ORGANIZATIONAL FACTORS AND PERSPECTIVES
FROM DECISION-MAKERS.

Jennie de Vries

Technical University Delft

Faculty of Technology, Policy and Management

September 2017

Electronic version available at http://repository.tudelft.nl

What drives cybersecurity investment?

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **System Engineering, Policy Analysis & Management**

Faculty of Technology, Policy and Management

by

Jennie de Vries

Student number: 4174496

To be defended in public on September 29 2017

Graduation committee

Chairperson	: Prof. Dr. Ir. P. van Gelder, section Safety and Security Science
First Supervisor	: Dr. Ir. W. Pieters, section Safety and Security Science
Second Supervisor	: Dr. Ir. M. Kroesen, section Transport and Logistics
External Supervisor	: J. Quist, EY

Summary

One of the leading perspectives from literature is that decisions about investments should be made based on a comprehensive cost-benefit analysis and that decisions are generally made based on the attacks and incidents that cause the organizations the greatest loss in monetary value. But main problem why many organizations do not undertake this sophisticated financial analysis or an comprehensive cyber risk assessment is because of the lack of available data about costs, benefits and the likelihood and impact of attacks (Rowe & Gallaher, 2006). So how do organizations determine how much they should spend on cybersecurity? The goal of this study is therefore to increase the understanding of this decision-making process and how organizational factors influence the decision-making process regarding cybersecurity investments. In organizations, decisions about the investment strategy are made by individuals. In this study it is expected that professionals who make decisions about cybersecurity investment on a daily basis are doing that with a certain perspective. Therefore the second goal of this study is to increase the understanding how perspectives from decision-makers influence these investment strategies. A perspective, according to Exel and Graaf (2005), is: "A person's viewpoint, opinion, beliefs or attitude". In this study a perspective is defined as how to deal with cyber risk and how this influences the decision how much to invest in cybersecurity. These goals result in the following main research question and sub-questions:

"What drives cybersecurity investment?"

(1) How is the cybersecurity investment decision-making process described in literature?
(2) What cybersecurity investment strategies exist in practice?
(3) What organizational factors influence these cybersecurity investment strategies?
(4) What are individual perspectives from decision-makers on cybersecurity investments?
(5) Can the identified investment strategies be explained from individual perspectives of decision-makers?

The first research question will be answered with literature research. The second and third sub question will be answered with data from of the Global Information Security Survey. This survey is conducted by EY among 1735 respondents, all CIOs, CISOs and other executives who are dealing with cybersecurity decision making on a daily basis. This dataset will be subjected to latent class analysis: "Cluster analysis is the art of finding groups in data" (Kaufman & Rousseeuw, 2005) . The goal is to identify clusters of groups who share the same objects, characteristics or behaviour of security professionals and identify the groups that are distinctively different from other professional segments. The latent class analysis (LCA) will therefore be used to identify clusters. The fourth and fifth sub question will be answered by means of the q-method. The aim is to find underlying individual perspectives of the cybersecurity decision-making regarding investments. The perspectives are unknown upfront and have to be found. In order to do so the q-methodology can be used to explore perspectives.

Four types of investment strategies are found with the LCA in the dataset of the GIS survey. The main differences between the strategies is the initial investment and the change of investment in the coming 12 months. These differences can be explained from the effect of organizational factors. In the first group there are two factors that could explain the found investment strategy. First the budget constraints are identified as a major concern and second is the factor that no incidents with serious financial damage happened that could explain that investment are not felt as necessary. In the second group the regulation has been indicated a major concern and could explain the investment behaviour, 80 percent of this group are large public organizations. It can be concluded that rules and regulation is a more important driver in public organizations than in private organizations. In the third group the risk identification could explain the

investment behaviour. Within this group all type of risks have a very high priority. And in the fourth group the type of industry and the client requirements could explain the high investment. These requirements could make that security receives a high priority. What is interesting is that the type of industry does not significant influence the cluster membership of the investment strategies, which is something that was expected upfront.

In addition four different perspectives are found with the q-method. Within these four groups there are several factors that could explain the certain perspective regarding cybersecurity investment behaviour. In the first group there is a concerned perspective and is characterised by its concern about unknown risks and social engineering. In the second group there is a resilient perspective and is characterised by its focus on risk avoidance, incident response and resilience. In the third group there is a hierarchical perspective and is characterised by its focus on the management and the unawareness of their employees. The fourth group has a flexible perspective and is characterized by aversion towards rules and regulation and its focus on the risk assessment. It is expected that organizations influence an individual's perspective, however the number of respondents was too low, which makes that the relation between organizational factors and the perspectives found is unclear. Although meaningful results are found from the analyses, there are some limitations too. In the LCA, the composition of the respondents is not perfect and there are some ambiguities with variables.

The additional value of this study lies mainly in the combination of the two different methods used to find different type of investment strategies, organizational factors that influence investment strategies and to find individual perspectives from decision-makers regarding cybersecurity investments. With the first research method a large dataset had been analysed (over 1700 respondents). Large datasets about investments, financial situations and organizational factors in cybersecurity are scarce. However, personal perspectives were not included in this dataset, therefore the second research method has been used, namely: the q-methodology. The q-method was to find individual perspectives of decision-makers and this has result in an explanation about a population of perspectives. A disadvantage of this method, however, is that result are not an explanation about a population of respondents. This means that with the results of the q-method one cannot say anything about a certain population. But with the Global information security survey dataset one could say something about the population. Therefore this combination shows additional value.

One cybersecurity investment strategy does not fit all. Organizations and individuals have different needs. The practical consequences is that there are different strategies for different target groups. Since these particular strategies and perspectives are known, one could divide organizations and individuals into these clusters and can act accordingly. For example, large public organizations can be classified into the second investment strategy. More research is, however, needed to whether these models can be used to make predictions and to the effect of organizations on individuals. Based on investment strategies their drivers and the individual perspectives it might also be possible to classify the groups in terms of level of security. The level of security can be expressed in a level of maturity. The maturity level can be useful in guiding an organization in the process towards the highest possible maturity level. It can also be used to evaluate an organization's current status of security. This combination of the strategies and perspectives with the maturity level of safety needs more research. In addition more research about the role of decision-makers within companies is important, so who makes decisions and for example how much influence does a CISO has within an organization? And how much does the investment strategy influence the actual implementation, and who determines the implementation strategy and can this person influence the investment strategy too? In addition more research is needed to determine the efficiency of security measures which could make it easier to determine where to allocate ones resources.

Table of Contents

1. Introduction and research questions

1.1.Introduction

In April 2011, one of the biggest data breaches took place. Sony PlayStation and Online Entertainment were hacked and 102 million customers' credentials were stolen (Shackelford, 2012). In total this cost Sony between one and two billion dollar directly. Sony is not the only company that was hit by cyber-attacks, according to recent numbers almost 80 percent of the US companies suffered from financial losses due to data and computer breaches (Meijeren, 2016). Some estimate that one in five to one in ten computers are infected with some sort of malware and often without the owner knowing (Bauer & van Eeten, 2009). Cyber-attacks are no longer a matter of if, but when. And the range of cyber threats are evolving very quickly.

The awareness of managers about their cybersecurity has increased as cyber-attacks now regularly cost firms millions. It makes organizations more aware of the cyber risks they are facing. However, in practice it seems very difficult to determine the cyber risks and to determine to what criminals we must protect ourselves from (Berg et al., 2014). This is mainly due to the fact that threats continue to evolve and threat landscapes are changing. In response organizations are improving their defences from very basic level in the '70 to more sophisticated, robust and formal processes nowadays (EY, 2016).

With this increase of the number of cyber-attacks organizations can face serious losses and need to consider investing in their security, how much they should invest and on what measures. However for organizations it is often not clear what investments are efficient and what investments provide "enough protection" (Bojanc & Jerman-Blazic, 2008). Many worry about not having enough budget, the right team with the right knowledge, the latest technology and on top of that many worry that they still suffer from a cyber-attack despite the fact that they did everything to prevent one. The EY Global information security survey states that almost 87 percent of board members and C-level executives said that they lack confidence in their company's level of security (EY, 2016).

But what does enough protection mean to a company and what does it take to get to that level of security? A rational approach to define the adequate security level involves identifying all risks, vulnerabilities, the probabilities of successful attacks and all the possible costs to mitigate the vulnerabilities (Dynes, Goetz, & Freeman, 2008). Then one of the biggest challenges is to consider how to defend against those potential cyber-attacks and how to best spend the resources.

The optimal level of security investments depends on the efficiency of the investment and therefore the costs should be lower than the security returns from the investments. However, multiple aspects make it difficult to determine the optimal level of security and determine this optimal level of investment. First is the limited availability of reliable (cost-effective) information, making that professionals make decisions based on incomplete data, or based on assumptions (Soo Hoo, 2000). This could lead to under- or overinvestment. Second is the difficulty in determining the risks one is facing and determining the actual impact and probability of a risk occurring due to the range of threats and evolving environment. How people think of risks, mostly guides their behaviour in how they make decisions regarding their security; therefore it is very important to get more understanding about this process. And last is that humans are not always the best decision-makers. Any decision in cybersecurity always involves some sort of trade-off, whether it is costs, time, convenience, resources, capabilities and so on (Singer & Friedman, 2014). For example,

security costs money, but it also costs time, or the tension between security and usability. In addition, humans can be susceptible to multiple biases in decision making, which makes this trade-off very difficult (Kahneman, 2011; Schneier, 2008)

One of the leading perspectives from literature is that decisions about investments should be made based on a comprehensive cost-benefit analysis and that decisions are generally made based on the attacks and incidents that cause the organizations the greatest loss in monetary value. But many organizations do not undertake this sophisticated financial analysis due to the lack of available data about costs, benefits and the likelihood of attacks (Rowe & Gallaher, 2006). So rarely does an organization make a comprehensive cost-benefit analysis or cyber risk assessment prior to the decision on investment. But how do organizations determine how much they should spend on cybersecurity? The goal of this study is therefore to increase the understanding of cybersecurity investment strategies and how organizational factors influence the decision-making process regarding cybersecurity investments.

In organizations, decisions about the investment strategy are made by individuals. In this study it is expected that professionals who make decisions about cybersecurity investment on a daily basis are doing that based on a perspective. Therefore the second goal of this study is to increase the understanding how perspectives from decision-makers influence this investment strategies. A perspective, according to Exel and Graaf (2005), is: "A person's viewpoint, opinion, beliefs or attitude". In this study a perspective is defined as how to deal with cyber risk and how this influences the decision how much to invest in cybersecurity.

As mentioned above, it is expected that investment strategies are influenced by an organization and by the individuals that take decisions about investments on a daily basis (Figure 1). It is also expected that individuals are influenced by the organizations they work in, for example due to the type of organization. In theory multiple normative methods are described to make the best decisions about investments and the allocation of resources to optimize ones cybersecurity.

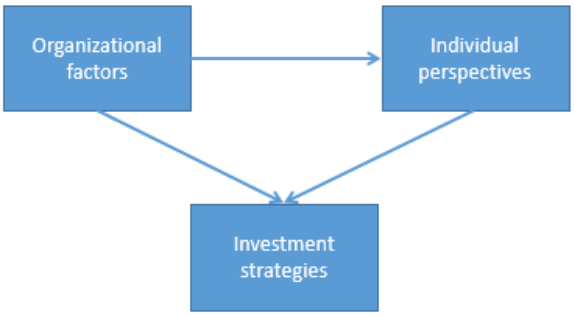

Figure 1 - Conceptualisation of influences organizations and individuals on investment strategies

However, despite the fact that there are multiple models and methods to assist in decision-making, there are still gaps in knowledge. The main problem is that those methods and models are in place to support decision-making and try to determine what the best decision is to take, but is mostly not possible to asses due to lack of reliable information. There is a gap between the normative decision-making theories about how decisions should be made and the use of these methods in practice.

What lacks in research is the exploration of the decision-making process regarding cybersecurity investments in practice, how organizational factors influence these investment strategies and the perspective of decision-makers regarding their investment in security. And how these organizations influence the individual perspectives. This results in the following main research question and sub research questions:

"What drives cybersecurity investment?"

1) How is the cybersecurity investment decision-making process described in literature?
2) What cybersecurity investment strategies exist in practice?
3) What organizational factors influence these cybersecurity investment strategies?
4) What are individual perspectives from decision-makers on cybersecurity investment strategies?

5) Can these investment strategies be explained from perspectives of decision-makers?

To answer these questions this research will explore the investment strategies and perspectives in two different ways (see figure 2). First a latent class analysis will be performed on the data from the Global Information Security Survey and second the Q-method will be performed in order to capture the possible individual perspective.

The Global Information Security Survey is a survey performed by the company EY amongst almost 1750 respondents. This existing dataset will be used to find different type of investment strategies and to explore what organizational factors might influence these investment strategies.

As mentioned above it is probable that humans make decisions subject to their personal perspectives. The Q-method will therefore be used as an addition and to examine if these investment strategies can be explained from individual perspectives. The literature research is to support both these methods. The different research methods will be explained in chapter 2.

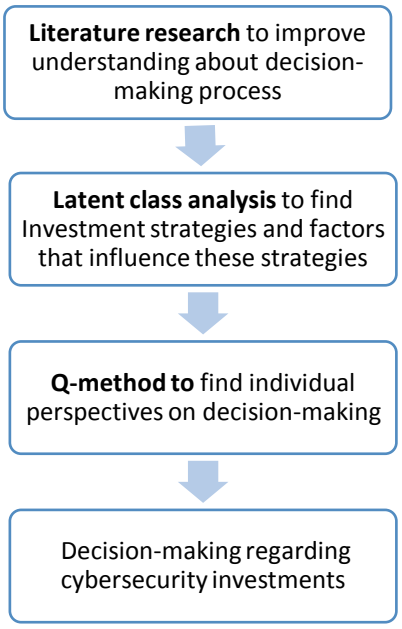

Figure 2 - Research methods

1.1. Relevance of the project

In literature the decision-making regarding cybersecurity investments is a rather new subject. Very little is known about the drivers behind the decision-making in combination with cybersecurity. Multiple research has been done about financial models and methods to justify cybersecurity investments, such as the Net Present Value, Return on Security Investment, Return on Investment and the Annual Loss Expected method. However as already mentioned above the inputs for these type of quantitative analysis are very difficult (Rowe & Gallaher, 2006; Soo Hoo, 2000).

This thesis attempts to gain more insight into those drivers and decision-making theory regarding cybersecurity investments. Most studies that have been done focus on the question what the best decision is that can be taken. Not many researchers have actually take this step back to investigate the drivers behind those decisions. So assessing the underlying perspectives is scientifically relevant.

This research tries to increase the information that is available about how decision-making in practice is being done. It tries to find groups which have shared investment strategies, drivers or have a shared perspective on their cybersecurity investment decision-making. The benefits of this clustering is that it is a way to describe complex behaviour and gives better understanding of that behaviour. This allows design of tailor-made policies suited to the specific needs of various clusters. Policy-making based on these outcomes can to be examined in future research or can be performed by EY. Expected outcomes are for example that in the public sector investments are being done based on rules and regulation, and based on those type of outcomes one could tailor policies towards different clients.

