisions and does not misuse the systems.

The uncertainty avoidance score of 53, also means that there is a higher chance that people from the Netherlands resist change if they do not feel comfortable with it. In the interview a few of the respondents mentioned that the Dutch will not follow rules and procedures if they do not understand the benefit of the rules. If they perceive the rules as unnecessary, they will not comply with them. Many of the respondent stated that the Germans had more procedures and rules, and were stricter than the Dutch companies. Having more procedures and rules, and being stricter can be derived from the uncertainty avoidance dimension. Germany has a score of 65, while the Netherlands a score of 53 on the uncertainty dimension. Thus, an increase of merely twelve has a noticeable effect on how people comply with procedures and rules.

CONCLUSION

It can be concluded that there is a relation between national and organizational culture. As mentioned in Chapter 3, there are scholars who believe that there is a relation between national and organizational culture, while others state the opposite. The scholars who claim that there is no relation between the two, say that organizations develop their own culture to make them competitive with other organizations. The competitiveness can be dependent on the organization's structure, strategies and objectives. But the core values to reach those strategies are still dependent on national culture. The respondents of the interview also stated that they experienced clear differences between countries in the way that the deal with a problem. One of the respondents stated that he experienced that people from countries in the Southern part of Europe follow more rules and procedures. France and Spain are two countries in that region and both score 86 on Hofstede's uncertainty avoidance dimension. Thus, national cultural differences influence the way people operate in organizations.

4.5 INFLUENCE OF CULTURE ON INFORMATION SECURITY

From the interviews it can be concluded that information security culture is influenced by the national culture. Most of the people that were interviewed were part of an organization that also had subsidiaries in Germany. Even though they were the same organization, they did not have the same policy and measures implemented. This does not refer to the technical measures, but the organizational measures. The companies in Germany had more rules and procedures, compared to the Dutch culture where people are coached to make their own decisions not dependent on a procedure.

POWER DISTANCE

Employees involvement is considered as one of the important values for creating an effective security culture (von Solms & von Solms, 2004). The employees should be considered in the decision-making process when the security rules will be established. If this is not the case, employees might feel forced to follow certain rules without understanding or agreeing with them. The Netherlands has a low power distance and from the interviews it was concluded that the employees' opinions are considered. Thus, the low power distance can be considered as a positive factor in establishing an effective information security culture.

FEMININITY

Cooperation is required for maintaining a secure organization. The Dutch culture, a feminine society, promotes cooperation. This could also be concluded from the interviews, as the respondents stated that employees could take part in the decision-making process for implementing new policies and technologies. The employees also helped new employees in making them feel comfortable and teaching them what the procedures are for performing their tasks. Thus, the feminine score of the Netherlands has a positive effect on information security.

INDIVIDUALISM

Based on Hofstede's dimension, in individualistic cultures people act in their own interest rather than in the group's interest. In collectivistic cultures, people value the group's achievements above the individual ones. The negative consequence of an individualistic nature on information security, is that people might ignore and not act if they see a colleague not living up to the security rules. They can do this, since an incident may affect the organization as a whole and not on an individual

level. On the other hand, people in strongly collectivistic culture, people share passwords and confidential information with their colleagues, since they might consider them as family. So both cultures within this dimension may have negative consequences on information security. However, from the interviews it was concluded that even though the Netherlands is an individualistic culture, they still try to create a collectivistic culture in the organization. They do this, by organizing events where colleagues can bond in an informal setting, especially people from the same department. In the organization, the performances are measured per department. Thus if an employee of one department makes a mistake, his colleagues within the same department try to help him in order to save the image of that department. If an incident occurs, the whole department will be held accountable for it. This led to employees watching over each other, stimulating each other to be aware of the information systems security and to comply with the rules. Thus, it can be a contributing factor to create relatively small teams/departments, where people are stimulated to look after each other to keep up the image of the team as a whole.

UNCERTAINTY AVOIDANCE

The score for this dimension is 53 for the Netherlands. This means that people in the Netherlands lean towards an uncertainty avoidance culture. This can have a negative effect on information security, as information security requires employees to follow certain rules and procedures to minimize risks. However, we concluded from the interviews, that is not something the Dutch prefer. One of the interview respondents stated that when employees are busy with a certain task (writing and important email, etc.) and encounter a security threat on their workstation, they neglect it in order to finish their task. Thus, the task they are performing has a higher priority than the security threat. This requires the security specialist to intervene before the threat can cause a serious damage. The consequence of the threat can be seen as an uncertain situation, since it is not clear what damage it can cause. One would therefore expect that the 'uncertainty avoidance factor' of the Dutch culture would lead to the respective person to stop his task and take the necessary precautions to mitigate the threat.

Cultures with a high uncertainty avoidance score, are less willing to take risks and to accept organizational change. Every change has to be incremental, and not a complete radical change. Hofstede, states that people in these cultures have anxiety and rely on experts to deal with the uncertain situations and that these cultures need rules and procedures to feel safe and secure.

However, based on the interviews, companies in the Netherlands stimulate individuals to make their own decisions and gave them a lot of responsibility, without having written rules and procedures. Not having clear rules can sometimes lead to people not knowing how to act in certain situations. The interviewee states that the Dutch do not like to follow unnecessary rules and to be monitored constantly. However, security is a topic that needs more rules and procedures to act as a guideline and constant reminder for employees on maintaining aware behavior.

LONG TERM ORIENTATION

The Netherlands sores above average on this dimensions, which is characterized by persistence, having a sense of shame. From the literature review, we found that employees of an organization will not comply with the measures and policies if they do not feel that the management is convinced that these policies will benefit the organization in the long term (Glaser & Pallas, 2007). As we concluded from the interviews, the Dutch do not follow rules if they do not make sense to them, thus if they do not see the benefit of the rules and policies.

Another characteristic of long term orientation is persistence. It was expected that the Dutch would be persistent in following the rules independently of the situation. However, from the information obtained from the interviews, we saw that people often neglect the security rules in order to finish a certain task, even if there is a possible threat. It can be said that they are persistent in finishing the task they are busy with, but at the expense of security, which should have a higher priority.

Finally, sense of shame is defined as a motivating awareness of ethical responsibility. This characteristic could not be completely seen from the interviews. Based on the score, which is 67, one would expect that the employees would be more aware towards the information systems. However, many employees often neglected rules, such as logging off, sharing confidential information, and continuing work on a task when there is a possible threat. Also two of the interviewees, mentioned that previous employees still tried to access and copy information from the organization they worked at. Thus, it looks more like unaware behavior than aware behavior towards information security.

4.6 SUMMARY

Table 13, contains a summary of the dimensions with their characteristics and respective implication on information security. Not all characteristics of the dimension are summarized, but only those applicable in the Netherlands based on the interview results.

Table 4:Summary of dimensions and the implications on information security

Dimension and characteristic	**Implication on information security**
Power distance	
No real hierarchy	More responsibility and freedom to perform tasks. Employees can make decisions without consulting superiors. Some of these decisions may affect the systems negatively.
No detailed instructions expected from superiors	Employees may not know the safest way to perform certain tasks, which may lead possible risks in the information system.
Employees opinions valued	Employees' opinions are considered in the decision-making process for implementing new rules and technologies. By considering their opinion, they are more likely to comply with the rules and not neglect them.
Individualism	
Own interest above group interest	Not giving opinions to managers about possible bottlenecks in the system concerning security.

	Neglecting security rules to finish certain tasks. Not reporting security incidents. Using company's information for own profit.
Femininity	
Cooperation valued	Looking after each other to comply with security standards. Working as a team to improve security.
Employees involved in decision-making	More willingness to comply with security rules.
Uncertainty avoidance	
No written policies and procedures	Not having a guideline with the security standards and rules to follow, could lead to unnecessary incidents.
Willingness to take risks	Taking risks, such as accessing certain prohibited websites, or saving confidential information on unencrypted devices, can cause incidents which are easily avoidable.
Long term Orientation	
Persistence	Can be positive or negative, depending per person. Some person can be persistent in complying with the security rules, while

	others persistent in finishing a task even if there is a possible risk.
Sense of shame/awareness of ethical responsibility	By having a sense shame, people can think of the consequences of a violation and thus try have aware behavior towards the information systems.
Benefit of rules/ measure needs to be stated	The future benefit of rules and measures need to be stated and made understandable for everyone, so that they are more willing to comply with them.

CHAPTER 5 SURVEY: RESULTS & ANALYSIS

5.1 INTRODUCTION

An online survey was developed to evaluate whether the conclusion of the interviews, namely that culture influences information security, is also applicable to other companies in the Netherlands. The survey also collected information on the technical measures that have been implemented, in order to get insight on the state of information security in the Netherlands.

The survey questionnaire consisted of a short introduction followed by the questions. These questions were developed based on the information found in the literature review. They were split into four categories namely Network security, Physical security, Organization Management and Risk Management. To maximize the response rate, a letter containing the link of the questionnaire enclosed in a TU Delft envelope, was sent to the companies. Using a TU Delft envelope, should increase the trustworthiness of the questionnaire. The data of the questionnaire was analyzed using the statistical analysis tool SPSS.

5.1.1 TARGET POPULATION

ICT technologies can be applied in many sectors ranging from pure ICT companies to healthcare and other industries. The ICT applications may differ per sector, but they have in common that computers are connected to some kind of network through which they can be controlled and monitored. Almost all, if not all, companies in the Netherlands make use of the internet. In this chapter, the most targeted sectors from the point of view of intrusion are listed, based on a research conducted by Sing (Singh, Gupta, & Ojha, 2014). Figure 11 presents the percentage of companies within a sector that have been victim of an intrusion

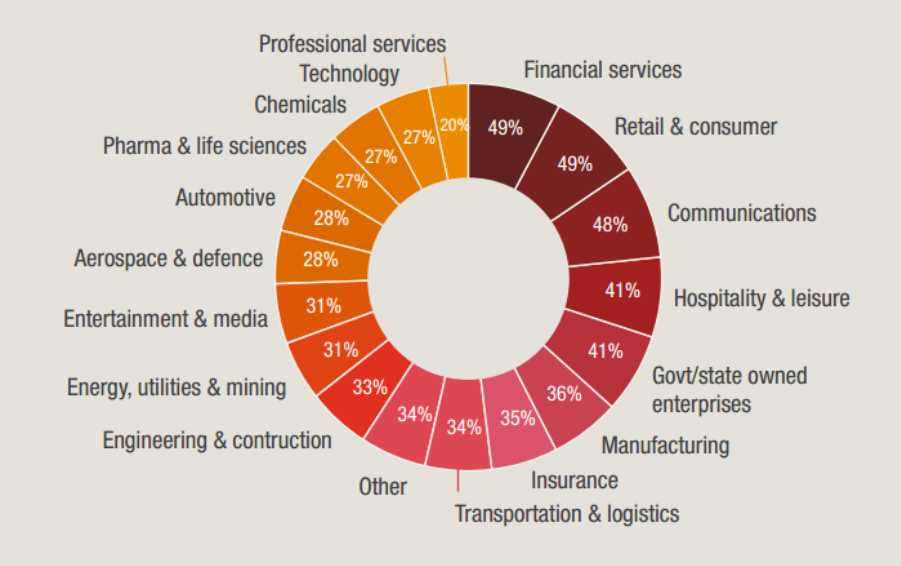

Figure 10: Percentage of intrusion per economic sector. Adopted from, "Economic Crime. What you need to know". Retrieved from http://www.pwc.com/gx/en/economic-crime-survey/.

BANKING AND FINANCE

Financial institutions and their customers are often victims of targeted cyberattacks. One of the main issues here is to identity fraud connected to online banking. The new mobile payment services represent a new exploitable possibility for attackers.

TRANSPORTATION AND LOGISTICS

The processes in the supply chain of this sector are often targeted to disrupt the business continuity. The supply chain is controlled by a software which serves as a gate for attacks, usually DOS attacks. Beside disruption of the supply chain, the data containing the goods that are being stored is often also compromised.

ENERGY

The energy sector is becoming more automated which provides cost and performance benefits with the use of IT. However, the power grid automation network faces security risks because the systems and applications in the network were not originally designed for an IT environment (Wei, 2010). This weak points can be exploited by attackers with a financial or political agenda by intruding the network. Especially nuclear power plants seem to be a desirable target for attackers. In 2003, a computer network server of the Ohio's Davis Besse nuclear power plant was infected with a worm, what prevented the Safety Parameter Display System from working (Kim, 2014).

HEALTHCARE

The use of ICT processes in healthcare is also increasing as well as in insurance companies. Networks are often compromised to access the patients' data records in order steal their financial information such as their bank account information.

ICT SERVICES

The ICT sector, especially those who offer cloud services and databanks are targeted by attackers to steal confidential information.

MILITARY/DEFENSE

"Digital weapons work…they don't put forces in harm's way, produce less collateral damage, can be deployed stealthily, and are dirt cheap. (They have) changed global military strategy in the 21st century" – Ralph Langner. Cyber espionage by military organizations has been incorporated as key factor in military operations targeting other military organizations from other countries. China and the United States among other countries have specialized departments for conducting cyber war (Clarke & Knake, 2011).

5.1.2 DESCRIPTIVE STATISTICS

The target group were Dutch companies operating in the sectors IT, Accountancy, Assurance, Electronics, Energy, Production, and Logistics. The military and defense sector was not included. Companies of different sizes were purposely contacted to be able to differentiate between them. About 1180 companies were contacted to participate in the survey with approximately 130 companies per sector. The responses were disappointingly low at only at a maximum 35, with a response rate less than 5 %. The questionnaire was not answered consistently and the responses per variable differed for the dataset. For example, only 28 respondents stated in which sector their company was, while only 28 stated the company size. The low response rate, limits the possibilities to perform certain tests. Due to the big difference in the number responses between sectors, it is not possible to differentiate between them in order to draw conclusions on cultural differences between sectors.

Table 3 shows that only 27 of the 35 respondents stated in which sector they are.

Table 5: Sample distribution based on sector

Sector	**Frequency**	**Percent**
IT	12	34.4
Accountancy	4	11.4
Assurance	2	5.7
Electronics	3	8.6
Energy	2	5.7
Production	2	5.7
Logistics	2	5.7

Table 4 presents the distribution of the data set based on company size. The company size is categorized according to the definition by the European Commission based on number of employees:

- Large: >251
- Medium: <250
- Small: <50

Table 6: Sample distribution based on company sizes

Size	**Frequency**	**Percent**
Small	23	65.7
Medium	4	11.4
Large	1	1

COMPANIES WHO HAVE BEEN A VICTIM OF AN INTRUSION

The small size of the data set makes it impossible to differentiate between company sizes, therefore the dataset will be combined in order to find significant results. The first variable that will be looked at is the variable intrusion victim, indicating whether a company has been a victim of an intrusion. The results presented in Table 5 illustrate that the majority of the companies have not been a victim of an intrusion.

Table 7: Companies that have been a victim of intrusions

Intrusions victim	Frequency
Yes	20
No	13

5.1.3 REPRESENTATIVENESS TEST OF COMPANY SIZES

The majority of the companies are small, so this is expected to be the case in this sample as well. To test the representativeness of the sample against the figures from MKB Nederland, the chi-square test was used.

The distribution of the company sizes was analysed by 'MKB Nederland' on a population of 1,247,555 active companies ("De staat van het mkb",2015). The results were:

- Independent business (1 person): 70%
- 2-10 employees: 25%
- 10-50 employees: 4%
- 50-250 employees: 0.8%
- >250 employees: 0.2%

In this research, the population was separated in three sizes namely small, medium and large with small being less than 50 employees. Therefore, the first 3 groups as defined by MKB, were combined together to perform the tests. The expected percentage was used to calculate the expected values of the population who were asked to participate in the survey. The result can be found in Table 6, while the results of the chi-square test are presented in Table 7.

Table 8: Observed and Expected Values of the Variable Size

Size	**Observed Value (person)**	**Expected Value (person)**	**Observed Percentage (%)**	**Expected Percentage (%)**
Small (<= 50)	23	1,168	82.14	99
Medium (<=250)	4	9	14.28	0.8
Large (>250)	1	3	3.57	0.2

"MKB Cijfers, definities en organisaties belangrijk voor marktonderzoek". Retrieved from http://www.mkbservicedesk.nl/569/informatie-over-midden-kleinbedrijf-nederland.htm

The Chi-square was performed with the observed and expected values from Table 3. The hypotheses are:

H_0: There is no significant difference between the observed and hypothesized value

H_1: There is a significant difference between these values.

The test returned a significance value smaller than α (0.05), therefore the null hypothesis needs to be rejected. This confirms that there is a significant difference between the observed and expected percentages. This means that the distribution of the sample size is not representative of the target population, which means that the results related to company sizes cannot be generalized. The composition of the responses could have been influenced by the selection of the companies that the letters were sent to.

Table 9: Observed and Expected Values of the Variable Size

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The categories of Size occur with the specified probabilities.	One-Sample Chi-Square Test	.000	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

5.2 ANALYSING EXPECTATIONS

In this section, the descriptive statistics for the variables intrusion victim, written policy, actively spoken about security and level of concern, are listed in tables. These variables are chosen since they have a correlation with the uncertainty avoidance dimension. The lack of the data made it impossible to study the analyse the other cultural dimensions.

EXPECTATION 1: COMPANIES WILL HAVE A WRITTEN POLICY

A written policy is an important element of an information security culture, since it provides all the guidelines, roles and responsibilities for employees. Having a written policy provides employees knowledge on how to deal with uncertain situations. Based on the interview results, we concluded that none of the interviewed companies had a written security policy. However, it was still expected that the majority of the companies would have a written policy, based on the score of 53 on the uncertainty avoidance dimension. But as can be concluded in table 8, the majority of the companies do not have a written policy.

Table 10: Number of companies that have a written policy

		Size			
		Small	Medium	Large	Total
WrittenPolicy	No	12	2	0	14
	Yes	3	2	1	6
Total		15	4	1	20

EXPECTATION 2: COMPANIES WILL GIVE SECURITY TRAINING TO THEIR EMPLOYEES

Security training to increase employees awareness is another critical element of an information security culture (da Veiga & Martins, 2015a). Security trainings are meant to make employees more aware, increase their compliant behavior, and give them knowledge how to deal with uncertain situations. It was expected that the majority of the companies would give security trainings as the Dutch culture is a risk avoiding one. However, from Table 9 can be concluded that the majority of the companies do not give security training.