In this study the Global Information Security Survey is used for analysis. This is a worldwide survey and each year almost 1700 participants are willing to cooperate, making it a very valuable dataset. With the help of this study and analysis it can be determined whether subjects are missing in this survey that could be of

importance. And if so, these matters can be added to the survey next year, which can improve the dataset and even more information can be obtained from this survey.

De Wit (2017) states: for the security of an organization we are depending on the judgement of one or several security professionals. Those security professionals decide what measures to take, and what level of security is acceptable. If a judgement is based on wrong or unreliable data (which happens often, as mentioned above) this could lead to bad or wrong decisions by underestimating the risks we are facing. So this means that a decision made by one or several security professional has impact on an organization as a whole but also on the society. For example organizations in public sectors such as health care who need to take care of the protection of personal data. More understanding about the decision-making process of those security professionals could therefore affect the whole society.

1.2. Structure of study

The structure of this study is as follows. First, in chapter 2, the research methods will be explained. This explains the mutual relationship between the methods and explains how they will be performed step by step. Thereafter, in chapter 3, the results of the literature research are described. This explains the decision-making process in cybersecurity. This also forms the framework which is used for the latent class analysis and for the q-method. After that in chapter 4, the results of the analysis of the Global Information Security Survey dataset will be explained and in chapter 5 the results of the Q-method will be explained. Finally it will provide conclusions, a discussion, recommendations, critical remarks and future research in chapter 6.

2. Research methodology

This chapter explains the different research methods used for this study. The following methods are used to answer the research questions:

Literature study	Sub question 1: How is the decision-making process in cybersecurity investment described in literature?
Latent class analysis	Sub question 2: What cybersecurity investment strategies exist in practice? Sub question 3: What organizational factors influence these investment strategies?
Q-methodology	Sub question 4: What are individual perspectives from decision-makers on cybersecurity investment strategies Sub question 5: Can these organizational factors be explained from individual perspectives of decision-making?

2.1. Literature study

Sub question 1: "How is the decision-making process in cybersecurity investment described in literature?" will be answered by means of a literature study. The literature will be gathered via the following scientific search engines Google Scholar, TU Delft Library and Scopus. A variety of search terms can be used like: cybersecurity, risk management, investment, decision-making, strategy, investment strategy, cyber resilience, security, safety, cyber space, psychology of security, drivers, cyber insurance and a combination of these keywords. The table in appendix A shows which search terms are used for each search-engine. Some articles are also used for the collection of literature and is indicated as a source and the title of the article found. By means of the literature research it is expected that a framework will be made which explains the decision-making process in cybersecurity investments. This framework will then be used as input for the latent class analysis and the q-method.

2.2. Latent class analysis

The second sub question: "What cybersecurity investment strategies exist in practice?" and the third sub question: "What organizational factors influence these investment strategies?" will be answered with the result of the Global Information Security Survey. This survey is conducted by EY among 1735 respondents, all CIOs, CISOs and other executives who are dealing with cybersecurity decision making on a daily basis. This survey tries to find out how organizations deal with cybersecurity issues, how they prepare for cyber threats coming, how to guard themselves against cyber-attacks, how they react and recover and how much they invest and expect to invest. These 1735 respondents are from all over the world and from a variety of industries (EY, 2016). The following section will first explain the type of analysis and then it will explain the how the data is used for this type of analysis.

To reveal different investment strategies the latent class analysis is used. The latent class analysis aims to find meaningful groups of people that are similar in their responses on measured variables (Magidson & Vermunt, 2004).

As Kaufman states: “Cluster analysis is the art of finding groups in data” (Kaufman & Rousseeuw, 2005). The goal is to identify clusters of groups who share the same objects, characteristics or behaviour of security professionals and identify the groups that are distinctively different from other professional segments (Kaufman & Rousseeuw, 2005). Traditional cluster techniques, such as K-means uses algorithms to assign all cases to ‘k’ clusters, however one of the major problems with this techniques is that the cases are assigned deterministically to clusters (Magidson & Vermunt, 2002). The number of clusters has to be decided upfront and the class assignment is depend on the position of the clusters that is assigned upfront. This could eventually lead to wrong classification.

The latent class analysis has several advantages over traditional clustering techniques (Magidson & Vermunt, 2002):

- Uses probability-based classification. The latent class method uses model-based posterior membership probabilities estimated by maximum likelihood to classify clusters (Magidson & Vermunt, 2002). The cases are classified into clusters by calculating the chance of a case belonging to a certain cluster. The probability of belonging to a clusters is based on the combination of observed indicators and the covariates.
- Variables do not have to be standardized and variables can be of mixed scale types (Magidson & Vermunt, 2002). The latent class analysis is relatively easy to deal with variables of mixed measurement levels. Both simple and complicated distributions can be used for the observed variables within clusters. The GISS dataset consist of a great combination of types of variables (nominal, ordinal, continuous and count variables). Therefore the traditional cluster analysis is not possible. In addition, when using traditional cluster methods variables must be standardized, while with latent class analysis this is not necessary.
- Latent class analysis is not as sensitive to missing data as traditional analysis (Magidson & Vermunt, 2002). The latent class analysis differs in the way in which it deals with missing values to the traditional cluster analysis. The GISS data has multiple missing values in many rows. The cluster analysis will delete a row if a missing value exists, resulting in too much data loss. With the latent class analysis, however, missing data is not a major problem. It is not as sensitive to missing data as traditional cluster techniques which makes is easier to classify a respondent into a segment when some of the data is not available.
- Latent class analysis uses statistical tests to determine the number of clusters instead of determining the number of clusters upfront.

It is expected that the identified groups, who have for example shared needs, attitudes, demographics, or behaviour, have a shared investment strategy regarding their cybersecurity. The benefits of the clustering are that it is a parsimonious way to describe and capture complex behaviour and gives better understanding to that behaviour due to holistic profiles. The expectation of the outcome of this research is to identify main organizational factors that significant influence these different type of investment strategies. For example an outcome could be that in the public sector less investments are being done compared to private sector organizations. And based on those outcomes one could tailor its policies towards different clients.

The latent class analysis will be performed with the data analysis tool Latent GOLD.

Figure 3 shows a conceptual model of the latent class analysis. The model consist of multiple indicators (A,B,C,D), the latent classes (X) and covariates (Z_1, Z_2). To be able to assess whether respondents have different investment behaviour the latent class analysis is used.

The indicators are dependent variables that are used to define or measure the latent classes. Indicators can be treated as nominal, ordinal, continuous, Poisson count, or binomial count (Vermunt & Magidson, 2005). An example to find investment strategies an indicator is the amount of money spent on cyber security within an organization. The covariates are variables that could have an influence on the investment behaviour. The covariates that need to be included in the model are to be found in the literature study in chapter three. These variables are variables that are used to describe or predict the latent classes.

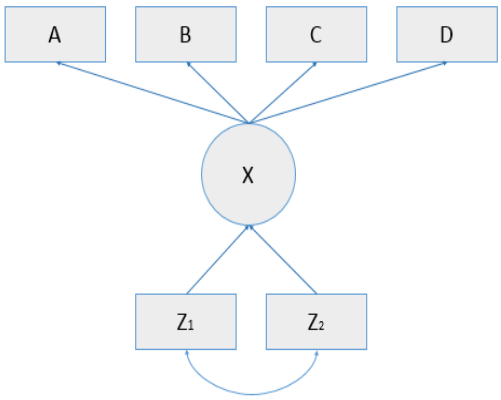

Figure 3 - model latent class analysis

Covariates can be treated as nominal or numeric and can be active or inactive. Active covariates are used to predict cluster membership. Inactive covariates do not influence this cluster membership, but are included to give more insight in the composition of the clusters (Vermunt & Magidson, 2005). An example of covariates are organizational factors such as the size of a company, the type of industry or the revenue of the company.

The reason why these factors could influence the investment in cybersecurity is explained in chapter 3: Dimension of cybersecurity decision-making. This chapter elaborates on this decision-making process and the most important factors that can ultimately affect the investment. This list of factors is based on the given dataset as mentioned above, and it may not be complete.

In chapter 4: the latent class analysis, the indicators and covariates will be explained in detail as well as the operationalization of these variables. And it discusses the sample composition of the Global Information Security Survey, the final latent class model and the results.

The dataset is a combination of the six types of variables (Symmetric binary, asymmetric binary, nominal, Ordinal, Interval, Ratio). For the latent class analysis a trade-off needs to be made when selecting the number of segments. What needs to be prevented is the risk that the diversity that is identified is meaningless in diversity.

2.3. Q-Methodology

The fourth sub question: “What are individual perspectives from decision-makers on cybersecurity investment strategies? And the fifth sub question: “Can these organizational factors be explained from individual perspectives of decision-making?” will be answered by means of the q-method. The aim is to find underlying individual perspectives of the cybersecurity decision-making regarding investments. It is expected that several organizational factors will be found based on the GISS dataset that influence the investment strategy. To investigate whether there might be individual perspectives that influence these strategies and the decision-making regarding cybersecurity investments, a technique to identify perspectives will be used. Therefore the third question will be answered with the called q-method.

The perspectives are unknown upfront and have to be found. In order to do so the q-methodology can be used to explore perspectives. Respondent need to rank different statements from their point of view with a quasi-normal distribution, so for example from most agree to most disagree (Exel & Graaf, 2005). This ranking of the statements represents an individual’s perspective on the topic and eventually this method will focus on the range of viewpoints that belong to groups. This makes it possible to get more understanding of the perspectives of security professionals on cybersecurity investments.

The combination of the statements about decision-making regarding cybersecurity investments is the particular perspective. The statements form the total story about the decision-making in cybersecurity and the ranking of these statements by individuals forms their perspective.

The researcher does not imply her personal statements and use them as a q-set. It is not possible to be create a really complete set of statements, as there is always something else to be said. But the set should contain a representative condensation of information (Watts & Stenner, 2005). This method does not impose meanings or statements upfront, but it asks the participant to decide what is meaningful and hence what has value and significance from their perspective, and therefore the participants apply their own opinion to the statements (Watts & Stenner, 2005). This method focusses on the range of viewpoints that are favoured by specific groups of participants (Watts & Stenner, 2005). In addition the interviewer can ask the participants for the reasons why he/she has ranked the statements in a certain way. This is especially important for the statements on both extreme ends, in this way one can discover the underlying motivation.

The q-method will consist of the following steps: the definitions of the concourse, the development of the q-sample, the selection of the p-set, the q-sorting and the interpretation of the results (Exel & Graaf, 2005). For this method only a small group of respondents is needed in contrast with R methods. It will be a strategic selection of people that are expected to have a different perspective. The steps of the q-method are explained in more detail in chapter 5, with the results of the method. The steps are explained in more detail in chapter 5: Q-methodology which also includes the final model and results. This method will result in different perspectives and therefore makes it possible to answer the sub-question.

To summarize, the following relations will be investigated with the following research methods. See figure 4 below.

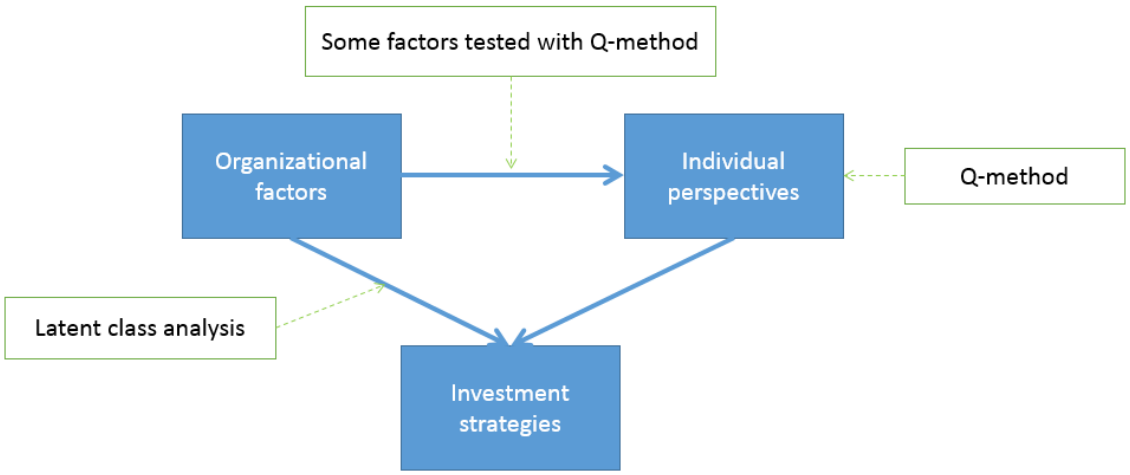

Figure 4 - Research methods used

3. Decision-making process cybersecurity investments

Cybersecurity is explained as: "Being free from danger or harm caused by the malfunction or failure of ICT or its misuse. Danger or harm through misuse, malfunction or failure can consist of limited availability and reliability of ICT, breaches in the privacy of information stored in ICT or damage to that information's integrity" (Berg et al., 2014). Cybersecurity concerns the protection from threats that use a cyberspace. Such threats could target information assets and therefore information security can be seen as a part of the cybersecurity. (Refsdal, Solhaug, & Stolen, 2015). However, information security could for example also be securing data which is on paper and is therefore not cybersecurity. In this research the focus will be on cybersecurity and is therefore not limited to the protection of information assets only. In cybersecurity the threat landscape is wider and could include assets such as life, health, reputation, revenue and so on.

Organizations should invest in cybersecurity to protect against events such as risks of loss, misuse, disclosure or damage, with uncertainty regarding the probability of the events. This could mean that one decide where to allocate the resources to mitigate the risks and that investments try to mitigate the risks of a negative event. Decision-making, risk-management and investment strategies are therefore connected to each other (Beissel, 2016).

This chapter is to explain different types of investments support methods and the problems it entails when using those methods in practice. After that it will elaborate on the risk management as a method to deal with complexity and to support the decisions regarding investments. And then it will discuss the role of humans in the complex decision-making process. And finally it shows a framework which shows how decisions in cybersecurity investment could be made in practice and what aspects could influence this in practice.

3.1. Investment strategies in cybersecurity

Despite the fact that average loss per organization is over 2 million US dollar, many are not adequately investing in information and cybersecurity (Gordon & Loeb, 2002). Numerous research has been done on models and methods to justify those security investments. Most of these are financial models and methods.

But what is the optimal level of investment? Every organization will have some level of security. Pure economically the optimum level of investment is where the marginal costs of increased security is equal to the marginal decrease in costs due to incidents (Dynes et al., 2008). However for this method organizations need full information, they may know how much they spend on their security but the true costs are very difficult to determine (Dynes et al., 2008). For example some costs are rather concrete such as time spent to recover, other costs are less tangible such as reputation damage expressed in monetary loss, which makes this very difficult to determine.

Gordon & Loeb (2002) proposed an economic model that determines the optimal amount of investment in information security. They state that for this optimal level of investment, organizations must make a trade-off between the costs and benefits of the investment. The investment will increase if the vulnerability increases. However, they state that the investment depends on the level of vulnerabilities and that little or

no security can be justified if the level of vulnerability is extremely low or high. However Gordon & Loeb are assuming that managers who allocate resources have all possible information available on vulnerabilities, threats and the impact of a breach. But especially in cybersecurity the lack of reliable data is one of the main reasons that economic models and methods are of limited use for evaluating the efficiency of cybersecurity investments (Rowe & Gallaher, 2006). In addition cyber threats and methods of attack are constantly changing and evolving rapidly and there is a reluctance towards public sharing of information on attacks and associated costs for organizations (Meulen, 2015). This reluctance to share information means that organizations might underestimate the risks of a cyber-attack and therefore make suboptimal investments. But it is the sharing of information that could lead to more accurate models and methods and enables organizations to make decisions based on full information (Bisogni, Cavallini, & Trocchio, 2011). Another aspect of Gordon and Loebs' financial model is that they only took the trade-off between costs and benefits into account. However, more aspect exist that could influence the decision-making, for example the economic incentives such as externalities that might arise when decisions made by one party affects others.

According to Rowe & Gallaher there are two aspects that obstruct the optimal investment level. The first, which is also mentioned above, is the lack of reliable information for quantitative analysis. The second is the externalities and public-goods nature of cybersecurity knowledge (Rowe & Gallaher, 2006). In addition, Rowe & Gallaher are one of the few researchers who actually take the step back to investigate the drivers behind the investment decisions. They mention that more information is needed about factors that influence an organization's investment and implementation strategies. They identified multiple drivers that could influence decision-making and put focus on the type of internal and external information that is needed in the decision-making process (Rowe & Gallaher, 2006). Some of their drivers is included in this study and explained in the next chapters. The question remains whether the trade-off between costs and benefits is the most important, and do decision-makers even make this trade-off since many react to an incident and spend whatever seems necessary at that point. Quantitative analysis is rather difficult, costly and in many cases they state: "Even impossible to acquire" (Rowe & Gallaher, 2006).

Rue et al. (2007) have done a comprehensive study on the analysis of financial models that help decision makers allocate their resources to cybersecurity, and also mention the fact that credible data is often missing, which makes the models less representative (Rue, Pfleeger, & Ortiz, 2007). Beside that there are multiple aspects that make the decision-making regarding investment difficult such as:

- The uncertainty about threats and vulnerabilities
- The determination of the consequences of a successful attack and the impact
- The uncertainty about the likeliness of an attack
- The uncertainty about the effectiveness of mitigation measures

"No single model by itself can provide a comprehensive justification for cybersecurity investments". In theory multiple models exist to support the decision-making, but due to the multiple difficulties it is unclear if the models can be used in practice. It is important to get more understanding how decision-makers and their organizations rely on those theoretic methods and models or that they rely on other drivers to find an acceptable strategy for investing in cybersecurity.

The investment strategies are now approached from an economic perspective. Economic incentives imply that any investment in security must result in more profits, because of increased profits or reduced costs. But how do organizations actually determine how much to invest in their security? Do they only have economic incentives or are their decisions also based on other drivers such as for example government regulations, costumer requirements or retaining reputation? Or do organizations perform comprehensive

risk analysis and base their investment on that? It is likely that organizations make decisions based not solely on their financial analysis, but on other perspectives as well. Those perspectives will not answer the question what the most optimal level of security investment would be, but gives insight in the decision-making process as a whole.

3.2.Decision-making process cybersecurity

To somehow deal with the uncertainty and the complexity of decision-making in cybersecurity investments, many organizations acknowledge the growing importance of risks and risk management. One can argue that risk-management is a way to deal with uncertainty and complexity and supports the decision-making. For example one tries to assign numbers/probabilities to a certain risk which supports ones decision. However, one could also argue that risk-management is a decision-making process itself. One way or the other, there are various risk management processes which are widely used in organisations (some more than others).

As mentioned above, the definition of cybersecurity is the **protection** of ones **assets** from **threats** that can cause any **harm**. These four aspects are most important in the decision-making process.

A growing number of organizations is using risk management as support for the protection of their assets from threats and determining where to allocate their resources. For the decision-making process risks need to be measured, weighed and compared. Then resources need to be allocated to manage these risks and need evaluation and argumentation. Cyber risk-management can be seen as a normative way of decision-making. It tries to support the decision-making to assign weights to the probability and impact of the risks and therefore tries to determine what the best decision is.

One could therefore argue that risk management is used to support the decision-making, but one could also argue that risks management is a decision-making process on its own. But where does the decision-making takes place within the risk management? During the risk management and risk assessment decisions are constantly made. One thing is clear and that is: risk management and decision-making is complex.

So let's start with the definition of risk. Multiple authors have a definition of risk; it comes down to the potential that something goes wrong and thereby causes harm or loss. Neil (2012) states that *:* "Risk is an event that can have negative impact" (Neil, 2012) and a cyber-risk is a risk that is caused by a cyber-threat (Refsdal, Solhaug, & Stolen, 2015). This could for example be a confidentiality breach caused by a malware attack or a loss of availability caused by a Distributed Denial-of-service (DDos) attack.

In the end all organizations are exposed to risks and must do some sort of risk management to control their security. The question remains how security professionals in organizations asses and evaluate risks. The risk management is a policy process in which risks are weighed and decisions about acceptable risks are made. Multiple risk management processes exist, which come down to the identification of risks, the assessment of risks and the treatment of risks. In addition there are feedback loops such as the monitoring and reviewing that are continuous processes, see figure 3.

To manage risks, one needs to understand risks. Therefore risk management can be used, this is the process of identifying, characterizing and understanding risk (Soo Hoo, 2000). The most standard risk assessment proposes to decompose risks into two components: (1) the probability of a risks occurring and (2) the impact a risk can cause, and then multiplying them to measure the size of the risk. However this basic method can be impractical and irrational when applied blindly and therefore not always sufficient for decision making (Neil, 2012). A more structured process is the assessment by NEN-ISO 31000 and consist of the following five steps: the context establishment, risk identification, risk analysis, risk evaluation and risk treatment (Refsdal et al., 2015). This seems a very transparent and objective process, however the decision making regarding cybersecurity are based on subjective decisions.

So first one has to decide what to protect, then one has to know what the threats and risks are, then one can manage the risks with a certain treatment strategy and this determines the investment strategy and eventually tries to prevent one from harm. This decision-making process explains how decisions about cyber risk 'should' be made in theory (figure 5). However, various external aspects could influence this decision-making process as well or have direct impact on the type of investment strategy. The next sections will elaborate on each aspect of this decision-making process.

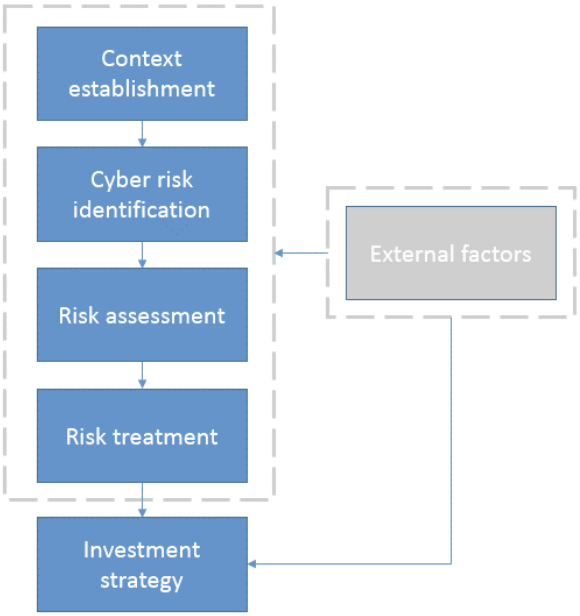

Figure 5 decision-making process cybersecurity

3.3.Context establishment

Today, information security is often explained as the protection or preservation of three key aspects of information: availability, integrity, and confidentiality (figure 6). It is related to the protection against the risks of loss, misuse, disclosure or damage.

- Availability: accessibility of information and the guarantee of reliable access to the information by authorized people (Rouse, 2017).
- Integrity: information must be precise, accurate, unmodified and consistent. Meaning that the data is modified only in acceptable ways, by authorized people, by authorized processes and is meaningful and correct (Li, Mao, & Zdancewic, 2003).
- Confidentiality: a set of rules that limits access to information, access must be restricted to those that are authorized only (Rouse, 2017).

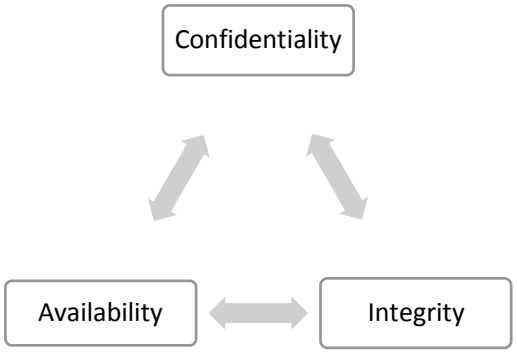

Figure 6 - key aspects of information protection

Context establishment is the first level in the risk assessment and defines the goals and objectives. The focus of an organizations could be on one of these aspects. For example, a manufacturing company with an industrial control system, confidentiality of their information might not be as important as the availability of their systems. A day without operating machines can cause major financial damage. Integrity, on the other hand, can be more important than the availability of a system for companies who want to keep their recipe a secret e.g. Coca Cola. So one should determine what assets need protection and how critical,

important or valuable these assets are. Typical cyber assets could be information infrastructure, services and networks. But one should take into account assets that can be harmed as well such as reputation, market share, revenue or legal compliance (Refsdal, et al. 2015). And to what degree do they require protection? After that one needs to define the risk scales, which means to determine the likelihood and the consequences. This could for example be monetary loss, however as already mentioned this can be very difficult to determine. So during context establishment one decides what the most important assets are and what type of protection they need.

To give more clarity in the type of assets, this is the question that is asked in the GIS survey and the corresponding possible answers. The GIS survey asked the respondents what information in their organization they consider the most valuable to cyber criminals and asked them to indicate the most important assets to their organizations. This could be for example: customer personal information, customer passwords, R&D information and board member personal information etcetera. So the risk management starts with the context establishment and is to determine the most important assets an organizations wants to secure. The focus could be on one of these assets or on all, or organizations do not focus on the context establishment at all. Figure 7 shows the first level of the decision-making process.

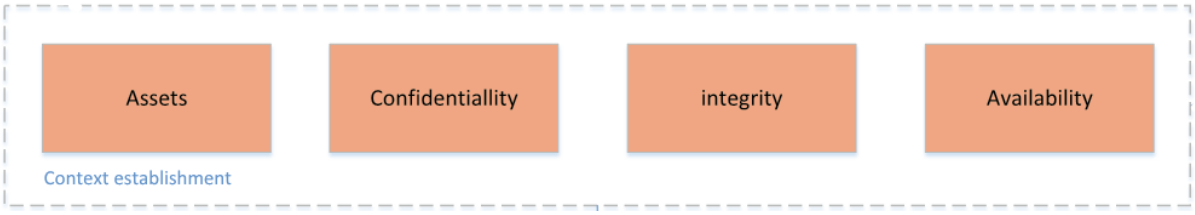

Figure 7 - level 1 context establishment

3.4. Cyber Risk identification

Risk identification is the second level: to identify threats, to understand how they may lead to an incident and to exploit vulnerabilities. As Refsdal et al, states: “Without assets there is nothing to harm, without vulnerabilities there is no way to cause harm, and without threats there are no causes of harm”. However risks contain uncertainty and uncertainty makes it difficult to identify, assess and manage the outcome of risk (Sahlin, 2012). According to Sahlin (2012) there are two reasons that cause uncertainty in risk, first uncertainty is caused by a lack of knowledge about the risk and second uncertainty is caused by too many unpredictable variables. However, one could also argue that risks are by their very nature uncertain and that one assigns probabilities to deal with this uncertainty.

In addition Sahlin (2012) mentioned that risk theories ask too much from the decision-makers because it demands perfect information. In practice there is no such thing as perfect information. It is very difficult to determine the cyber risks due to the fact that threats continue to evolve and threat landscapes are constantly changing (Berg et al., 2014). Additionally, not much data is available on threats since organizations are not willing to share information, do not store information or there simply is no information about the root cause (Dynes et al., 2008). So during the risk identification one decides what threats exist and what risks one needs to take into account.

Cebula & Young, (2010) attempts to identify the sources of operational cybersecurity risk into four classes: actions of people, systems and technology failures, failed internal processes and external events. Each of these classes are divided into subclasses which can be seen in the overview below (figure 8). In the GIS survey the respondents were asked who or what they consider the most likely source of an attack and which

threats and vulnerabilities have increased their risk exposure. Interesting is whether these factors influence the type of investment. In many organizations the focus is on operational risks to information and technology assets, although people and facility assets need to be considered too. Optimal risk management involves a balance between all types of risks (Cebula & Young, 2010), however it may happen that organizations focus too much on one of these subclasses. This division of risks can be useful to define different perspectives of professionals. For example a risk on a DDoS attack demands a different approach and investment than the risk of a malicious employees. The focus on one type of risk could drive a professional to invest in their security. Figure 8 shows the second level of the decision dimension in cybersecurity.

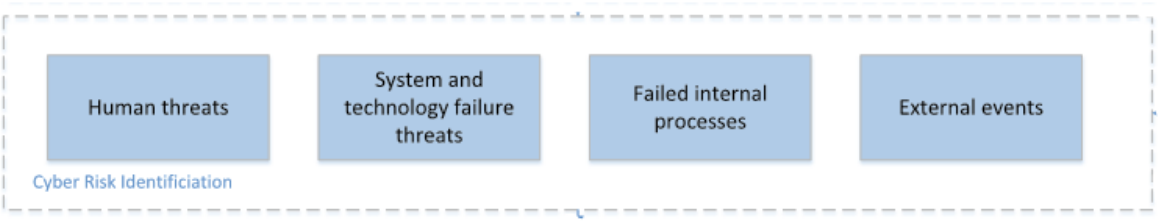

Figure 8 - level 2 cyber risk identification

1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Processes	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disasters**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
1.2 Deliberate	2.1.4 Obsolescence	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2.1 Fraud	**2.2 Software**	3.1.5 Information flow	4.1.5 Unrest
1.2.2 Sabotage	2.2.1 Compatibility	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.3 Theft	2.2.2 Configuration management	3.1.7 Service level agreements	**4.2 Legal issues**
1.2.4 Vandalism	2.2.3 Change control	3.1.8 Task hand-off	4.2.1 Regulatory compliance
1.3 Inaction	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3.1 Skills	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.2 Knowledge	2.2.6 Testing	3.2.2 Metrics	**4.3 Business issues**
1.3.3 Guidance	**2.3 Systems**	3.2.3 Periodic review	4.3.1 Supplier failure
1.3.4 Availability	2.3.1 Design	3.2.4 Process ownership	4.3.2 Market conditions
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Economic conditions
	2.3.3 Integration	3.3.1 Staffing	**4.4 Service dependencies**
	2.3.4 Complexity	3.3.2 Funding	4.4.1 Utilities
		3.3.3 Training and development	4.4.2 Emergency services
		3.3.4 Procurement	4.4.3 Fuel
			4.4.4 Transportation

Figure 9 - Classification of Cyber risks (Cebula & Young, 2010)

3.5. Risk assessment

Risk assessment is the third level of the decision-making process. The risk assessment consists of the risk analysis, the risk evaluation and the risk treatment strategy.