Table 11: Distribution of security training based on company size

Size vs Security training

Count

		Size			
		Small	Medium	Large	Total
Security_training	No	9	2	0	11
	Once	3	1	1	5
	Regularly	1	0	0	1
Total		13	3	1	17

EXPECTATION 3: THE MAJORITY OF THE COMPANIES ARE VERY CONCERNED ABOUT SECURITY INCIDENTS

It was expected that the majority of the companies would be very concerned about security incidents, since not being concerned and not openly speaking about it in the organization can lead to careless behavior of employees as they do not understand the severity of their actions (Puhakainen & Siponen, 2010). As intrusions are uncertain situations, it is expected that people will be concerned about these situations. The results shown in Table 10 also confirms this expectation, as 18 of the respondent seem to be concerned about it. Uncertainty accepting culture may be less concerned than uncertainty avoiding culture, since they feel at ease in uncertain situations and thus may be less concerned about them.

Table 12: Size vs level of security concern

		Size			
		Small	Medium	3.00	Total
Concern	Somewhat concerned	18	3	1	22
	very concerned	5	1	0	6
Total		23	4	1	28

5.3 TECHNICAL MEASURES IN THE COMPANIES

Table 10 lists the measures that are implemented in companies in the Netherlands. These are measures to protect the information systems as well as the environment. The left column contains the measure, while the right columns contain the numbers of companies that have implement the measure. In the data set not all questions were answered consistently. For example, looking at the variable data encryption, of the 23 companies that answered this question, 6 had data encryption as a security measure and the rest not. As can be seen further, only 6 companies answered the question about a separated guest network.

Table 13: Summary of measures that are implemented in companies in the Netherlands.

Measure	**Implemented /Sample size per variable**
Antivirus	
Data encryption	6/23
Username/Password required to login	23
Password change policy	16/25
Separated guest network	5/6
Multi-factor authentication	3/25
Information classification	7/7
Security training	6/17

Business continuity plan	5/14
Business trip security policy	6/9
Physical security	10
4-eyeprinciple for certain rooms	
Security team	7/8
Employee screening	5/8

5.4 SUMMARY

From both, the survey and interview results it can be concluded that the companies do not have a written security policy. It was expected that the opposite would be true, because the Netherlands scores above average on uncertainty avoidance which is characterized by having more written rules and procedures to deal with uncertainties. However, people in the Netherlands do not like rules and procedures for performing their tasks as they limit them in thinking out of the box, which might explain why they have no written policy. However, security rules are important as they guide employees' behavior and make them aware of what they are allowed to do. Furthermore, the majority of the companies are not really concerned with information security incidents and do not actively speak about it in the organization. This could be the effect of employees not being aware of information security incidents. Many of the companies did have a password change policy, but did not see the necessity of changing the password so often. Thus, it can be concluded that the level of awareness of employees is low, which can also be caused by the lack of awareness trainings given by companies.

CHAPTER 6 DESIGN AND EVALUATION OF THE CULTURAL FRAMEWORK

6.1 DESIGNING THE CULTURAL FRAMEWORK

One of the goals of this research is to establish an information security framework as a cohesive mechanism binding people and technical measures. Edgar Schein developed an organizational culture model to make culture more visible within an organization and also what steps need to be followed to bring a cultural change. He stated that there are direct and indirect mechanisms within organizations and that the organizational culture model is influenced by direct mechanisms such as behavior, opinions, status and appointments. On the other hand, indirect mechanisms such as mission of a company, formal guidelines, corporate identity, rituals and design do not influence organizational culture (Schein, 2006).

Thus, we know that the national culture has an effect on the information security culture. This section is to illustrate how Schein's model can contribute to information security.

ARTEFACTS

These are the visible elements in the organization such as logos, architecture, structure, processes and clothing. It includes everything that one hears, sees, and feels when encountering a group with an unfamiliar culture (Schein, 2006).

ESPOUSED BELIEFS AND ASSUMPTIONS

This category includes standards, values, and rules of conduct. These are values that an organization has that gets a group moving in dealing with internal and external problems., If a method a leader proposes works, and continues to work, this method will gradually become a shared standard. This is an example of behavior that unconsciously contributes to the organizational culture

The respondents of the interviews stated that the Dutch culture values that people can work independently and value opinions and discussions. They also like to give people responsibility and freedom in performing their tasks and not restrict them to certain procedures and rules. Thus, the values and rules of conduct from the national culture are reflected in the values of the organization,

which further illustrates that organizational culture is related to national culture. Furthermore, we concluded that culture affects employees' compliance to the security rules. The ISO 27000 framework, does have controls to deal with employees' compliant behavior through awareness programs and monitoring etc. This framework does not include the effect of culture. It was concluded that certain measures, such as monitoring, work well for some cultures, but not for others. Therefore, it is important that the effect of culture on compliant behavior should be considered in the risk management plan of an organization. The organization can improve employees' compliant behavior through artefacts and beliefs to ensure confidentiality, integrity and security.

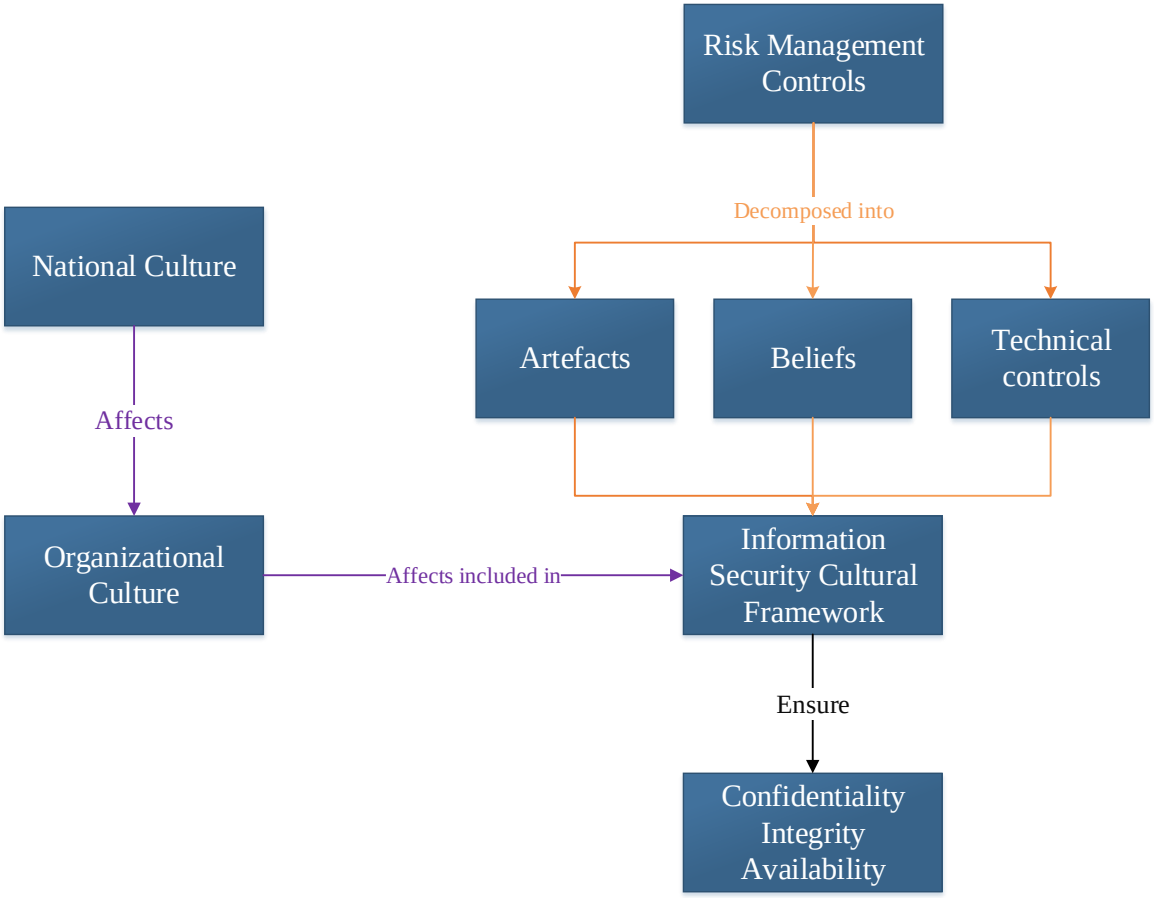

Figure 11: Culture and Risk management

Table 14, contains Hofstede's dimensions with the possible security implications, and the solution for those implications. As can be seen the major contributors for changing behavior are awareness

programs, and written policy. Visible elements in the organization can also help improve the awareness of employees in an organization.

Table 14: Hofstede's dimension, security implications and possible solutions.

Dimension and Implication	**Possible solution**
Power distance	
More responsibility and freedom to perform tasks. Employees can make decisions without consulting superiors. Some of these decisions may affect the systems negatively.	Written Policy containing guidelines on how to deal with the information systems, and constraints, clarifying what employees are not allowed to do.
Employees' opinions are considered in the decision-making process for implementing new rules and technologies.	This is a positive for information security. Thus employees should always be considered in the decision-making process
Individualism	
Not giving opinions to managers about possible bottlenecks in the system concerning security. *Neglecting security rules to finish certain tasks.* *Not reporting security incidents.* *Using company's information for own profit*	Employees need to be aware of the consequences of an incident. These consequences can be clarified in the written policy or on visible elements throughout the organization. Awareness programs is also the best element to change people behavior, since they can better understand how the system operates and also the purpose of the security rules.
Femininity	

Looking after each other to comply with security standards. *Working as a team to improve security.*	Cooperation should be stimulated within the organization. As seen in one of the companies, employees look after each other if someone does not lock the system.
Uncertainty avoidance	
No written guidelines, procedures, unnecessary risk taking	Written policy and awareness programs
Long term Orientation	
Persistent, sense of shame, stating benefit of rules	Written policy, awareness programs, and visible elements in the organization.