3.5.1. Risk analysis

During the risk analysis one tries to estimate likelihoods and consequences for the identified risks in the previous step. The estimation of the likelihoods is to determine the probability of an incident to occur and the consequences include the impact on the organizations, mostly expressed in monetary loss. However the predictions of consequences are very complex and dependent on multiple aspects and actors (Wit, 2017). What organizations for example do is security testing (penetration, vulnerability, system tests etc.) to explore possible outcomes of attacks, but this can only be executed for known risks. Some security risks we simply do not know or cannot imagine, the so-called “black swans”. This already leads to problems in the risk identification step. Another option is to make use of predefined repositories of attacks and vulnerabilities, however one always needs to adjust them to one’s own organization, with its specific targets and assets (Refsdal et al., 2015). In addition it can be very hard to estimate the likelihood of occurrence, since most of the times human intent and motives are involved in the threat. What makes the estimation of the probability difficult as well is the effect that people tend to underestimate the probability as mentioned above in the decision-theory section. So during the risk analysis one tries to decide what the probability and the impact of a risk is. This level is the risk assessment and includes the decisions that can be made based on the identified risks in the previous level. Figure 10 shows the third level of the decision dimensions: cyber risk assessment.

The focus during the risk assessment can be on multiple aspects. First the focus can be on the decision what risk to take into account and what risk one considers as less or more important. This may mean that an organization focuses only on a small number of risks they consider to be the most important. Second the focus could be on the likelihood and consequences. This means that an organization, for example, only takes risks into account with a high likelihood or with major consequences. The third focus may be on the level of acceptance and that this level of acceptance determines which risks to take into account. And last the focus could be on the countermeasures only. This could mean that an organization only considers the available countermeasures it has, and thus does not take the risks into account. In this focus on ‘countermeasures’, one could also focus on one type of measures. This is explained in the following section.

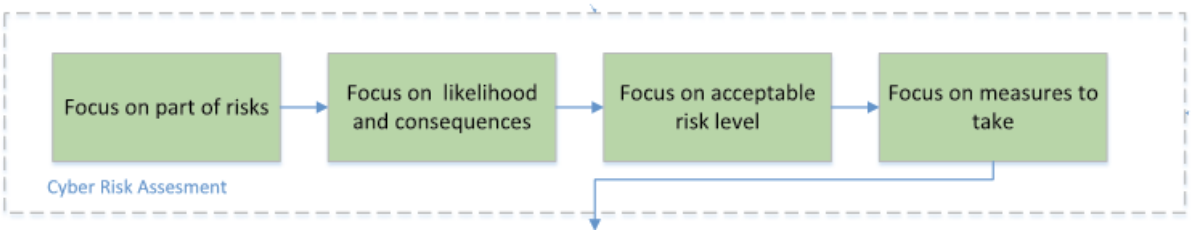

Figure 10 - level 3 Risk assessment

3.5.2. Risk evaluation and treatment

During the risk evaluation and treatment one needs to determine which risks should be treated and what measures to take. So during this step one decides on what risks to focus and what the acceptable level of risk is (figure 9). Organizations should at least be protected against the vulnerability identified in the abovementioned section to some level. This protection could for example be the installation of firewalls and the use of encryption. However, even with the best protection and security measures in place an

organization will not be 100% secure. According to Gordon, Loeb, & Sohail, (2003) losses from security breaches are always likely to occur.

In addition to the evaluation one also decides what treatment strategies can be used and what measures can be taken. This is also the step in which the resources will be allocated. This means that one decides where and how much to invest in the treatment strategies. This level includes the strategies in risk management for the treatment of risks and can be defined into the following four categories:

- Risk mitigation: reduce the cyber risk by means of technical, human oriented, legal or organizational means.
- Risk transfer: transfer of the risk to a third party. This could for example be an insurance company. For example, Gordon et al. propose a cyber-security insurance to reduce the risk of financial losses.
- Risk avoiding: avoid the risks by eliminating the risk cause and/or consequences. This often seems impossible to obtain.
- Risk acceptance: basically retains the risk and accept all possible losses. This often seems impossible due to regulations, which makes it impossible to ignore certain risks.

The focus may be on either one of these measures or can depend on the risks a company is facing. And based on these risks a company can determine which measures suits best. Figure 11 shows the fourth level

Figure 11 - level 4 risk treatment strategy

of the decision dimensions: the different treatment strategies.

Conclusion risk management

What can be concluded is that a risk is something that can, in theory, be measured and the task of risk management is to reduce the risk as much as possible. Then there is something like the perception of risks that is people's perspective about risks and their way of relating to them. In cybersecurity it is this measurement of risks that is very difficult so what is important is to get an idea how people estimate risks, how they make decisions and how they determine what risks are acceptable and what not.

As mentioned above, in the cyber risk assessment the decisions are made typically without information about the probabilities of the outcomes, the consequences and the likelihood of occurrence. So one could argue that it is decision-making under uncertainty. However one could also argue that risk is by its nature uncertain and risk management is used to deal with this type of uncertainty. So where are the decisions made during the risk management? During cyber-risk management and assessment multiple decisions are made. In the last step organizations try to determine how and what to invest. What can be concluded is that this decision can be influenced by the whole decision-process of cyber risk management, but organisations could also only focus on a small part of the risk management, so only this small part influences the investment strategy.

The question that remains is: does every organization make such a comprehensive risks assessment? In theory, risk assessment is used to support the best decision, but does it work and it is used in practice? For example, does the budget of an organization determine to what extend a risk assessment performed? And if it does, does that mean that smaller organizations make decisions not based on a risk assessment? How an individual use the risk assessment can be a perspective that a professional has on the decision-making.

So for example an individual only focusses on the cyber risks identification and only takes one type of risk into account: namely the risk of a careless employee. Then this individual only takes measures to deal with this risk and determines its investment strategy based on this risk only. Then this can be seen as a perspective. The next section will elaborate on the other aspects that influence the decision-making process or the investment strategy directly.

3.6. External factors

Risk management is often more difficult in practice than in theory. The standard cost-benefit calculations are almost impossible to perform. Thus, in considering the decision-making process it is expected that organizations are influenced by other factors as well. Or organizations might only perform a small part of the risk management process or focus on a few risks only. Examples of organizations that may not perform the whole risk management process are organizations that are heavily restricted with a fixed budget and can only cover vulnerabilities, or organizations that only invests in their cybersecurity to comply with rules and regulations. In the next section different factors that might influence the investment strategy of an organization are discussed, see figure 12. It starts with the economic factors, then the rules and regulation, reputation, and incident response.

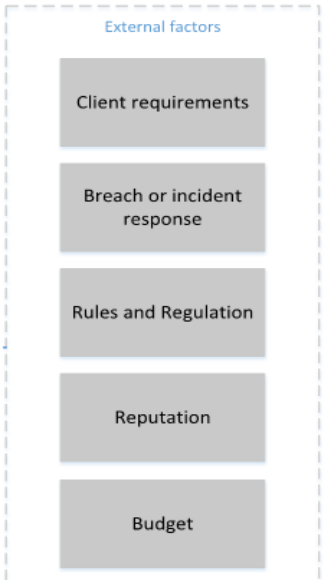

Figure 12 - External factors

3.6.1. Economic factors

Budget

According to Rowe & Gallaher (2006) only a few organizations determine their budget for cybersecurity through an extensive cost-benefit analysis and/or a risk management framework. As mentioned in section 3.2: investment strategies for cybersecurity as a business case is very difficult to attain. As Gordon, (2007) states this is due to the difficulties in assigning the benefits derived from cybersecurity and there are externalities associated with cybersecurity investments. As a result of these difficulties organizations might have insufficient budgets that cannot support what is needed for the desired acceptable risk level.

Fielder et al., (2016) also state that organizations can be heavily restricted with the available budget for cybersecurity. Most of the time this budget is insufficient to cover all the vulnerabilities that their system may have. That is why organizations have to make trade-offs regarding how they would defend their systems. They state that 86% of CISOs were concerned about their lack of sufficient funding to defend their systems. So a fixed budget can definitely influence the investment strategy.

Reputation damage

The consequences of cyber-attacks can go beyond organizations' material damage. Reputation damage could have more impact and in the end cost more money than material damage. For example in the financial sector it is vital to ensure the reliability of the organization. When there is a breach and the reliability decreases this has a direct impact on the reputation and market share. In the worst case scenario the service provided by the organization can no longer be sold. So negative publication will probably damage a firm's reputation and cause customers to lose confidence and could give competitors advantage (Almann & Kelly, 2008). Reputation could therefore also be categorized under economic incentives.

Client requirements

Client requirements can provide a strong incentive for organizations to invest in their cybersecurity (Michael P. et al. 2006). It could be possible that business relationships demand organizations to have certain cybersecurity hardware, software, policies, and procedures. In competitive markets, these customers may choose another party. Thus, the risk of customer-exit, in for example the financial sector, could be a strong incentive to secure against cyber-attacks (Sales, 2013).

Best practice

Since it is rather difficult to perform a satisfactory return on investment calculation for security spending multiple organizations use the best practice approach. This approach is simply said: the same kind of investment as your competitors (Almann & Kelly, 2008). This could result in the herd mentality, leading to investments in security measures which might not be efficient at all. Almann and Kelly (2008) give the example of firewalls: firewalls are a great success in the marketplace. However, most firewalls are not effective at all and there are many more measures that are much more effective. Firewalls have their success due to auditors who demand organizations to have one.

3.6.2. Rules and Regulations

Rowe & Gallaher, (2006) argue that regulations are one of the most often cited drivers affecting an organization's investment strategy. They conducted a survey in the US amongst multiple private organizations and stated that approximately 30% of their motivation for security was accounted for by regulatory incentives. Because of such regulations, professionals come to realize that they have to invest in their security in order to comply with the rules and regulations.

Kovacs, (2014) state that over the past three years organizations in the United States have increased their cybersecurity investments due to regulatory pressure. For example data protection and privacy laws are accelerating spending on IT security solutions. However, regulations could also have a negative impact on the security. For example, many spend a lot of effort on complying with regulations and this detracts from efforts to develop effective security capabilities (Dynes et al., 2008). Dynes et al. (2008) give the example that a security professional is now putting effort in assuring that the door to his data centre is of a certain thickness, rather than working on more effective security measures. One might argue that this regulation therefore misses its purpose. However several legislations give positive incentives to organizations to invest in cybersecurity, which they would not do otherwise. This is for example the European Network and Information Security directive, which aims at creating a common level of network and information security within Europe. The cooperation between the Cybersecurity Incident Response teams in the different member states is an important part of this (NCSC, 2016). For example companies with essential services are obliged to report infringements in their information system. With this directive the European Union aims to give organizations an incentive to keep their security at a certain level by requiring parties to take appropriate security measures and to report incidents. Terms as 'appropriate measures' however do not give sufficient support for multiple organizations because of the ambiguities of how they can meet requirements (Meulen, 2015). What could also happen is that organizations determine their optimal level of security based on Internal Standards Organization (ISO) 17799 or NIST 800 series guidelines (Gallaher et al. 2006). Meulen (2015) however states that multiple organizations do not recognize rules and regulations as their number one driver. They mention that institutions and legislators lag behind and that most legislation has a less adaptive character, because the process of creating it could take a long time. So governmental measures could be an incentive but need to be up to date.

3.6.3. Breach or incident response

Cybersecurity can be seen as an unnecessary investment or a burdensome cost on the organization, until a breach has happened. Organizations then may react to a breach and spend whatever it takes to solve the

problem. Cybersecurity incidents may attract a lot of media attention and can lead to reputation damage and customer exit as a result. Meulen (2015) states that media attention is an incentive for companies to invest in their security to prevent this negative attention. The tangibility of the risks is an important factor. Through the media attention, a risk suddenly becomes very tangible and makes that organizations take action.

Conclusion external factors

What can be concluded is that multiple factors besides the risks management process could influence the investment behaviour of professionals. As mentioned above, the risk management process could be seen as a normative tool to deal with cyber risks and to determine the optimal level of investment. However, in practice risk management is complicated and these external factors indicate this. These external factors need to be considered in further research, in chapter four and five is explained how these factors are included in both the analysis.

3.7.Decision-making under uncertainty

In the section above risk management is explained, which could be explained as decision-making under uncertainty, since risks are in their nature uncertain. But risk management could also function as a normative tool to support security professionals in making decisions regarding their investment strategy and to support the uncertainty in decision-making. Security professionals doing these risks assessments on a daily basis might be susceptible to decision-making biases. These susceptibilities will be explained in this section and will be considered in further analysis to determine if this susceptibility is visible in practice.

Numerous research is done on decision-making in general and decision making under uncertainty. The core of most decision theories is that: "If a person is rational, she will choose an option that maximizes what she expects to gain from her choice" (Roeser et al., 2012). Decision making theories shape the way one thinks about risks and how one 'should' rationally choose from risky options (Roeser et al., 2012).

Johnson and Busemeyer (2010) distinguish two types of decision-making theory. First is the normative focus on decision making, which tries to determine what the 'best' decision is to take in any given situation. The second is the descriptive focus which tries to understand the reason why people make certain decisions (J. G. Johnson & Busemeyer, 2010). This research will focus on the latter. In the first focus one tries to treat decision problems in expectation terms, and derive solutions that maximize the expected utility. However, in the assessment of cyber risks this quantification is difficult which makes the normative decision-making difficult. Humans might therefore make suboptimal decisions. As mentioned above: this research tries to describe how humans (in this research cybersecurity professionals) make decisions, rather than trying to find the ideal decision for any situation.

A well-known descriptive decision-theory is the: "Prospect theory" by Kahneman and Tversky (Kahneman & Tversky, 1979). This theory describes the way humans choose between alternatives that involve risk. It describes biases in decision making people are susceptible to. The "certainty effect" is the phenomenon where people overweigh outcomes that are considered certain, relative to outcomes that are probable. This means that people are influenced if there is a certain gain at stake. It shows that people rather choose something with a certain outcome, than something with an higher utility but with an uncertain outcome (Kahneman & Tversky, 1979). However, in cybersecurity the outcomes are mostly not certain and if something happens, a breach for example, the outcome is reversed and the gains are replaced by losses. So what happens then? People tend to behave differently when the choice concerns a certain or uncertain loss. The so-called "reflection effect" implies that people are risk seeking when the outcome is negative and they

prefer a loss that is probable over a smaller loss that is certain (Kahneman & Tversky, 1979). With the losses of a security breach in mind this reflection effect might influence the decision-making in choosing the option with a higher uncertainty, even though it does not have the best outcome. The certainty effect might influence the decision-making as well, since reducing the probability of an incident can be felt like as a win. However "reduced security incidents" is less tangible, since you do not know what would have happened if you did nothing. So what might happen is that professionals tend to choose security measures with certain outcomes. Another effect that Kahneman and Tversky (1979) describe is the "Value function" and implies that we tend to overweight and overestimate the probability of rare events. As mentioned above, decisions about security risks could involve weighing probabilities and impact and according to this value function those probabilities can be perceived higher than they actually are. Which therefore could lead to overrating security risks and other decisions.

What can be concluded is that the certainty effect, the reflection effect and the value function effect can all influence the way we deal with risks in cybersecurity and the way we make decisions in cybersecurity. These effects will be considered during the question why professionals decide to invest in cybersecurity. In addition it will be considered if these effects exist in practice.

3.8. Decision-making process framework

Based on the literature study in this chapter the final framework the decision-making process in cybersecurity is created, see figure 13. The final framework shows the decision-making process of cybersecurity investments as it is described in literature. This shows how decisions about investment could be made in practice and what aspect could influence these investment strategies, and it is not to show how decisions should be made to make the best possible investment.

Risk management should start with the first level and then continue with the second and so on. However, in practice decisions can be made throughout the whole process. Decision makers may focus on a particular aspect of the whole process and external factors influence the decision-making process as well. In this study, this focus on a particular aspect is a perspective on the decision making regarding cybersecurity investments. For example, an organization could be heavily restricted by its budget and determine their investment strategy based on this budget and try to allocate their resources as efficient as possible.

This framework has different effects for the latent class analysis and for the q-method. The latent class analysis will be performed with an existing dataset. The framework will be used to select variables from the dataset and include them in the analysis. This means that from this dataset variables will be used that fit in this framework. What could happen is that not all dimension will be covered by the dataset. An example of a variable for the second dimension: cyber risk identification is for example: "The threats and vulnerabilities that have most increased the risks exposure over the last 12 months". How this variable and others are used in the latent class analysis will be explained in chapter 4.

The second analysis will be performed by means of the Q-methodology. For the Q-methodology, as mentioned above, statements will be created. The framework will be used to select an equal number of propositions per dimension. This structure forces to select statements widely different from one another and makes the q-set broadly representative. The statements represent the best possible extent of perspectives regarding cybersecurity investments. The number of statements that are included in the analysis will be explained in chapter 5.

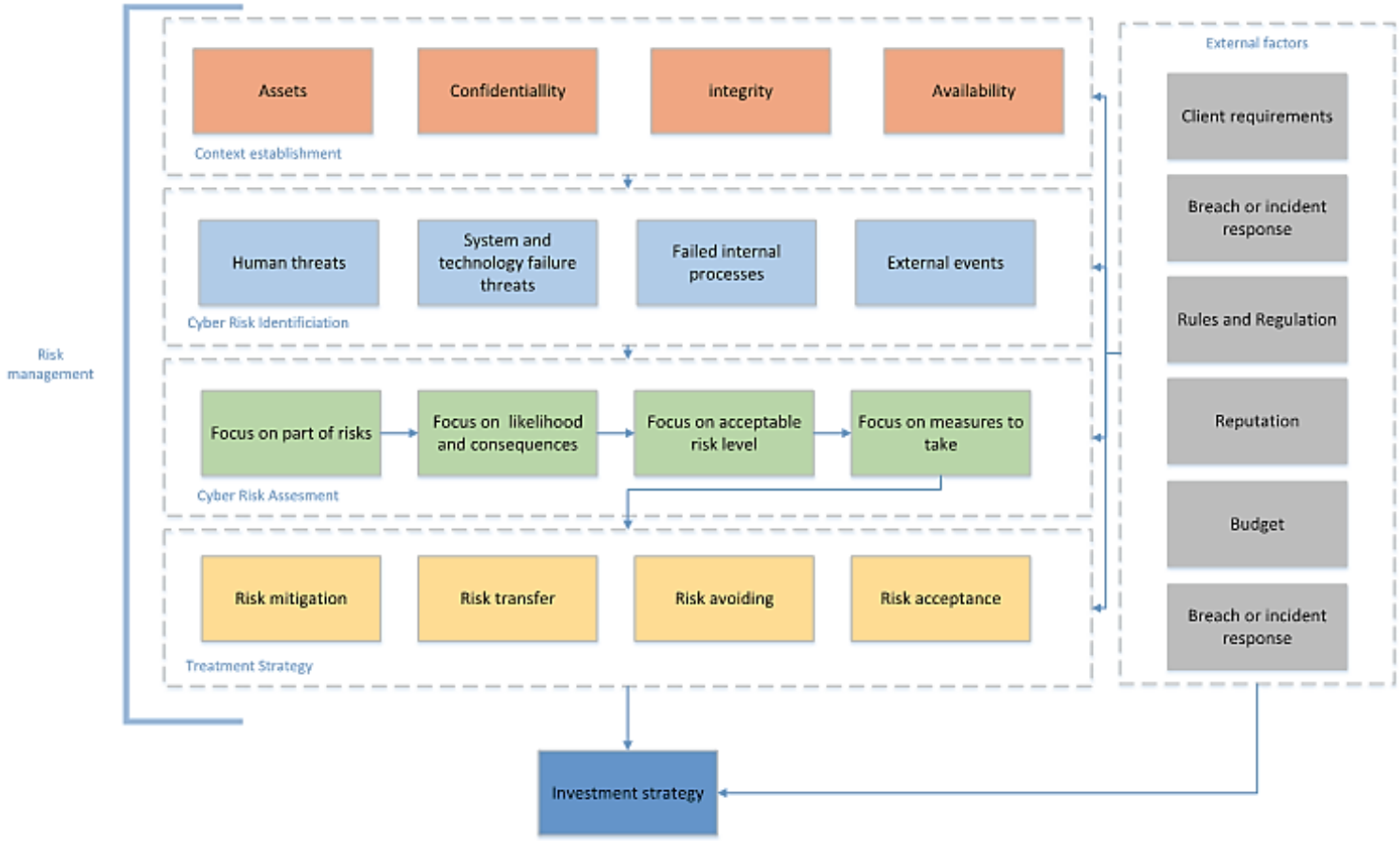

Figure 13 – Framework with influences on cybersecurity investment decision-making process

4. Latent class analysis and results

To be able to assess whether respondents have different investment behaviour the latent class analysis is used. This chapter is to explain the methodology of the latent class analysis, the variables and to describe the final model and results.

This chapter first discusses the sample composition of the Global Information Security Survey, and after that it discusses the operationalization of the indicators and other variables that are used in the model. Based on the availability of the data and on the previous chapter about the dimensions of the decision-making the variables are included in the model.

Finally this chapter discusses the latent class model estimation and the method to determine the number of latent classes. After that the chosen model will be presented and the identified classes are described.

4.1. Sample composition

The Global Information Security Survey (GISS) is conducted by EY among 1735 respondents, all CIOs, CISOs and other executives who are dealing with cybersecurity decision making on a daily basis (EY, 2016). Table 1 shows an overview of the composition of the survey. EY's 19th GISS captures the responses of 1735 C-suite information security professionals, representing many of the world's largest and most recognised global companies. The research was conducted between June-August 2016 (EY, 2016). The number of respondents by position is shown in table 1.

Important to notice is that for the variable: Number of employees, a scale has been used with 10 different options from less than 1000 employees to 100.000 and above. According to international standards a small company has less than 50 employees, a medium sized company has between 50 and 249 employees and a large sized company has greater than or equal to 250 employees (European Commission, 2017). It is unfortunate that less than 1000 employees is not clearly specified in the survey. However, in order to make a distinction, the number of employees less than 1000 is referred to as small and medium sized companies and everything above will be referred to as large companies, so this variables is transformed into three different options.

What also should be noted is that in the composition of industries many respondents are in the financial sector. This is probably due to the fact that many clients of EY are in this sector and this survey is a representation of the clients of EY. The number of health organizations for example is relatively low compared to the other industries.

It is expected that the respondents are independent from each other because of the fact that the respondents are all from different companies or organizations.

Table 1 - GISS composition

Variable	Type	Number	Percentage
Total number respondents		1735	
Respondents by position	Chief information security officer		23%
	Information Security executive		12%
	Chief Information Officer		12%
	Information technology executive		11%

	Chief Security officer		3%
	Internal audit Director		3%
	Chief Technology officer		3%
	Network/system administrator		3%
	Business unit executive		2%
	Chief financial officier		1%
	Chief risk officer		1%
	Other		27%
location	Japan	52	3%
	EMEIA	662	38%
	APAC	365	21%
	Americas	656	38%
Type of organization	Private	557	0%
	Public	556	32%
	Government or Non-profit	174	10%
Total spending on cybersecurity	Less than US1	804	46%
	Between 1 and 2	284	16%
	Between 2 and 10	281	16%
	Between 10 and 50	143	8%
	Between 100 and 250	22	1%
	More than 25	136	8%
Change of security budget coming 12 months	Increased by more than 25%	190	11%
	Increased between 15% and 25%	274	16%
	Increased between 5% and 15%	479	27%
	Stayed approximately the same	533	31%
	Decreased between 5% and 15%	57	3%
	Decreased between 15% and 25%	12	1%
	Decreased by more than 25%	19	1%
	Don’t know	141	8%
	Missing	45	3%
Change of security budget last 12 months	Increased by more than 25%	264	15%
	Increased between 15% and 25%	247	14%
	Increased between 5% and 15%	412	24%
	Stayed approximately the same	600	34%
	Decreased between 5% and 15%	38	2%
	Decreased between 15% and 25%	13	1%
	Decreased by more than 25%	24	1%
	Don’t know		0%
	Missing	42	2%
Total financial damage	Between 0 and 100.000	550	31%
	Between 100.000 and 250.000	160	9%
	Between 250.000 and 500.000	67	4%
	Between 500.000 and 1 million	35	2%
	Between 1 and 2.5 million	23	1%
	Above 2,5 million	18	1%

	Don't know	311	18%
	Had no information security incidents that resulted in any financial damage	528	30%
Type of industry	Wealth & asset management	30	2%
	Transportation	39	2%
	Telecommunication	70	4%
	Technology	125	7,1%
	Retail and wholesale	78	4,5%
	Real estate	50	2,9%
	Provider care	3	0,2%
	Professional firms & services	55	3,1%
	Private equity	2	0,1%
	Power and utilities	81	4,6%
	Other	104	5,9%
	Oil & gas	48	2,7%
	Mining & metals	36	2,1%
	Media and entertainment	57	3,3%
	Life sciences	29	1,7%
	Insurance	127	7,3%
	Healthcare	69	3,9%
	Government & public sector	105	6,0%
	Diversified industrial products	82	4,7%
	Consumer products	105	6,0%
	Chemicals	16	0,9%
	Banking & captial markets	349	19,9%
	Automotive	47	2,7%
	Airlines	16	0,9%
	Aerospace & defence	12	0,7 %
Number of employees	Small & Medium <1000	424	24,2%
	Large >1000	831	47,5%
	Missing	495	28,3%
Total Revenue	Small <10 million	75	4,3 %
	Medium 10-50 million	106	6,1%
	Large > 50 million	942	53,8%
	Missing	627	35,8%

4.2.Operationalization of variables

The model consist of indicators, latent classes and covariates. This section discusses the indicators and the covariates. The indicators are dependent variables that are used to define or measure the latent classes. Indicators can be treated as nominal, ordinal, continuous, Poisson count, or binomial count (Vermunt & Magidson, 2005). The covariates are variables that could have an influence on the investment behaviour. These factors are described in the framework discussed in section 3.7. Covariates are variables that may be used to describe or predict the latent classes and can reduce the classification error. Covariates can be treated as nominal or numeric and can be active or inactive. Active covariates are used to predict cluster membership. Inactive covariates do not influence this cluster membership, but are included to give more insight in the composition of the clusters (Vermunt & Magidson, 2005).

Figure 14 shows the conceptual latent class model which includes the indicators and covariates. So based on the literature study, it can be concluded that five different categories can have a significant influence on the investment behaviour. These are the context establishment, the risks identification, the risk assessment, the risks treatment strategy and the external factors. In addition it is expected that organizational characteristics such as size, total revenue and type of industry could have a significant influence on the investment behaviour. Based on the available variables in the GIS dataset the following dimension, besides organizational characteristics, are included: cyber risk identification and external factors. The other dimension are not covered in the GIS dataset. These dimension will be covered with the q-method as second analysis. In appendix C the GIS survey questions are shown which include these variables.

For three dimensions there is no available data in the given dataset. First, the dimension context establishment. The most important type of assets would for example have been an interesting variable to include in the model. However, this information is not available. Second and third, data for the dimension risk assessment and the risk treatment strategy are lacking.

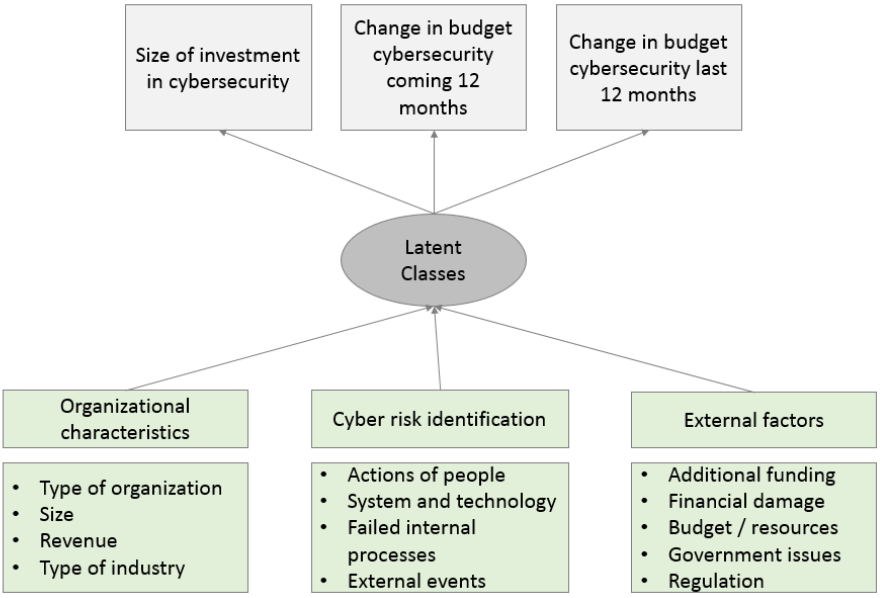

Figure 14 – conceptual latent class model

4.2.1. Indicators

The indicators are used to distinguish different clusters in the dataset. The goal is to distinguish different behaviour in the investment strategy in cybersecurity. Therefore the amount of investment, the change of investment in the previous 12 months and the change of investment in the coming 12 months are used as indicators. The amount of investment is defined as less than 1 US Dollar up to more than 250 US Dollar. The change of investment the coming and previous months is defined as increased by more than 25%, increased between 15% and 25%, increased between 5% and 15%, stayed approximately the same, decreased between 5% and 15%, decreased between 15% and 25%, decreased by more than 25% and don't know.