Figure 11, shows the elements of an information security cultural framework. Risk management should consider technology and culture as equally important, especially since employees' behavior causes many incidents. This cultural framework is specific for the Dutch culture, since the research was done in the Netherlands.

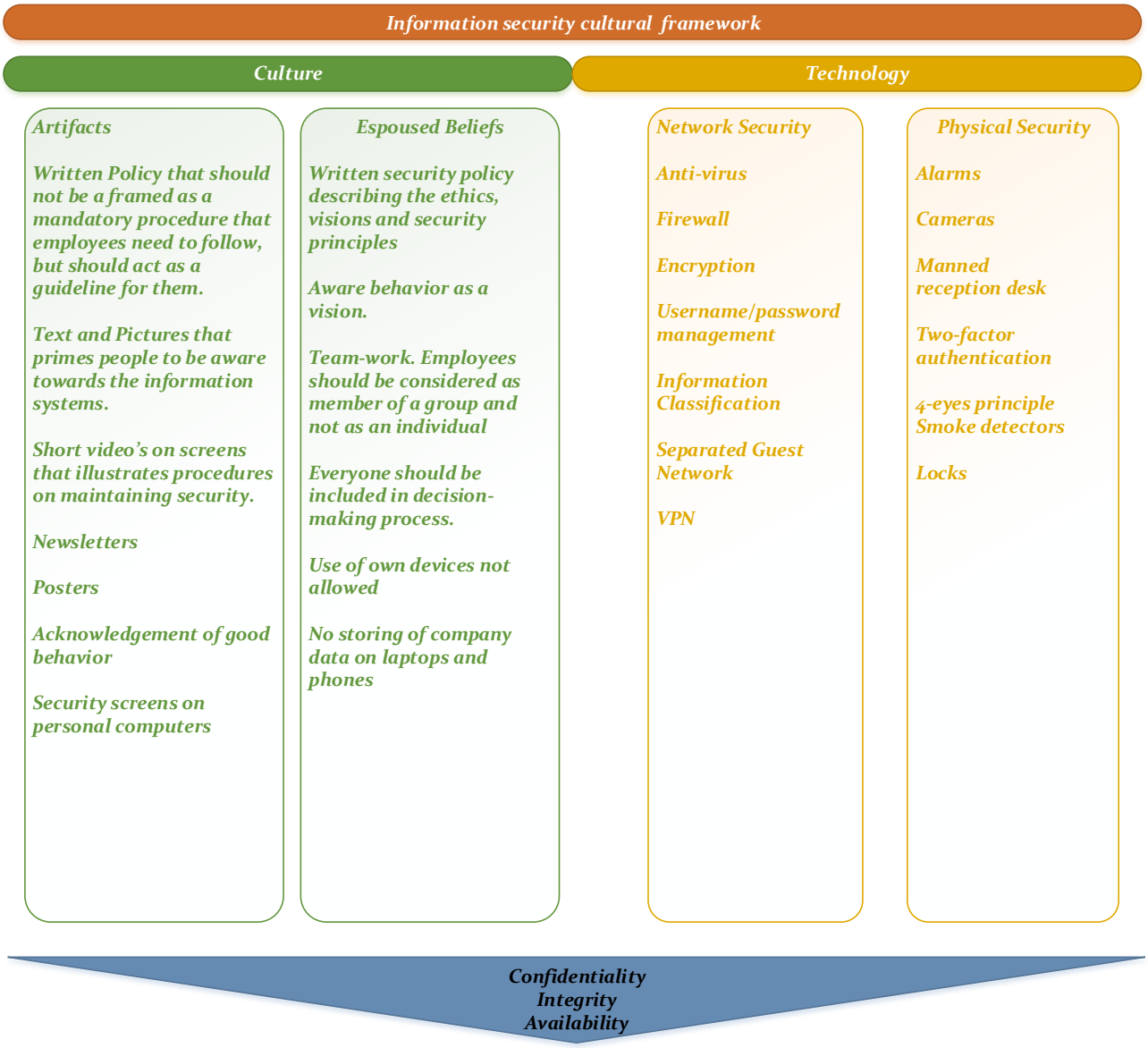

Figure 12: Information security cultural framework

6.2 EVALUATION OF THE FRAMEWORK

The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods (Hevner, March, Park, & Ram, 2004). A design artefact is complete and effective when it satisfies the requirements and constraints of the problem it meant to solve. There are several methods to evaluate a design, such as observing, analyzing, experimenting, testing, and descriptive evaluation. Evaluation of a designed IT artifact requires the definition of appropriate metrics and the gathering and analysis of data. Hevner et al. (Hevner, March, Park, & Ram, 2004) defined several methods to evaluate IT artifacts. However, the majority of the evaluation methods are not applicable to the framework proposed in this research. For instance, it is not possible to simulate the framework, as it deals with people and their behavior. Therefore, the evaluation has to be based on methods typically used in behavioral science, which is data collection and the subsequent empirical analysis. In Chapter 8, recommendations are given on how such an evaluation can be performed in the future. This section does however include a complexity analysis for each of the elements in the framework, with the aim to assess the ease or difficulty of its practical implementation.

WRITTEN SECURITY POLICY

Formulating a written policy can be very time consuming and complex depending on the size of the organization. The main criterion is that the policy should be easy to understand and available for everyone to access. The first step is to identify the goals of the organization, the rules, regulations and laws that the organization is subject to. After this the critical business processes must be mapped and prioritized. The information that passes through these processes needs to be identified as well as the persons responsible for them. For each of the processes, the vulnerabilities, and threats should be analyzed in order to develop contingency plans. The roles and responsibilities should be defined based on the job descriptions. The written policy should state that employees should communicate risks and vulnerabilities if they encounter or identify one.

From the cultural point of view, for in the Dutch context, the written policy should not contain many rules and procedures, in order not to put off or irritate the reader. Thus, it may take several iterations to formulate a policy that employees accept and are willing to comply with. This also means that the compliance with the policy needs to be monitored continuously by an auditing team. In conclusion, formulating a written policy can be very time assuming and therefore costly.

AWARENESS TRAINING

Awareness training should be department specific, since each department may face different risks. The awareness program should clarify which assets need to be protected (i.e. information, services, equipment) and against what threats (i.e. malicious, unintentional, physical). Initially, the questions need to be answered whether the losses prevented by awareness training weigh more than the cost off the awareness program. This means, that an inventory of all the assets need to be made as well as the possible losses if an incident occurs. Furthermore, if there is no expertise in the organization to provide awareness training, external people need to be hired. This inevitably comes with extra expenses.

GOAL PRIMING WITH ARTEFACTS IN THE ORGANIZATION

Priming refers to the passive, subtle, and unobtrusive activation of relevant mental representations by external, environmental stimuli, such that people are not and do not become aware of the influence exerted by those stimuli (Shanks et al., 2013). Auto-motive priming is a form of priming that suggests that goals can be automatically activated by environments in which that goal has been consciously activated repeatedly. After a while, the activation of the goal becomes more automatic until conscious activation of the goal becomes unnecessary (Tesser, Wood, & Stapel, 2005). Goal priming increases the chance that people would act upon a goal than when it was not primed. Behavior is affected by goals that they are not aware off, which can be done by having pictorial or verbal messages in the organization. Priming affects behavior in the absence of attention or awareness of the goal. The goal in the organization would be security awareness or even smaller goals such as always checking if you are logged out, creating strong passwords and not using repetitive parts in the passwords. Thus, by having text and pictures in the organization on walls or folders or on screens that stimulate awareness, it can unconsciously move people to be more aware of the security issues of information systems. These measures are not difficult to implement and can be less expensive than a written policy, and awareness training. The more visible elements used to spread the message, the more effective it will be for the organization. Effective visible elements are posters, newsletters, acknowledgement statements of good behavior, newsletters, and videos (Bosworth et al., 2014).

EMPLOYEE SCREENING

From both the survey and the interviews, it can be concluded the majority of organizations do not screen employees even when they have access to sensitive information. It is not always possible to perform a complete background check on someone and it may also be costly and time consuming. However, organizations may at least require a certificate of good conduct of their employees. This is not difficult to achieve and also not that expensive and may act as a filter for people with a criminal record.

CHAPTER 7 CONCLUSION

In this section, the conclusions of the thesis are given. The aim of the research was to propose an information security cultural framework that incorporates the influence of culture on compliant behavior. The research question was: *Which factors of culture need to be considered for ensuring information security compliant behavior?* In order to answer this question, it first had to be verified if there is a relation between national and organizational culture, since an information security culture is part of an organizational culture. If no relation was found between the two, then it would not be necessary to look at the relation between national culture and information security culture, but merely at the relation between organizational and information security culture. Furthermore, the thesis elaborated on the importance of information security culture, and on its key elements.

The research sub-questions were:

- *What is the importance of an information security culture?*
- *What are the key elements of an information security culture?*
- *What is the relation between national and organizational culture?*

WHAT IS THE IMPORTANCE OF AN INFORMATION SECURITY CULTURE?

An organization's culture can improve the level of information services security. The majority of information security incidents are caused by employees who do not comply with the organizational policies and procedures. An information security culture with the values of knowledge, awareness and secure behavior can minimize the incidents caused by employees. The information security culture should also consider the effects of national culture on employees' compliant behavior, as the national culture influences the employees' compliance. For instance, Germany has a slightly higher score than the Netherlands on the uncertainty avoidance dimensions. Yet, the mere difference of 12 points between these two countries has a noticeable effect on how people deal with security.