4.2.2. Covariates

In section 3.7 the dimension of cybersecurity decision making is discussed and this includes all the aspects that might have an influences on the investment behaviour. As mentioned in section 3.7, the dataset used for the latent class analysis an existing dataset and not all information wanted is available in this dataset. Therefore the following covariates are included in the model.

Active covariates

Organizational characteristics

The organizations characteristics are expected to have a significant influence on the investment behaviour. The following variables are included in the model:

- Type of organization which is defined as: government or non-profit, private or public organization and is included as a nominal covariate.
- Number of employees which is defined in the GISS dataset in 16 levels ranging from less than 1000 up to more than 100.000. This is recoded into two different levels according to European standards to: small/medium <1000 and large >1000. This variable is included as nominal covariate.
- Total revenue which is defined in the GIS dataset in 15 levels from less than 100.000 up to more than 5 billion US Dollar. This is recoded into three different levels according to European standards as: small which is less than 5.6 million US Dollar, medium which is greater than or equal to 5.6 million US dollar and 22.8 million US Dollar and large which is greater than 22.8 million US Dollar. This variable is included as nominal covariate.
- Type of industry which can be seen in the table 1 above, 26 different types of industries are included as nominal covariate.

External factors

The following external factors are included in the model:

- Additional funding needed for cybersecurity which is defined in 5 levels from 0-25%, 26-50%, 51-75%, over 100% and don't know. This variable is included as nominal covariate.
- Total financial damage past year which is defined in 8 levels from between 0 and 100.000 US Dollar, 100.000 to 250.000 US Dollar, 250.000 to 500.000 US dollar, 500.000 to 1 million US Dollar, 1 and 2.5 million US Dollar and above 2.5 million US Dollar, don't know and had no information security incidents that resulted in any financial damage.
- The main obstacles or reasons that challenge your Information Security operation's contribution and value to the organization defined as:
    - Budget constraints (yes/no)
    - Lack of resources (yes/no)
    - Government issues (yes/no)
    - Fragmentation compliance or regulation (yes/no)

Risk identification

As discussed in the literature study there are four risk classes: actions of people, systems and technology failures, failed internal processes and external events. In the GIS survey respondents were asked who or what they consider the most likely source of an attack and which threats and vulnerabilities have increased their risk exposure. These question are categorized in the four risk classes, as can be seen in table 2 below. Interesting is whether these four classes have a significant influence on the investment behaviour. The variables in the GIS dataset were defined with the following five levels: highest priority, high priority, neutral, low priority and lowest priority and not applicable if the risks was not applicable to the respondent. The average of these variables is included in the class model as active nominal covariates.

Table 2 - risk identification

Risk identification	Variable GIS dataset
Risk actions of people	Vulnerability – careless or unaware employees Vulnerability — related to social media use Threat — phishing Threat — spam Threat — internal attacks (e.g., by disgruntled employees) Threat — fraud Threat — espionage (e.g., by competitors)
Risk systems and technology failure	Vulnerability — outdated information security controls or architecture Vulnerability — related to cloud computing use Vulnerability — vulnerabilities related to mobile computing use Threat — zero-day attacks Threat — malware (e.g., viruses, worms and Trojan horses)
Risk failed internal processes	Vulnerability — unauthorized access (e.g., due to location of data)
Risk external events	Threat — natural disasters (storms, flooding, etc.) Threat — cyber-attacks to steal intellectual property or data Threat — cyber-attacks to steal financial information (credit card numbers, bank information, etc.) Threat — cyber-attacks to disrupt or deface the organization

Inactive covariates most likely source of attack

The following variables are included as inactive covariates, the most likely source of attack from:

- Malicious employee (yes/no)
- Careless employee (yes/no)
- External contractor (yes/no)
- Customer (yes/no)
- Supplier (yes/no)
- Other business (yes/no)
- Criminal syndicates (yes/no)
- State sponsored attacker (yes/no)
- Hacktivist (yes/no)
- Lonewolf (yes/no)

Inactive covariates do not influence the cluster membership, and are included to give more insight in the composition of the clusters. These variables are not included because all are covered by the risk identification and in particular are covered by the risk of actions of people. If these variables are included in the latent class analysis then there is a chance that this class of risk will occur too often and causes imbalances.

4.3.Latent class model estimation

In a latent class analysis respondents are clustered based on the fact that they have the same investment behaviour. To estimate the model correctly it first estimated without any covariates, see table 3 for the outcomes of this estimation. Several methods exist to determine which models fits best.

The first method is based on the L^2. The model L^2 assesses how well the model fits the data. The L^2 indicates the amount of association among the variables that remains unexplained after estimating the model. The lower the L^2, the better the fit of the model to the data. One criterion for determining the number of clusters is to take the p-value. The p-value represents the estimation that the L^2 statistics follow a chi-square distribution for each model. Generally, when the p-value is smaller than 0.05 the model provides an adequate fit and is most parsimonious. Using this criterion the best model is given by model 4, the 4-class model with a p-value of 0.01.

The second method depends on the Bayesian Information Criterion (BIC) to determine the best model fit and the number of classes. The model with the lowest BIC is preferred. Using this criteria model 3 would fit best. It is important that the different classes clearly differ from each other and are well interpretable based on the indicators. The difference with the four class model is relatively small and the four class model shows that there are four clusters that are well interpretable and differ from each other as well. The four-class model shows a fourth class which has a very large investment and this class is not shown in the three class model. Thus combining this with the L^2 criteria the four class model is chosen.

Table 3 - latent class model estimation

Model	Log-likelihood	BIC(LL)	L^2	BIC(L^2)	Degrees of freedom	p-value	Class.Err.
1-Cluster	-8135.45	16419.60	1630.56	-1544.37	427.00	0.00	0.00
2-Cluster	-7812.21	15929.27	984.08	-2034.70	406.00	0.00	0.01
3-Cluster	-7606.78	15674.55	573.22	-2289.42	385.00	0.00	0.10
4-Cluster	**-7533.47**	**15684.08**	**426.61**	**-2279.89**	**364.00**	**0.01**	**0.14**
5-Cluster	-7489.97	15753.22	339.60	-2210.75	343.00	0.54	0.14
6-Cluster	-7456.84	15843.10	273.34	-2120.87	322.00	0.98	0.14
7-Cluster	-7435.88	15957.34	231.43	-2006.64	301.00	1.00	0.15
8-Cluster	-7420.55	16082.82	200.77	-1881.15	280.00	1.00	0.21
9-Cluster	-7410.43	16218.72	180.53	-1745.25	259.00	1.00	0.22
10-Cluster	-7402.80	16359.60	165.26	-1604.37	238.00	1.00	0.29

4.4.Different patterns in investment behaviour

The outcome of the latent class analysis shows that there are four classes different from each other and are well interpretable. Table 4 shows that cluster 1 contains 38 percent of the cases, cluster 2 contains 33 percent of the cases, cluster 3 contains 22 percent of the cases, and cluster 4 contains the remaining 7 percent. The conditional probabilities show the differences in response patterns that distinguish the clusters. The complete table which includes the covariates is table 6. The four classes are discussed below including some distinguishable characteristics of the respondents per class.

4.4.1. Significance indicators and covariates

Based on the Wald test the significance of the indicators and the active covariates can be determined. This test indicates that the indicators significantly differ between the classes and that almost all covariates significantly affect cluster membership. As can be seen in table 4 below (in green), with a confidence level of 92 percent, there are 11/15 covariates that significant affect cluster membership. In the next section the four different clusters will be explained and the distinguishable characteristics of the respondents per class which are based on the significant covariates.

There are also some similarities between the clusters. What is interesting is that within all clusters almost 70 percent of the respondents consider the lack of executive awareness or support as a main obstacle that challenge their cybersecurity. In addition within all clusters between 40 - 65 percent of the respondents consider the lack of resources as a main obstacle that could challenge their cybersecurity as can be seen in table 6.

Table 4 - significance Wald test indicators and covariates

	Indicators	**Wald**	**P-value**
Investment strategy	Annual spend on information security	288.88	0.00
	Change of budget coming 12 months	219.84	0.00
	Change of budget last 12 months	235.75	0.00
	Covariates		
Cyber risk identification	Threat actions of people	23.50	0.07
	Threat failed internal processes	28.18	0.02
	Threat systems failure	15.26	0.43
	Threat external events	10.61	0.78
External factors	Budget constraints	14.68	0.00
	Lack executive awareness or support	11.09	0.01
	Fragmentation compliance or regulation	7.49	0.06
	Management government issues	0.19	0.98
	Lack of resources	6.78	0.08
	Additional funding needed	66.48	0.00
	Total financial damage past year	42.96	0.00
Organizational factors	Type of organization	17.54	0.01
	Type of industry	86.88	0.11
	Total revenue	60.41	0.00
	Number of employees	38.19	0.00

4.4.2. Small investment and no changes in budget

The first and largest class is a group with a small investment and no expected changes in this investment. 38 percent of the respondents belong to this class. Besides making a small investment in security they expect that the coming 12 months this budget will not increase and the past 12 months this budget did not change either. As expected, within this group of respondents almost 30 percent has a small revenue and almost 80 percent is a small company with less than 1000 employees. Notable is that 68% of the respondents noted that budget constraints was one of the main obstacles of reasons that challenge the information security contribution and value to the organization. The fact that these organisations have budget constraints could explain that the investment is very low and that this will probably not change the coming 12 month. One could say that if the investment is low the risk would be low as well, however almost 40 percent of the respondents indicate that the threat of action of people is their high or highest priority

risk. The budget constraints could therefore explain the low investment besides the high priority risks. What could also have contributed to this investment not changing is the fact that 40 percent had a small total financial damage, up to 100.000 US Dollar and almost 42 percent did not have an information security incident that resulted in any financial damage. This could indicate that if damages to an organisation are small to none, they are not driven to increase their budget.

4.4.3. Medium investment and increasing budget

The second class is a group with a medium amount of investment and expect to increase their budget up to 25% the coming 12 months. This second largest class contains 33 percent of all respondents. What is interesting is that of this group almost 25 percent states that fragmentation compliance or regulation is one of their biggest challenges. This could indicate that this group will increase their (already relative high) investment the coming 12 months to comply with upcoming rules and regulations. In addition, half of this group showed that they had a large financial damage in the past year due to security incidents, up to 500.000 US Dollar. Which could also explain why this group will increase their spending. What should be noted is that in this group almost 85 percent has more than 1000 employees and very large revenue. What is interesting is that this group mainly contains of public or governmental organizations.

4.4.4. Small investment and great increasing budget

The third group contains 22 percent of the respondents. This group represent a group with a small investment at the moment but have an increase in this budget the last 12 months with more than 25% and expect to increase this budget the coming 12 months with more than 25 percent. A large part of this group, almost 70 percent, are small companies with less than 1000 employees. What is interesting is that almost 40 percent of this group indicates that all four risk classes have a high or highest priority. This could explain that they feel the need to increase their small investment because of the risk identification.

4.4.5. Large investment without information

The last group contains 6 percent of the respondents. This group has a very large investment, 77 percent spends more than 250 million US Dollar on information security and 70 percent do not know whether their budget has changed the last 12 months or will change the coming 12 months. They also do not know whether additional funding is needed, or if they had total financial damage the past year due to a security incident. It seems that this group spends a lot of money on their security but do this based on incomplete or absent data. As expected this group has a high revenue and 64% is a large company with more than 1000 employees. What is interesting is that three types of industries are well represented. These are the telecom industry, technology industry and banking and capital markets. Especially the latter industry is known for having their security as a high priority, mostly due to client requirements. This could explain the high percentage (20%) of banking and capital markets in this group.

Table 5 - latent class model only shown with indicators

	Small investment and no changes in budget	**Medium investment and increasing budget**	**Small investment and great increasing budget**	**Large investment and no information**
	Cluster 1	**Cluster 2**	**Cluster 3**	**Cluster 4**
Cluster Size	**38%**	**33%**	**22%**	**7%**
Indicators				
Annual spending on security				
Less than US$1 million	0,74	0.09	0.63	0.06

Between US$1 million and US$2 million	0.13	0.16	0.20	0.06
Between US$2 million and US$10 million	0.10	0.38	0.12	0.05
Between US$10 million and US$50 million	0.00	0.24	0.05	0.03
Between US$50 million and US$100 million	0.01	0.04	0.00	0.03
Between US$100 million and US$250 million	0.01	0.04	0.00	0.00
More than US$250 million	0.01	0.05	0.00	0.77
Change security budget the last 12 months				
Increased by more than 25%	0.06	0.14	0.43	0.05
Increased between 15% and 25%	0.06	0.20	0.23	0.10
Increased between 5% and 15%	0.26	0.30	0.22	0.00
Stayed approximately the same (between +5% and -5%)	0.56	0.33	0.08	0.16
Decreased between 5% and 15%	0.03	0.02	0.00	0.00
Decreased between 15% and 25%	0.01	0.01	0.00	0.02
Decreased by more than 25%	0.02	0.00	0.02	0.00
Don't know	0.00	0.00	0.02	0.67
Change security budget the coming 12 months				
Will increase by more than 25%	0.00	0.05	0.40	0.03
Will increase between 15% and 25%	0.04	0.17	0.41	0.07
Will increase between 5% and 15%	0.38	0.42	0.10	0.07
Will stay approximately the same (between +5% and 5%)	0.51	0.29	0.03	0.10
Will decrease between 5% and 15%	0.03	0.05	0.00	0.00
Will decrease between 15% and 25%	0.01	0.00	0.01	0.04
Will decrease by more than 25%	0.01	0.01	0.02	0.00
Don't know	0.03	0.01	0.04	0.69

Table 6 - latent class model shown with covariates

Active Covariates		Cluster 1	Cluster 2	Cluster 3	Cluster 4
Risk: actions of people	not applicable	0.01	0.02	0.02	0.04
	highest priority	0.23	0.17	0.20	0.30
	high priority	0.22	0.18	0.24	0.26
	neutral	0.32	0.37	0.33	0.12
	low priority	0.20	0.24	0.18	0.28
	lowest priority	0.02	0.02	0.03	0.00
Risk: systems and technology failure					
	not applicable	0.08	0.04	0.07	0.10
	highest priority	0.18	0.11	0.20	0.17

	high priority	0.20	0.24	0.23	0.33
	neutral	0.28	0.37	0.26	0.29
	low priority	0.21	0.21	0.21	0.08
	lowest priority	0.05	0.02	0.04	0.03
Risk: Internal processes					
	not applicable	0.32	0.30	0.25	0.33
	highest priority	0.06	0.15	0.18	0.08
	high priority	0.19	0.18	0.18	0.18
	neutral	0.16	0.18	0.22	0.17
	low priority	0.16	0.15	0.09	0.14
	neutral	0.11	0.05	0.08	0.10
Risk: External events					
	not applicable	0.16	0.15	0.17	0.27
	highest priority	0.19	0.13	0.16	0.14
	high priority	0.14	0.18	0.14	0.21
	neutral	0.20	0.24	0.27	0.12
	low priority	0.20	0.22	0.21	0.20
	lowest priority	0.11	0.08	0.06	0.07
Main challenge lack of resources					
	no	0.44	0.42	0.34	0.59
	yes	0.56	0.58	0.66	0.41
main challenge budget constraints					
	no	0.32	0.44	0.47	0.45
	yes	0.68	0.56	0.53	0.55
main challenge lack executive awareness					
	no	0.67	0.78	0.68	0.70
	yes	0.33	0.22	0.32	0.30
main challenge government issues					
	no	0.72	0.70	0.76	0.74
	yes	0.28	0.30	0.24	0.26
main challenge fragmentation compliance or regulation					
	no	0.83	0.75	0.85	0.79
	yes	0.17	0.25	0.15	0.21
total revenue					
	<5	0.29	0.05	0.23	0.23
	5-10	0.22	0.10	0.23	0.06
	10-15	0.23	0.28	0.25	0.18
	15-20	0.07	0.35	0.15	0.18
	>20	0.18	0.22	0.13	0.35
type of industry					
	Wealth & Asset Management	0.01	0.01	0.03	0.00
	Transportation	0.05	0.00	0.03	0.01
	Telecommunications	0.02	0.05	0.01	0.11
	Technology	0.06	0.07	0.06	0.14

	Retail & Wholesale	0.03	0.08	0.03	0.01
	Real Estate (includes Construction. Hospitality & Leisure)	0.03	0.02	0.08	0.01
	Provider Care	0.00	0.01	0.00	0.00
	Professional Firms & Services	0.04	0.04	0.04	0.01
	Private Equity	0.00	0.00	0.00	0.00
	Power & Utilities	0.03	0.08	0.07	0.04
	Other	0.08	0.02	0.08	0.06
	Oil & Gas	0.01	0.04	0.02	0.00
	Mining & Metals	0.04	0.00	0.04	0.01
	Media & Entertainment	0.02	0.01	0.06	0.07
	Life Sciences	0.00	0.02	0.02	0.04
	Insurance	0.11	0.06	0.12	0.04
	Healthcare	0.03	0.05	0.05	0.03
	Government & Public Sector	0.13	0.02	0.04	0.11
	Diversified Industrial Products	0.07	0.06	0.03	0.01
	Consumer Products	0.05	0.05	0.06	0.03
	Chemicals	0.02	0.01	0.00	0.00
	Banking & Capital Markets	0.15	0.22	0.10	0.20
	Automotive	0.02	0.05	0.01	0.04
	Airlines	0.01	0.02	0.00	0.00
	Aerospace & Defense	0.00	0.01	0.00	0.00
Type of organization					
	Government or Non-Profit	0.16	0.13	0.11	0.18
	Private	0.51	0.20	0.54	0.49
	Public	0.33	0.67	0.36	0.32
Additional funding needed					
	0-25%	0.60	0.63	0.28	0.22
	26-50%	0.16	0.18	0.36	0.03
	51-75%	0.03	0.06	0.09	0.00
	Over 100%	0.03	0.01	0.12	0.01
	Don’t know	0.17	0.12	0.15	0.74
total financial damage past year					
	Between $0 and $100.000	0.41	0.27	0.40	0.14
	Between $100.000 and $250.000	0.02	0.12	0.09	0.04
	Between $250.000 and $500.000	0.00	0.10	0.03	0.02
	Between $500.000 and $1 million	0.01	0.04	0.03	0.00
	Between $1 million and $2.5 million	0.00	0.02	0.02	0.03
	Above $2.5 million	0.00	0.02	0.01	0.02
	Don’t know	0.14	0.12	0.16	0.43
	Had no information security incidents that resulted in any financial damage	0.42	0.30	0.25	0.32
number of employees					
	<1000	0.80	0.15	0.69	0.36
	>1000	0.20	0.85	0.31	0.64

4.5. Conclusion

What can be concluded is that four groups are found in the dataset of the GIS survey. Within these four groups there are several factors that could explain a certain investment behaviour. The significant covariates that determine cluster membership are:

- Threat actions of people
- Threat failed internal processes
- Lack of resources
- Budget constraints
- Lack of executive awareness or support
- Fragmentation compliance or regulation
- Total revenue
- Type or organization
- Additional funding needed
- Total financial damage past year

In the first group there are two factors. First the budget constraints are identified as a major concern and could explain the investment behaviour. And second is the factor that no incidents with serious financial damage happened that could explain that investment are not felt as necessary. In the second group, with the medium investment and increasing budget, the regulation has been indicated a major concern and could explain the investment behaviour. In the third group, small investment and great increase in budget, the risk identification could explain the investment behaviour. Within this group all type of risks have a very high priority. And in the fourth group, who have a large investment but no information, the type of industry and the associated client requirements make that security receives a high priority, which could explain the high investment.

5. Q-method and results

To be able to capture individual perspectives of decision-makers the q-method is performed. In this chapter the six steps of the q-method are described and performed. This chapter will discuss the following steps: the concourse, the selection of the q-sample, the selection of the p-set, then the q-sort, which is the ranking of the statements, after that the correlation and factor analysis and finally the results.

The framework which is discussed in chapter 3.7 will be used to structure the statements and to make sure that the best possible extent of perspectives are covered by the statements. This means that each dimension should be covered in the statements: context establishment, the categories of risks, cyber risk management strategies and the external factors.

5.1. Step 1: Concourse

The first step of the q-method is the concourse. The concourse is a set of statements and opinions that covers that is said or written about decision making regarding cybersecurity investments and factors that influence these decisions. This set of statements is derived from interviews, literature research, news and fora. The statements represent the best possible extent of perspectives regarding cybersecurity investments. The interviews are done with cybersecurity decision-makers in the field, so these are people that make decisions or can influence the decision-making in an organization about the investment strategy for cybersecurity.

The framework which is presented in chapter 3.7 is used to structure the topic of decision-making in cybersecurity investments. Each of the categories that has been covered by the framework, needs to be covered by the statements. Per category approximately ten statements are included, which resulted in 185 statement in total, see appendix F . The set of 185 statements is not suitable to present to the respondents. Therefore this set needs to be reduced to a selection of approximately 40-60 statements, which is called the q-sample. This is explained in the next section: step 2: the q-sample.

5.1.1. Respondents and data collection for concourse

The respondents for the interviews to collect data for the concourse and the interviews for the Q-sort are strategically chosen; this means persons who are expected to have a clear perspective regarding the cybersecurity investment decision-making. As can be seen in the figure, within the Q-method there are two rounds of interviews, first is for the concourse and the second is for the q-sort. The respondents for both these interviews are strategically chosen from the target group.

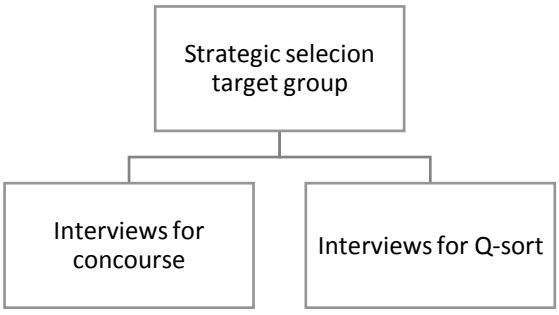

Figure 15 - respondent selection and interviews

The target group consist of people that take decisions about cybersecurity investments or have an impact on the decision-making process or can influence this process. It is important to select people who are expected to have a distinct perspective, in order to cover the whole framework.

In this research it is assumed that here are two factors that can influence the perspective of decision-makers and therefore have different perspectives. These factors are: the type of sector: private versus public organizations and the size of a company: small <1000 employees and large >1000 employees. Both private and public sectors are facing fundamental challenges regarding cyber threats. The private sector have more examples of best practices in cybersecurity since their existence is in many cases dependent on good security within competitive markets. Public organizations, however, have not always been dependent on good security but are catching up and recognize the scale and magnitude of today's cyber threats (Parsons, 2017). So it is expected that these industries have a different perspective on the decision-making regarding cybersecurity investments. The size of a business often coheres with the size of the available budget and investment strategy. In a smaller company with a limited budget for example, decisions can be based on incomplete risk information and focus on a small amount of risks and not on the complete and detailed risk assessment, due to high costs. The expectation is that professionals within larger companies have different perspectives on the investment than security professionals in smaller companies.

For the concourse six respondents are interviewed. These respondents are people that make decisions about the cybersecurity investment or have impact on the decisions regarding cybersecurity investment have been interviewed. The respondents are from public and private organizations and from small and large organizations. All respondents want to be anonymous, due to sensitive information. Only information from people that actually make decision or have such an impact on the decision-making is considered relevant for this study. The following respondents were interviewed and have the following position within the company:

- Director large private company
- CISO small private company
- CISO large governmental organization
- Cybersecurity professional large governmental organization
- Cybersecurity professional small private company
- Cybersecurity professional large private company

The interviews are based on the framework presented in chapter three. A summary of the interviews is shown in appendix D.

This resulted in many statements that cover the many categories of the framework. Some categories were not covered well and are completed with sources as journals, forums and news sites, as shown in appendix A. The statements should have a normative character and thus some statements are adapted and differ from the original source.

5.2. Step 2: Q-sample

The set of 186 statements is not suitable to present to the respondents. Therefore this set needs to be reduced to a selection of approximately 40-60 statements, which is called the q-sample (Exel & Graaf, 2005). The development of the q-set is done with the so-called inductive way of structuring the concourse. With the help of clusters one can define what propositions belong together based on content. Ultimately within each homogeneous cluster an equal number of propositions will be chosen. This way one maximize the intrinsic heterogeneity and thus the representativeness of the final set of propositions. The framework which is created in chapter three is used to select an equal number of propositions per category. This structure forces to select statements widely different from one another and makes the q-set broadly representative. Each category of the framework contains approximately two statements. As a result a number of 47 statements are selected from the 186 statements, which can be seen in table 8. A comprehensive discussion why these 47 statements were chosen can be found in appendix E.

5.3. Step 3: P-sample

As mentioned above: the p-set is not a random set of respondents. It is a strategically selected sample of respondents who are theoretically relevant to the problem under consideration; persons who are expected to have a clear and distinct perspective regarding the cybersecurity investment decision-making and may define a factor.

As mentioned above it is expected that two factors can influence the perspective of decision-makers, namely: the type of sector and size of the organization. So based on the following factors the respondents will be strategically chosen:

- Sector: public sector vs private sector.
- Company size: small and medium <1000 employees vs large > 1000 employees (This number of employees is based on the GIS survey in which companies with less than 1000 employees is referred to as small companies).

The selection of the respondents started in personal networks and the respondents are obtained in all different kinds of domains such as: healthcare, consultancy, IT, marketing, deployment agency, start-ups and governmental organizations. The function vary from CEO's, CISO's, owners, directors, higher management and IT or security managers. Eventually 18 decision-makers were willing to participate in this study. All 18 respondents could make decisions about investment or could influence the decision-making process. Figure 16 shows the distribution of respondents. As can be seen the small and medium private organizations are slightly overpopulated. This is partly due to the fact that small businesses are referred to as less than 1000 employees. Due to confidential and sensitive information several decision-makers asked for anonymity, therefore the results will be anonymous.

Eventually, one also wants to determine whether there is a significant relation between the organizational factors (size and type of sector) and the perspectives found. This number of respondents could influence this significance between these organizational factors and the individual perspectives. Due to the low number of respondents it is possible that this relation is not significant, but is based on coincidence. However, if it is not significant it is still possible to determine the direction of the relation. The relation between these organizational factors and the perspectives is discussed in sector 5.6: interpretation of results.

	Small and medium organization (<1000)	Large organization (>1000)
Public organizations	4 respondents	4 respondents
Private organization	7 respondents	3 respondents

Figure 16 - number of respondents per group

5.4. Step 4: Q-sort

In this step every person in the P-set will rank order the statements in the Q-set within a predetermined quasi-normal distribution from most agree to most disagree. The condition of the instruction will be: "To what extent do you agree with the following statements? ". The ranking procedure is according to Brown (1980) the technical means whereby data are obtained for factoring. An example of the distribution is shown in figure 17. This distribution forces respondent to make explicit considerations and ensures that respondents assess the statements relative to each other. Each respondents is forced to actively construct his or her perspective. Through this procedure each statement (potentially) interact with all other statements, and one measures the position and importance at the same time. The quasi-normal distribution is no more than a reflection of how the distribution of views around a subject typical is. Other distributions would lead to the same outcomes (Exel & Graaf, 2005). In addition to this q-sort the respondents were asked to explain the statements placed on the extreme ends of the distribution. This information is helpful for the interpretation of factors later in the next section.

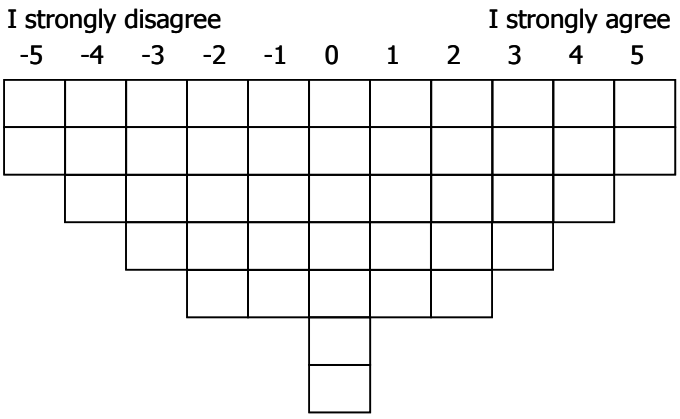

Figure 17 - forced distribution to sort statements

5.5. Step 5: Correlation- and factor analysis

The goal of the analysis is to find shared perspectives amongst the respondents. By factorizing the correlations between the respondents groups can be formed. The groups are in other words respondents who have chosen the same statements in approximately the same configuration. The analysis starts with the calculation of the correlation matrix. This matrix represents the level of (dis) agreement between the individual sorts. Next this correlation matrix is subject to factor analysis, to identify the number of different groups of q sorts. Respondents who have similar perspectives will share the same factor. The factor analysis determines how many factors exist in the total set of Q sorts. Respondents 'loading high' on one factor means that the respondent significantly correlates with the factors.