WHAT ARE THE KEY ELEMENTS OF AN INFORMATION SECURITY CULTURE?

Based on the literature research, the key elements of an information security culture are a written policy, security awareness and training. Security awareness refers to the marketing and promotion of security inside the organization such posters, e-mail reminders which are motivational by nature. Security training is an actual security course that takes place in a classroom or online with the purpose to teach the employees how the systems should be used in a secure way, and also to stimulate the employees to demonstrate security compliant behavior.

WHAT IS THE RELATION BETWEEN NATIONAL AND ORGANIZATIONAL CULTURE?

The interviews verified Hofstede's claim that there is a relation between organizational and national culture, because individuals take the social values and norms they receive from birth to the organizations they work in. These values are also enforced by the managers through training, monitoring, and through other socialization processes. As concluded from the interviews, managers in the Netherlands give employees freedom and responsibility to perform their tasks, which is a characteristic of the low power distance of the Dutch culture.

WHICH FACTORS OF CULTURE AND WHICH RISK MANAGEMENT MEASURES NEED TO BE CONSIDERED FOR ENSURING INFORMATION SECURITY COMPLIANT BEHAVIOR OF ORGANIZATION EMPLOYEES?

The reasoning behind this research was that many organizations have technical security measures implemented but neglect the effect human behavior has on information systems. Human behavior is dependent on national culture, as the national cultural traits are ingrained in the people of a culture. The organizational cultural values are derived from the national culture. This was confirmed from data obtained via the interviews. The result of the thesis is a security cultural framework containing, national, organizational and risk management measures to improve the employees' compliant behavior. The framework consists of the following elements.

WRITTEN POLICY

The Risk Management measures aimed to improve employees' compliant behavior are: a written policy and awareness training. The written security policy should contain all the guidelines, and rules that employees have to comply with. To make employees of the Dutch culture comply with the written policy, it is important not to formulate it with too many rules and procedures, as it can cause irritation.

VISIBLE ARTEFACTS

Newsletters, short videos, security texts on walls, and security messages on employees' computer screen in order to prime them to be more aware towards the information system.

ESPOUSED BELIEFS AND ASSUMPTIONS

This category includes standards, values, and rules of conduct. These are values that an organization has that gets a group moving in dealing with internal and external problems. National culture has an effect on information security, which can either be good or bad depending on the cultural trait. The cooperation characteristic of the Dutch culture within departments is a good factor for ensuring information security as well as the low power distance, where employees' opinions are considered for implementing new policies. This increases the willingness of employees to comply with the policies. The values and standards of the organization should deal with the individualism of the Dutch so that they put the security of the organization above their own interest.

CHAPTER 8 RECOMMENDATIONS AND FUTURE RESEARCH

The purpose of information security is to ensure the confidentiality, integrity and availability of information and information systems. This cannot be achieved by only having technological measures implemented. The main focus should be on employees, since the major incidents are caused by them either due to their careless behavior or on purpose. The thesis studied the effect of national culture on information security in the Netherlands, to understand the effect of the Dutch culture on information security and how they comply with the rules. By studying this, problems derived from culture can be defined, and in turn solutions can be found to deal with these problems. This information can then be used as a guideline for companies in the Netherlands in setting up the security framework and enabling them to tackle certain subjects before any damage occurs. The results of the research a specific for the Dutch culture, as each country has different cultural traits. The key characteristics of the Dutch culture are individualism and femininity; thus the result may be generalizable for countries with similar cultures. In this chapter, the main findings of the influence of culture on information security are stated and recommendations are given.

8.1 RECOMMENDATION

WRITTEN POLICY

It cannot be overstated that a written policy is an important element of an information security culture, as it contains all the rules, guidelines, procedures and constraints for employees. However, the majority of the companies interviewed do not have written policies. This is a cultural trait of the Netherlands, derived from the uncertainty avoidance dimension. The Dutch consider rules and procedures as constraints on their way of performing tasks, since they like thinking out of the box and work in unconventional manners. Therefore, an important recommendation is that in the Netherlands, a written security policy should not be framed as a set of procedures and rules that employees must follow. Instead, it should be formulated in a way that makes the employees aware of security threats and of the consequences following from their lack of compliance with the security rules. The security policy should be a document that provides information on actions with their possible risks, being more of a guideline rather than a list of rules and procedures.

AWARENESS PROGRAMS

Awareness programs help making security rules and procedures understandable for employees, and increase their willingness to comply with them. The ideal size for a training course is between 10 and 15 participants, because it enables them to maintain personal contact with each other and it also stimulates people to state their viewpoints and opinions.

The Dutch culture scores high on individualism, but at the same time the data show that there is cooperation within the departments, as employees tend to look after each other. This behavior should also be stimulated for the sake of better security. For example, employees who forget to sign out are reminded by their colleagues to do so. New colleagues acquire this behavior and also remind others to sign out. This can be applied for other problems as well, for example in the case of employees who neglect security rules in order to finish a task on time and take their work home on a laptop. This cannot always be monitored by the security department, but it can be minimized from occurring if employees stop doing it and explicitly stimulate others to follow their example.

If an organization is large, an awareness training would be expensive for the whole organization. In such a case, some employees can be selected from each department to take part in the security training. After the training, they can transfer what they have learned to the other employees in a motivating way.

DECISION-MAKING PROCESS

Another good aspect of the Dutch culture is that employees' opinions are considered in the decision-making process. They can help formulate the security rules and help decide with measures need to be implemented. When they know that their opinions count, they will be more willing to comply with the security rules. This aspect should be strengthened in order to enhance the security culture.

PASSWORD CHANGE POLICY

The majority of the organizations interviewed have a password change policy, but as the interviewees said, employees often keep a fixed part in their password. The only part they change is the month or the year, depending on the change policy. This can be very harmful, since it makes it easier to guess someone's password. Therefore, beside a change policy, a measure should be

implemented to prevent employees from using a part of a previous password, or a multi-factor authentication should be installed.

COMMUNICATION

Both the literature review and interview results led to the conclusion that communication with employees is the key to safeguarding the organizations. The measures and the corresponding risks should be explained to employees, so that they know that not only their reputation, but also that of their organization is at stake if an incident occurs. Especially small firms, who do not have many measures implemented, should communicate them well with their employees.

EVALUATION

To study the effectiveness of the proposed framework, it has to be evaluated based on methods typically used in behavioral science, which is data collection and the subsequent empirical analysis. The following methods are proposed:

1.SCENARIOS

The effectiveness of the framework can be tested with specifically designed scenarios to monitor how employees behave in dealing with a security threat, or more generally, how security-aware their behavior is (e.g., do they log off their workstation when leaving the workplace).

2.OBSERVATIONAL EVALUATION

A case study can be carried out to evaluate the effectiveness of the framework in practice. Before the framework is implemented in an organization, employees of a department can be interviewed to grasp their opinion on information security, and their behavior should also be monitored. After the framework has been implemented and used in practice, these employees can be interviewed again to see if their opinion and behavior on information security has changed. A survey can also be created to measure the effectiveness of the framework, namely if employees have become more compliant with the security rules. It is also possible to implement the framework in one department of the organization and monitor over time the differences with other departments.

The metrics to consider in the evaluation are:

- The frequency that employees forget to log out of their workstation.
- The frequency that employees report risks

- The frequency that incidents from careless behavior occur
- Employees perception of a written policy
- Employees compliance with the rules and procedures in the written policy
- Employees cooperation with colleagues to ensure security

8.2 LIMITATIONS OF THIS RESEARCH

LIMITATION 1

The results of the survey were disappointingly low as only 35 of the 1100 companies replied. This can be explained by the topic of the research, since many companies do not want to share sensitive information. This made it impossible to differentiate between sectors and company sizes. The interviewed companies were all from the IT sector, thus the conclusions possibly hold only for this sector.

LIMITATION 2

Only one of the interviewees was a security expert. Other employees may not find the policies as important as the security experts. The security expert also gave some recommendation on how awareness programs can be executed effectively. The other interviewees did not really have recommendations on how to improve security.

8.3 FUTURE RESEARCH

The people that were interviewed were from Dutch companies, but there are also foreign companies with foreign managers in the Netherlands. For example, there are several Japanese companies in the Netherlands. The Japanese culture is very masculine and has a high score on uncertainty avoidance. Thus, they have another culture, but the majority of the staff are mostly Dutch. Thus, it would be interesting to see the security differences between foreign companies and local companies in the Netherlands, especially how the employees perceive and deal with the security policies.

The interviews were conducted in companies that have an informal culture, meaning they wore casual clothes and there was no real hierarchy visible. It is not known how the hierarchy is in companies with a more formal culture and if those companies have written policies that the

employees need to comply with. For further research, it is possible to analyze the differences in information security between companies with a formal and informal culture. It is also possible to study if there is a difference on how national culture is visible in these organizations.

The people that were interviewed were from companies within the IT sector. However, the finance and military sector have stricter policies and security measures. This means that people in those sectors comply more with the security policies and measures. Therefore, research can be conducted to study why this is the case, since the people working there are also from the same culture as in the other sectors.

Finally, it would be interesting to see the extent to which changes in scores of the dimension affect information security. As we saw, the score for uncertainty avoidance in Germany is only 12 points higher than in the Netherlands, but this already had some noticeable changes.

REFERENCES

Al-Mukahal, H. M., & Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations. *Information and Computer Security, 23*(1), 102-118. doi:10.1108/ICS-03-2014-0018

Andress, J. (2014). Chapter 1 - What is Information Security? In J. Andress (Ed.), *The Basics of Information Security (Second Edition)* (pp. 1-22). Boston: Syngress.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report, 13*(4), 195-201. doi:http://dx.doi.org/10.1016/j.istr.2008.10.006

Bosworth, S., Kabay, M. E., & Whyne, E. (2014). *Computer Security Handbook, Set*: Wiley.

Burrows, J. H. (1993). Information technology standards in a changing world: The role of the users. *Computer Standards & Interfaces, 15*(1), 49-56. doi:http://dx.doi.org/10.1016/0920-5489(93)90028-P

Cabric, M. (2015). Chapter 11 - Confidentiality, Integrity, and Availability. In M. Cabric (Ed.), *Corporate Security Management* (pp. 185-200): Butterworth-Heinemann.

Chow, C. W., Kato, Y., & Merchant, K. A. (1996). The use of organizational controls and their effects on data manipulation and management myopia: A Japan vs U.S. comparison. *Accounting, Organizations and Society, 21*(2-3), 175-192. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-0030077223&partnerID=40&md5=4c12d8e99cdf4872fa786c43b1c7c0ef

Clarke, R. A., & Knake, R. K. (2011). *Cyber war*: HarperCollins.

da Veiga, A., & Martins, N. (2015a). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176. doi:http://dx.doi.org/10.1016/j.cose.2014.12.006

Da Veiga, A., & Martins, N. (2015b). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review, 31*(2), 243-256. doi:http://dx.doi.org/10.1016/j.clsr.2015.01.005

Dalziel, H. (2015). Chapter 2 - ISO Security Management Categories *Infosec Management Fundamentals* (pp. 7-11). Boston: Syngress.

Day, C. (2013). Chapter 26 - Intrusion Prevention and Detection Systems. In J. R. Vacca (Ed.), *Computer and Information Security Handbook (Second Edition)* (pp. 485-498). Boston: Morgan Kaufmann.

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security, 56*, 63-69. doi:http://dx.doi.org/10.1016/j.cose.2015.10.001

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449-457. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2009.05.003

Ghosh, M. (2010). Mobile ID fraud: the downside of mobile growth. *Computer Fraud & Security, 2010*(12), 8-13. doi:http://dx.doi.org/10.1016/S1361-3723(10)70155-X

Glaser, T., & Pallas, F. (2007). Information security and knowledge management: solutions through analogies? *Available at SSRN 1014302*.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242-251. doi:http://dx.doi.org/10.1016/j.cose.2012.10.003

Halpin, E. F. (2013). *Digital Public Administration and E-Government in Developing Nations: Policy and Practice: Policy and Practice*: IGI Global.

Herold, R. (2010). *Managing an information security and privacy awareness and training program*: CRC press.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Q., 28*(1), 75-105.

Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. *Computer Law & Security Review, 29*(3), 236-245. doi:http://dx.doi.org/10.1016/j.clsr.2013.03.003

Hofstede, G. (1983). Cultural dimensions for project management. *International Journal of Project Management, 1*(1), 41-48. doi:http://dx.doi.org/10.1016/0263-7863(83)90038-8

Hofstede, G. (1994). The business of international business is culture. *International Business Review, 3*(1), 1-14. doi:http://dx.doi.org/10.1016/0969-5931(94)90011-6

Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security, 21*(5), 402-409. doi:http://dx.doi.org/10.1016/S0167-4048(02)00504-7

Ifinedo, P. (2009). Information technology security management concerns in global financial services institutions: Is national culture a differentiator? *Information Management & Computer Security, 17*(5), 372-387. doi:doi:10.1108/09685220911006678

Jarmon, D. (2002). A Preparation Guide to Information Security Policies. *SANS Information Security Reading Room*.

Khanna, R. (2013). Data breaches: the enemy within. *Computer Fraud & Security, 2013*(8), 8-11. doi:http://dx.doi.org/10.1016/S1361-3723(13)70071-X

Kim, D.-Y. (2014). Cyber security issues imposed on nuclear power plants. *Annals of Nuclear Energy, 65*, 141-143. doi:http://dx.doi.org/10.1016/j.anucene.2013.10.039

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security, 33*, 3-11. doi:http://dx.doi.org/10.1016/j.cose.2012.07.001

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59*, 60-70. doi:http://dx.doi.org/10.1016/j.cose.2016.02.004

Lee, Y., & Kramer, A. The role of purposeful diversity and inclusion strategy (PDIS) and cultural tightness/looseness in the relationship between national culture and organizational culture. *Human Resource Management Review*. doi:http://dx.doi.org/10.1016/j.hrmr.2016.01.001

Leidner, D. E., & Kayworth, T. (2006). Review: a review of culture in information systems research: toward a theory of information technology culture conflict. *MIS quarterly, 30*(2), 357-399.

Lilienthal, G., & Ahmad, N. (2015). Cyber-attack as inevitable kinetic war. *Computer Law & Security Review, 31*(3), 390-400. doi:http://dx.doi.org/10.1016/j.clsr.2015.03.002

Lim, J. S., Chang, S., Maynard, S., & Ahmad, A. (2009). *Exploring the relationship between organizational culture and information security culture*. Paper presented at the Australian Information Security Management Conference.

Moberly, M. D. (2014). Chapter 10 - Insider Risks and Threats to Intangible Assets. In M. D. Moberly (Ed.), *Safeguarding Intangible Assets* (pp. 133-143). Boston: Butterworth-Heinemann.

Mohelska, H., & Sokolova, M. (2015). Organisational Culture and Leadership – Joint Vessels? *Procedia - Social and Behavioral Sciences, 171*, 1011-1016. doi:http://dx.doi.org/10.1016/j.sbspro.2015.01.223

Nelson, R. E., & Gopalan, S. (2003). Do organizational cultures replicate national cultures? Isomorphism, rejection and reciprocal opposition in the corporate values of three countries. *Organization studies, 24*(7), 1115-1151.

Nemati, H. (2010). *Security and Privacy Assurance in Advancing Technologies: New Developments: New Developments*: IGI Global.

Pawar, M. V., & Anuradha, J. (2015). Network Security and Types of Attacks in Network. *Procedia Computer Science, 48*, 503-506. doi:http://dx.doi.org/10.1016/j.procs.2015.04.126

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Rodríguez, D., Busco, C., & Flores, R. (2015). Information technology within society's evolution. *Technology in Society, 40*, 64-72. doi:http://dx.doi.org/10.1016/j.techsoc.2014.08.006

Schein, E. H. (2006). *Organizational Culture and Leadership*: Wiley.

Schumacher, M. (2002). *Security Patterns and Security Standards.* Paper presented at the EuroPLoP.

Script Kiddies Rule The Internet. (2001). *Computer Fraud & Security, 2001*(3), 5. doi:http://dx.doi.org/10.1016/S1361-3723(01)03011-1

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14*, 36-45. doi:http://dx.doi.org/10.1016/j.diin.2015.07.002

Sennewald, C. A., & Baillie, C. (2016). 23 - Written Policies and Procedures. In C. A. Sennewald & C. Baillie (Eds.), *Effective Security Management (Sixth Edition)* (pp. 223-233): Butterworth-Heinemann.

Shaaban, H., & Conrad, M. (2013). Democracy, culture and information security: A case study in Zanzibar. *Information Management and Computer Security*, *21*(3), 191-201. doi:10.1108/IMCS-09-2012-0057

Shanks, D. R., Newell, B. R., Lee, E. H., Balakrishnan, D., Ekelund, L., Cenac, Z., . . . Moore, C. (2013). Priming intelligent behavior: An elusive phenomenon. *PloS one*, *8*(4), e56515.

Shih, T.-H., & Fan, X. (2009). Comparing response rates in e-mail and paper surveys: A meta-analysis. *Educational Research Review, 4*(1), 26-40. doi:http://dx.doi.org/10.1016/j.edurev.2008.01.003

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Journal of Military Studies, 4*(1).

Silva, S. S. C., Silva, R. M. P., Pinto, R. C. G., & Salles, R. M. (2013). Botnets: A survey. *Computer Networks, 57*(2), 378-403. doi:http://dx.doi.org/10.1016/j.comnet.2012.07.021

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying critical infrastructure sectors and their dependencies: An Indian scenario. *International Journal of Critical Infrastructure Protection, 7*(2), 71-85. doi:http://dx.doi.org/10.1016/j.ijcip.2014.04.003

Sumner, S. (2016). Chapter 6 - Security, Spear Phishing and Social Engineering. In S. Sumner (Ed.), *You: for Sale* (pp. 107-124). Boston: Syngress.

Sundqvist, A., & Svärd, P. (2016). Information culture and records management: a suitable match? Conceptualizations of information culture and their application on records management. *International Journal of Information Management, 36*(1), 9-15. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2015.08.004

Taylor, L. P. (2013). Chapter 9 - Addressing Security Awareness and Training *FISMA Compliance Handbook (Second Edition)* (pp. 79-86). Boston: Syngress.

Team, V. R. (2015). 2015 Data Breach Investigations Report.

Tesser, A., Wood, J. V., & Stapel, D. A. (2005). *Building, Defending, and Regulating the Self: A Psychological Perspective*: Taylor & Francis.

von Solms, B. (2000). Information Security — The Third Wave? *Computers & Security, 19*(7), 615-620. doi:http://dx.doi.org/10.1016/S0167-4048(00)07021-8

von Solms, B. (2006). Information Security – The Fourth Wave. *Computers & Security, 25*(3), 165-168. doi:http://dx.doi.org/10.1016/j.cose.2006.03.004

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security, 23*(5), 371-376. doi:http://dx.doi.org/10.1016/j.cose.2004.05.002

Watson, G. (2014). Chapter 15 - Staff Awareness and Training Programs *Social Engineering Penetration Testing* (pp. 339-359). Boston: Syngress.

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security, 44*, 1-15. doi:http://dx.doi.org/10.1016/j.cose.2014.04.005

Williams, P. (2001). Information Security Governance. *Information Security Technical Report, 6*(3), 60-70. doi:http://dx.doi.org/10.1016/S1363-4127(01)00309-0

APPENDIX I MEASURES

ICT SECURITY

- **Anti-virus** – An antivirus is a software program that is developed to prevent, detect and remove software viruses (malicious software) that causes harm to the system. It can be installed on the:
    - Mail servers – screening of all incoming mails for threats.
    - PC – as a software.
    - Storage devices – Anti-virus on storage devices to scan for threats transferred from personal devices.

- **Software updates / patching** – Software updates and patches can be used to fix bugs in the system to improve its performance and thus make it safer.
- **Firewall** – It is a software program that is designed to prevent unauthorized access to and from a private network. It can be implemented in a hardware or software form or combination of both. It can exist on an individual computer or as part of the entire network installed on a server or router.
    - **Host based firewall** – This is a software application installed on a single computer and usually comes with an anti-virus program. Most operating system manufacturers also include and firewall as part of the system.
    - **Network based firewall** – This firewall operates on a network level and it filters data that travels from the internet to the computers on the network. A kind of perimeter is set up that regulates the flow of data before it reaches the individual computers. Network based firewalls can be split into routers and proxy servers.
        - **Router** – These are hardware firewalls with certain firewall- rules that can filter traffic that enters the network by blocking protocols with the port numbers.
        - **Proxy servers** – This is a sever that functions as a firewall by acting as an intermediary between internal computers and external networks

by receiving and blocking “dangerous” data packets at the network boundary. It is a part of a gateway server that separates the network from the outside and a firewall that protects the internal network from outside intrusion.

- **Next generation firewall** – This is a hardware/ software based network security system that is able to detect and block cyber-attacks by enforcing security policies at the application level. It combines the capabilities of traditional firewalls, such as packet filtering, network address translation (NAT), URL blocking with Quality of service (QoS) functionalities such as SSL, SSH inspection and malware detection. It is better than the traditional firewalls by being able to detect threats on higher layers of the OSI model.
- **Intrusion detection software** – Other software that go a step further than the conventional anti-viruses that are used to detect and prevent security threats. The prevention of intrusions can occur automatically or is first sent as a warning message to the system administrator.
- **Encryption** – Encryption refers to the scrambling of data with a very large digital number key that can be used to make confidential information less easy to crack by a hacker.
- **Availability of Wireless network**

  A separated guest network makes minimizes the chance that an intruder gains access to the main network from which he can penetrate the system.
- **Virtual Private Network (VPN)** – this is a method used to enhance the security and privacy to private networks to protect sensitive data. Privacy is increased since the initial IP address is replaced with one from the VPN provider.
- **Username/Password management** – These are applications that hold the encrypted password safe to ensure secure logon onto computer.
    - Password can either be stored locally or can lie on a central server that checks if the password is correct. This single sign on (SSO) is a user authentication

process that enables a user to enter one name and password to grant access to multiple applications.

    - Multi-factor authentication – Extra authentication required such as a token to gain access to the network.

- **Renewable passwords** – It is safer if employees have to renew their password on a frequent basis.
- **Information classification** – Classification of the information in confidential and public within the organization by establishing rules. The confidential information should not be available to everyone in the organization. Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. There should be an initial classification and reclassification over time. The access control policy should also be mention when classifying information.

- **Cloud services** (confidential information in the cloud) – Refers to where the information of the organization is stored. There are different cloud services available that each deliver a different set of features for the client. He can decide what kind of information he stores on the cloud, confidential or not. Rules should also be set who has access to the information stored on the cloud and what will occur if confidential information is leaked by the vendor.

European cloud or American cloud – Companies should be aware that in Europe and America there are different policies regarding the information stored on the cloud. Therefore, they should be considerate on which information they store on the cloud.

PHYSICAL AND ENVIRONMENTAL SECURITY

- **Centralized user data storage** – Is the user data and other critical information stored in a central storage facility or on individual computers.
- **Multiple locks** – Are there multiple locks available to stop unauthorized entrance to the server room.
- **Manned reception desk** – A desk with a person who controls and checks the entrance of persons to specific area's in the building. The date and time of entry and departure should be recorded.
- **Visible identification required** – Employees and visitors are required to wear a visible identification and should report if they encounter someone who's not wearing one.
- **Intrusion detectors (alarms, cameras)** – The installation of alarms and cameras to detect and prevent unauthorized entrance in certain areas.
- **Smoke detectors** - Smoke detectors to detect if a fire occurs.
- **Access management** – Who has access to what information. Are all employees allowed to access all facilities or do you need to have a special pass? Or can one employee enter the storage room alone or do they need to access them with at least two people?
- **Cabling security** – protection of power and telecommunications cabling carrying data or for supporting critical services.
- **Biometrics, smart cards/tokens** - These are the physical authentication method used to grant an employee access to certain facilities.
- **Two-factor authentication** – requires username and password and something else that only the user has on them such as a physical token.

4-eyes principle – This refers to the policy that at least 2 individuals are required before an action can be taken, for example to enter the server room.

ORGANISATION MANAGEMENT

- **Organisational structure** – Defines the structure of the organization and if there is an IT staff available who controls and maintains the security of computers. They also install the necessary patches and updates and can analyse the employees' online behaviour. In smaller companies it can also be the case that there is no IT staff who maintains the computer. Do the employees have to perform updates for their own computers or is an external company hired to do this from time to time.

- **Screening of employees** – Refers to the screening of persons and how well they are screened before they are hired. Some of the measures that should be considerate are:
    - Extensive screening for sensitive jobs.
    - Screening the applicant's curriculum vitae and business references.
    - Confirmation of claimed academic and professional qualifications.
    - Checking for criminal records.

- **Policies included in contract** – Security policies should be included so that the employees are aware and can be held accountable for misbehaviour.
- **Security awareness and education/ Training** – Refers to the training the staff to deal with security threats and if these occur on a regular basis. The security policy should also define if the trainings are mandatory or not.
- **Acceptable behavior of users** - Covers permitted user activities, such as work-related use of the systems and information, and internet usage in particular. Are certain websites blocked for use or do they just receive a warning not to enter them. Can they use a unauthorized USB sticks on the computers.
- **Message forwarding** – Restrictions of forwarding messages to outsiders, since the messages can contain some confidential information.
- **Mobile computing** – refers to the use of personal devices on workspace or work devices at home.

- **Loss or theft of portable devices** – The protocol employees need to follow if a portable device of the company gets stolen.
- **Equipment repairs** – it should be made clear if the portable device fails, who will repair it. Will it be done internally or can the employee bring it to any repair shop to fix it.

Installation of unauthorized software – Are employees allowed to install own software on the company's computer?

APPENDIX II SECURITY THREATS

Cyber Bullying

The use of technology to harass, threaten, embarrass or target another person. This can be done by sending rude texts, mean tweets or by posting personal information, photos or videos to embarrass someone else

Cyber Stalking

A cyber stalker uses the internet to stalk their victim without being detected and harasses them with email or other means of electronic communication.

Cyber Squatting

This refers to the act of registering domain names, especially those registered with recognizable trademarks, with the intention of reselling them at a higher price. For example, if a cyber-squatter was the first person who created the domain tudelft.nl, TU Delft would have to pursue a lawsuit to force the cyber squatter to withdraw the name or TU Delft had to pay the price the cyber squatter asks for the domain.

Cybercrime

This typically refers to any type of financial criminal activity conducted over cyberspace, such as phishing, pharming etc.

Racketeering and blackmailing

Racketeering is an illegal act in which and illegal operation of an illegal business or scheme is used in order to create revenue. Racketeering includes acts such as bribery, illegal gambling, exploitation of children, money laundering etc.

Cyber attacks

Finally, cyber-attacks refer to attacks on the e-facilities of government, business and citizens. This includes spam, DoS attacks, spyware and other types of attacks (Gorge, 2007). Compared to normal attacks, cyber terrorism attacks can be considered as traditional terrorist attacks in the sense that these attacks are organized and lot of Intel was gathered to perfectly execute the attack (Gorge, 2007). The most common infrastructures that are targeted are Banking and Finance, telecommunication sector, agriculture, food industry, energy sector, drinking water, dams and infrastructures where chemicals and other dangerous materials are processed.

APPENDIX III SURVEY

ALGEMENE INFORMATIE

1. Hoe bezorgd bent u over het risico dat uw bedrijf loopt om een slachtoffer van cyberaanvallen te worden (denk hierbij aan inbreuken op IT systemen, het verlies van gegevens, phishing, etc.)?

   - ○ niet bezorgd
   - ○ een beetje bezorgd
   - ◉ zeer bezorgd
   - ○ geen mening over

2. Bent u bekend met cyber gerelateerde incidenten in uw bedrijf of bedrijven waarmee u een relatie had in de afgelopen 3 jaren?

   - ○ ja
   - ◉ nee

3. Wordt er in uw bedrijf of brancheverenigingactief gesproken over cyberaanvallen en cyberparaatheid?

   - ○ ja
   - ◉ nee

4. Heeft u uw beschermingsmaatregelen in de afgelopen 2 jaar veranderd?

   - ◉ geen verandering
   - ○ kleine veranderingen

- grote aanpassingen
- volledig nieuwe maatregelen ingevoerd

5. Hoe beoordeelt u uw security paraatheid ten opzichte van andere bedrijven?
   - minder goed voorbereid
   - ongeveer gelijk
   - beter voorbereid
6. In welke sector bevindt uw bedrijf zich?
   - accountancy
   - assurantiën
   - energie
   - transport en logistiek
   - productie
   - IT services
   - elektronica en elektrotechniek
7. Hoeveel werknemers telt uw bedrijf?
   - 1-5
   - 5-20
   - 20-50

- ○ 50-100
- ○ 100-250
- ○ 250-500
- ○ meer dan 500

DEEL 1: ICT VEILIGHEID

1. Heeft u een schriftelijk ICT-beveiligingsplan opgesteld?
   - ◉ ja
   - ○ nee
2. Gebruikt u anti-virus software?
   - ☐ op werkplekken (desktops, laptops, PCs in het algemeen)
   - ☐ op mailservers (actieve screening van binnenkomende e-mails)
   - ☐ op opslag- en fileservers
3. Heeft u een draadloos network (WiFi) op uw bedrijfslokatie?
   - ◉ ja
   - ○ nee
4. Maken alle medewerkers verbinding met het draadloos netwerk via hetzelfde, gemeenschappelijke wachtwoord (in tegenstelling tot elke werknemer een eigen, persoonlijk draadloos account en wachtwoord)?
   - ○ ja

- (•) nee

5. Is het draadloze netwerk toegankelijk voor gasten en bezoekers?

   - (•) ja
   - ( ) nee

6. Is er een wachtwoord nodig voor bezoekers om toegang tot het draadloos netwerk te krijgen?

   - ( ) ja
   - ( ) nee

7. Wordt de communicatie van de gasten op het draadloze netwerk gescheiden van het eigen netwerk (bijvoorbeeld via een VPN, afzonderlijk subnet of netwerk)?

   - ( ) ja
   - ( ) nee

8. Hoe en hoe vaak wordt de bestaande software in uw bedrijf bijgewerkt?

   - [ ] Geen updates op bestaande computers
   - [ ] Wanneer hardware reparaties worden uitgevoerd, worden ook updates geïnstalleerd[ ] Automatisch wanneer er nieuwe updates beschikbaar zijn
   - [ ] Handmatig, met onregelmatige tussenpozen
   - [ ] In een vaste routine, zoals dagelijks, wekelijks, maandelijks, etc.

9. Wanneer heeft u een gebruikersnaam en wachtwoord nodig om toegang tot bedrijfsmiddelen te krijgen?

- [ ] bij gebruik van een PC of laptop
- [ ] bij opstarten of gebruiken van specifieke applicaties
- [ ] bij verbinden met het network
- [ ] gebruik van bestanden op een gedeelde server van het bedrijf

10. Vereisen bedrijfspolicies u om wachtwoorden regelmatig te veranderen?

- ○ nooit
- ○ dagelijks
- ○ wekelijks
- ○ maadelijks
- ○ elke paar maaden
- ○ een keer per jaar
- ○ minder dan alle opties

11. Onderscheidt en classificeert u informatie op basis van wie het binnen het bedrijf mag zien en wat de gevoeligheid en waarde hiervan is (met uitzondering van financiële of salarisgegevens)?

- ○ Er wordt geen onderscheiding gemaakt
- ○ Toegang tot documenten is beperkt tot groepen en/of afdelingen, hier binnen mag iedereen documenten bekijken en aanpassen

- ○ Documenten zijn alleen toegankelijk voor de medewerkers die er toegang toe nodig hebben (bijvoorbeeld door hun rol in de organisatie, deelname van een specifiek project, etc.)

12. Wordt data binnen uw bedrijf versleuteld?

    - ☐ nee
    - ☐ Op desktop computers binnen het kantoor
    - ☐ Op laptops welke buiten het bedrijf gebruikt worden
    - ☐ Op mobiele telefoons
    - ☐ Op USB opslag, draagbare harde schrijven en SD-kaarten
    - ☐ Op opslag servers binnen het bedrijf
    - ☐ Op opslag servers bij cloud providers en externe data-opslag

13. Gebruikt u cloud service providers voor uw bedrijf (zoals Dropbox, Microsoft Azure of Google Drive)?

    - ◉ ja
    - ○ nee

14. Hoe heeft u de cloud provider voor uw bedrijf gekozen?

    - ☐ Op prijs
    - ☐ Functionele eisen

- ☐ Waar de meeste medewerkers reeds vertrouwd mee waren of al gebruikten
- ☐ Specifiek een Nederlandse / Europese leverancier uir privacy overwegingen
- ☐ Specifiek een Nederlandse / Europese leverancier uit juridische overwegingen
- ☐ Op basis van een bestaande zakelijke relatie

DEEL 2: FYSIEKE VEILIGHEID

1. Welke fysieke veiligheidsmaatregelen gebruikt u in uw organisatie?
   - ☐ Bemande receptive
   - ☐ Medewerkers moeten zichtbaar identificatie dragen
   - ☐ Gasten en bezoekers moeten worden begeleid door medewerkers
   - ☐ Werknemers gebruiken keycards (smart cards, tokens, biometrie) om toegang te krijgen
   - ☐ Alarm centrale, camera surveillance
2. Heeft u extra veiligheidsmaatregelen met betrekking tot fysieke toegang tot uw IT-systemen of specifieke apparatuur?
   - ☐ Twee-factor authenticatie
   - ☐ 4-ogen-principe (twee medewerkers moeten samen werken)
   - ☐ Apparatuur met opnamefunctie (mobiele telefoons, camera's, etc.) zijn verboden

DEEL 3: ORGANISATIE MANAGEMENT

1. Wie onderhoudt de ICT-infrastructuur (zoals het uitvoeren van updates, het installeren van nieuwe software, configuratie pc's, etc.)?

- ☐ Elke medewerker voor zich
- ☐ één of meer in IT gespecialiseerde werknemers
- ☐ Externe provider (uitbesteed)

2. Mogen medewerkers hun eigen apparaten (zoals laptop, USB stick en smartphone) naar het werk meenemen?

   - ○ Ja, er bestaan geen beperkingen
   - ○ Toegestaan om het apparaat mee te nemen, maar geen verbinding te maken met het bedrijfsnetwerk
   - ○ Toegestaan om het apparaat mee te nemen, echter alleen aan te sluiten op het gastnetwerk
   - ◉ Toegestaan om het apparaat mee te nemen, er mag een verbinding met het bedrijfsnetwerk gemaakt worden

3. Zijn medewerkers toegestaan om apparaten (bijv. een bedrijfslaptop) buiten het bedrijf mee te nemen?

   - ○ Nee
   - ◉ Ja, maar alleen op zakelijke reizen
   - ○ Ja, overal (zowel op zakelijke als priv'e reizen of thuis)

4. Welke veiligheidsmaatregelen zijn er op deze apparaten getroffen?

   - ☐ Geen maatregelen
   - ☐ Gegevens moeten worden versleuteld

- ☐ Alleen gegevens met betrekking tot de reis staan op het apparat
- ☐ Data wordt niet op de laptop opgeslagen, maar is uiterlijk toegankelijk via VPN
- ☐ Laptops zijn leeg, de gegevens zullen op de bestemming worden gedownload

5. Welk protocol wordt gevolgd wanneer een draagbaar apparaat is verloren of gestolen?
   - ○ Er bestaat geen officiële procedure
   - ○ Het apparaat wordt op afstand gewist
   - ◉ Anders, zie beneden in commentaar
6. Screent u medewerkers alvorens u deze aanneemt?
   - ○ Bevestiging van CV en zakelijke referenties
   - ○ Bevestiging van de vermelde academische en professionele kwalificaties
   - ○ Officiële Verklaring Omtrent het Gedrag (VOG)
   - ○ Anders
   - ○ Geen screening
7. Is er een opleiding van het personeel met betrekking tot het omgaan met veiligheid en bedreigingen?
   - ○ geen training
   - ○ bij het begin van het arbeidscontract
   - ◉ Met regelmatige tussenpozen

DEEL 4: RISICOBEHEERSING

1. Welke van de volgende risicobeheersing activeiten onderneemt uw organisatie?

   ☐ Er is een bestaande analyse van mogelijke risico's en bedreigingen voor de organisatie voorbereidt

   ☐ Zwakke plekken en tekortkomingen zijn geïdentificeerd en worden geëlimineerd

   ☐ Een Computer Emergency Response Team (CERT) welke op IT security bedreigingen en incidenten reageert is opgezet

2. Heeft u een business continuity plan (bedrijfscontinuïteitsbeheer) in uw bedrijf opgesteld voor het geval een incident zich voordoet?

   ◉ Nee

   ○ Op dit moment niet, maar deze is in voorbereiding

   ○ Ja

   ○ Geen idee

3. Evalueert u de paraatheid van uw bedrijf tegen bedreigingen?

   ☐ Security audits vinden plaats

   ☐ Security oefeningen worden gehouden