In this thesis the SPSS software is used to perform the factor analysis and has implemented the Varimax method, which is a factor rotation method. The rotation is according to the statistical principal "Varimax"(Watts & Stenner, 2005). The rotations shifts the perspectives and examines them from different angels and this results in final factors that represent a group of individual perspectives that are highly correlated to each other and uncorrelated with others (Exel & Graaf, 2005). The Varimax maximizes the variance of the least possible number of factors. This method is used to get a simple structure, which means a pattern in which each respondent's loads high on one factor and low on the other factors. So the Varimax method does not change any of the results.

5.5.1. Correlation analysis

So the correlation analysis represents the level of (dis)agreements between the respondents. A positive correlation means that the respondents have a high level of agreements. A negative correlation means that the respondents disagree with each other. Most correlations between the 18 respondents are positive, this means that most respondents agree with each other. The largest positive relation is 0.67 the largest

negative relation is -0.44 (see appendix G for correlation matrix). A high positive relation does not mean that the respondents automatically correlate to the same factor.

5.5.2. Factor analysis

To identify the number of different groups in the q sort the factor analysis is performed. In theory it is recommended to start with seven factors to rotate. The Varimax is therefore performed with seven factors, this resulted in correlations of respondents that loaded on only four of the seven factors. Therefore, four factors are needed to explain the data.

The optimum number of factors was determined based on several criteria. At least 3 persons should load enough per factor, normally this means at least a factor loading > 0.50. However, according to (Watts & Stenner, 2005) a q sort can be assigned to a factor with the formula: $\frac{1}{\sqrt{n}} \times 2.5$. Where N is the number of respondents = 18. This results in a factor loading of 0.59. This is a guideline for the maximization of the amount of single loadings in the total amount of respondents. However, with the factor analysis it is desirable to maximize the amount of single loadings of respondents, this means to have a maximal amount of respondents loading on one factor. And therefore have a maximum amount of respondents included in the analysis. So, the more respondents are included the more individual perspectives are included in the analysis. To maximize this amount of respondents on a factor different factor loadings were used, as can be seen in figure 18. When the factor loading is set at 0.45 the amount of respondents is maximized.

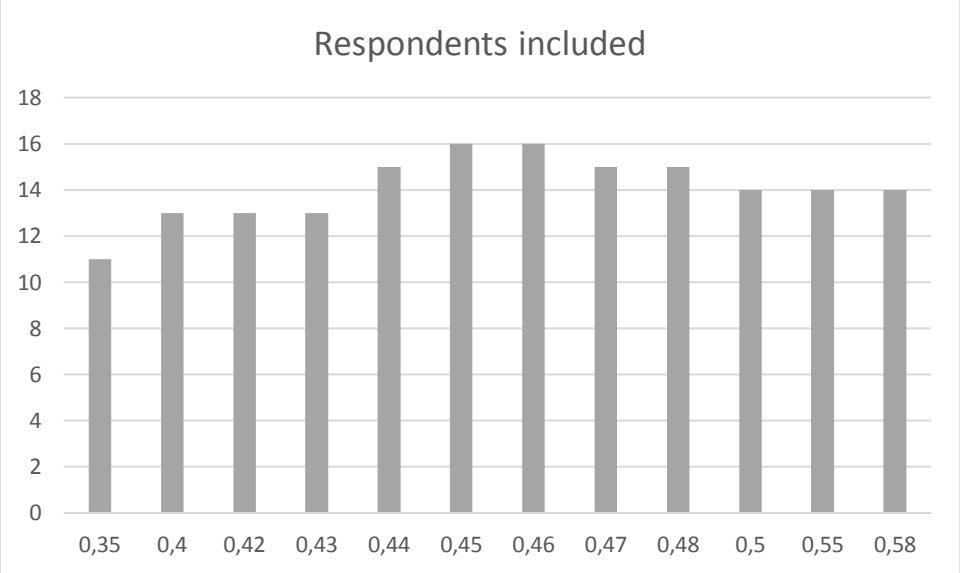

Figure 18 – Factor loading and number of respondents included

As mentioned above, the factor analysis resulted in correlations of respondent that loaded on only four of the seven factors. Therefore, only four factors are needed to explain the dataset. As can be seen in table 7 there are two respondents that have a high factor loading on more than one factor. When respondents are loading double there is no significant proof for a correlation to a single factor, therefore it is not possible to assign that respondent to one of the factors. So these two respondents are excluded from further analysis and the factor analysis is performed again without these two respondents.

Table 7 - Factor loadings

	Factor I	Factor II	Factor III	Factor IV
R1	0,605			
R2			0,606	
R3	0,502			0,528
R4			0,504	
R5	0,652		0,522	
R6	0,680			
R7				0,593
R8	0,614			
R9	0,486			
R10	0,840			
R11	0,602			
R12		0,470		
R13				0,742
R14		0,650		
R15		0,795		
R16			0,824	
R17	0,726			
R18		-0,738		

5.6. Step 6: Interpretation of results

The interpretation is the last step and is refered to as the most technical and scientific base of the Q. In the previous section the correlation matrix was calculated, which represents the agree or disagreement between the individual sorts. After that this correlation matrix was subject to factor analysis to identify similar perspectives on the topic and therefore have the same factor. And now in this section those identified factors will be interpreted. The interpretation of the perspectives is done based on the Z-scores. The two statements with the highest Z-score are valued with 5, the lowest Z-scores with -5 and so on. Behind every statement the factors scores will be shown as (S1 1, 3, 4, 4). This means statement 1, loading on the first factor is 1 on the second factor is 2, on the third factor is 4 and on the fourth factor is 4.

5.6.1. Relation between organizational factors and factor loading

To determine whether there is a significant relation between two variables the chi-square test is used. With several numbers one also gets an idea about the strength and direction of the relation between the variables. The first null hypothesis is that there is no relation between the size of company and the factor it loads high on and the second null hypothesis is that there is no relation between the type of sector of a company and the factor it loads high on.

The first test is performed on the type of sector and factor loading. The chi-square shows whether the relation between the type of sector and the factor loading is significant or not. The value of the chi-square is 1.4 with a significance level of 0.70 which is > 0.05. Therefore the null hypothesis cannot be rejected, which means that there is no significant relation between the two variables.

The second test is performed on the size of an organizations and factor loading. The value of the chi-square is 0.83 with a significance level of 0.84 which is > 0.05. Therefore the null hypothesis cannot be rejected, which means that there is no significant relation between the two variables. See appendix H for the tabs.

5.6.2. Factor I – Concerned perspective

The respondents in this group are highly concerned about two things. First is the difficulty to determine cyber risk and the changing threat environment and second is the increasing use of social engineering. There are multiple threats and yes they are continuously evolving. However, some respondents mentioned that there are a couple standard common attack methods. These attack methods become more sophisticated, but we know them. For example, attacks such as malware, phishing and DDoS will become more sophisticated, but they no new methods will be developed from out of nowhere. Social engineering is one of the risks these respondents do clearly know and it might therefore be that the emphasis is put on the increasing use of social engineering.

The respondents loading high on the first factor are concerned about unknown risks, compared to the other factors, these respondents highly agree with the statement: “it is very difficult to determine the cyber risks due to the fact that threats continue to evolve” (S2 **4**, -1, -3, 0). To manage risks, one needs to understand the risks. The respondents mentioned that the uncertainty about threats and likeliness makes it hard for the decision-makers to manage the risks, to determine what measures to take and what investments to make. This could also explain why the respondents highly disagree with the statement: “we only take risks with high likelihood and major consequences into account” (S20 **-4**, 2, 3, -1). This is probably due to the fact that it is difficult to determine cyber risks and that there is not sufficient information about risks and therefore it is not possible to only take those risks with high impact into account. The respondents in this group also agree in comparison with the other groups with the statement: Some security risks we simply do not know or cannot imagine therefore we cannot be 100% safe (S18 **3**, 2, 0 2). And highly disagree with the statement: With the best protection and security measures in place we are nearly 100% safe (S19 **-5**, -2, 2, -5). The respondents disagree with the statement: “Only taking mitigation measures is enough to cope with cyber risk” (S27 **-5**, 1, -3, 0). One of the reasons could be that the respondents agree with the statements that it is not possible to determine the type of risk, and that cyber threats continue to evolve, growing in size and become more and more complex and therefore mitigation measures will not be enough to cope with cyber risk. The respondents, however, disagree with the following two statements: “Back-ups and disaster recovery plans are too costly” (S7 **-4**,-4, 1, 1) and “Applying patches takes too much time and resources” (S12 **-4**, -2, 1, 1). So these are the mitigation measures they do take.

The respondents in this group highly agree with the statement: “Social engineering is becoming increasingly advanced and is one of our biggest concerns, and therefore requires awareness at all levels within the organization” (S9 **5**, -3, 2 -1). And slightly consider careless or unaware employees as the weakest link in the security system (S10 **1**, 1, 5, 3). The respondents in this group also agree with the following statement: “A breach or incident could have positive effects too, such as more awareness, as long as the impact is not too big” (S35 **4**, -1, -2, 3). This shows the importance of the awareness of the employees. Social engineering is becoming an essential form of hacking and is a serious concern to the respondents. Almost all organizations have developed awareness training, but for some respondents, social engineering is apparently, a bigger concern than for others. Not all respondents agree about the extent to which awareness training helps. Awareness training only helps up to a certain level, at some point the attacks become too sophisticated and attackers will find a way in. So what might be more important is learning how to mitigate problems when they occur (S. Johnson, 2017).

5.6.3. Factor II – Resilient perspective

The respondents which are loading high on the second factor try to avoid risk as much as possible and think that preventing attacks from happening is very difficult, if not impossible and put most focus on incident response and resilience.

While other respondents mentioned that risk avoiding is almost impossible, these respondents highly agree with the following statement: "An organization has to avoid risk as much as possible, for example do not store personal data that is not necessary to store" (S30 0, **5**, -2, -3). This makes clear that all respondents and thus organizations have different cyber security strategies. In addition they think that: "Incident response and resilience is more important than trying to prevent attacks from happening" (S32 -3, **5**, -1, -1) and that: "complete prevention of security breaches is technologically impossible and, in some cases even undesirable because of high costs" (S24 0, **4**, -1, 5). So the respondents that load high on this factor put more emphasis on response and resilience, probably because the prevention of breaches is impossible but also because some security risks one simply do not know or cannot imagine.

What is interesting is that this group disagrees with the statement: "We perform a comprehensive cost-benefit analysis, because an investment in security must result in a benefits" (S37 -2, **-5**, 1, 2). So the decisions to accept certain risks or avoid risk are probably not based on a comprehensive cost-benefit analysis. However the respondent do agree that some technical measures are too costly. So this could mean that the respondents in this group make decisions based on incomplete information.

The respondents in this groups also agree with the statement: "The existence of a vulnerability does not always mean it must be remediated. The organization may choose to accept the risk" (S22 -2, **4**, 3, 4) and that: "Acceptable risk levels should be set by management and based on the business's legal and regulatory compliance responsibilities" (S23 1, **3**,-1,-2). Other respondents agreed that the acceptable risk levels should be set by security professionals within the organizations. But these respondents agreed that it is management's responsibility to set the risk levels and ensure that the company meets the business objectives. A security professional might be an expert on the security level, but may not be an expert when it comes to meeting business goals. Therefore they probably agree that risk levels should be set by management and addressed as a holistic manner.

It seems that the availability of the systems is more important than the integrity of information because the respondents load negative on the following statement: "Integrity is more important than the availability of the systems. For example we want to keep some information secret and that has priority number one" (S5 1, **-5**, -1, 3). However contradicting is the loading on the following statement: "Unavailable systems due to physical external causes such as fire, floods etc. is a serious danger. We must have a high uptime" (S16 2, **-4**, 1, -2). But it could be that physical external causes are not a risk, but they do think that availability of systems is important. All organizations have different "crown jewels" to protect and this influence the type of perspective.

5.6.4. Factor III – Hierarchical perspective

This group of respondents is characterised by its focus on the unawareness of their employees, their focus on critical and vital information and their focus on the company's leadership. The major part of this group is from large private companies with multiple competitors, every respondent in this group works in a company with more than 1000 employees.

The respondents highly agree with the statement: "Careless or unaware employees are the weakest link in the security system. Cyber security awareness training can be a part of the solution" (S10 1, 1, **5**, 3). And think that their organization is a very interesting target for cyber criminals (S31 -2, -3, **-5**, 1).

The respondents also highly agree to the following three statements: "An employee or hacker who leaks vital information to a competitor is our biggest concern" (S3 -3, -3**, 5**, 0) and "Failure to properly secure and

protect confidential information can lead to the loss of business and clients and is our biggest concern" (S4 2, -1, **4**, -4) and "A cyber-attack can seriously damage our company's reputation" (S39 0, 0, **4**, -1). This clearly indicates what the respondents considers as important, namely: vital information, business and clients and reputation.

What is interesting is that the respondents definitely do not want to make use of cyber insurance because they highly disagree to the following statement: "Cyber insurance can function as a replacement for sound cyber-security and cyber resilience practices" (S29 -3, 0**, -4**, -1). As mentioned, for these respondents a number of assets are very important, namely: confidential information, reputation and business and clients. The loss of information, business or clients and reputational damage is something that is very difficult to express in monetary value. As a result, the respondents think that insurance is useless which makes it almost impossible to determine to what amount you want to insure. And what might be more important: the damage has already been done and insurance will not solve that.

"It is not complicated to prevent the impact of ransom ware such as wannacry, some technical basics such as back-up and awareness of your employees should be enough to avoid impact. (S25 1, 2**, -4**, 1). According to the respondents it is complicated because they are focussed on the unawareness of the employees. They know that employees are the weakest link in the system. Awareness training can help a little, but there will always be someone that does not work safely or clicks on unsafe links for example.

Another interesting focus is on the company's leadership. The respondents highly agree with the statement: "Half the battle is won when your company's leadership stresses the importance of company data and its integrity" (S6 2, 1, **4**, 1) and also to the statement: "The biggest problem is the awareness of the board. The top management is underestimating the cyber risks and not willing to invest (S13 -1, 2, **3**, -3). The board's involvement might be growing in many companies, but these respondents clearly show that awareness of the board is still a problem. Many board members do not understand cyber risks, or are not willing to invest. And this is not the only problem, the respondents also agree with the statement: "I am concerned that we do not have enough budget, the right team with the right knowledge and the latest technology available" (S36 -1, -1, **2**, 0).

5.6.5. Factor IV – Flexible perspective

The respondents that load high on factor IV have a focus on the risk assessment and have an adverse behaviour towards rules and regulations.

The respondents characterized by factor IV are not quite content with the existing regulations. The respondents think that: "ISO 27001 is an outdated standard. Nowadays it is not just about the technical approach to cyber security" (S46 0, -2, 1, **5**) and that the GDPR sends the wrong message.

Rules and regulation can function as a motivation for security. Because of such regulations, decision-makers come to realize that they have to invest in their security in order to comply with the regulations. However the respondents disagree with the statement: "Organizations are forced to be aware and invest because of the fines they may face from the GDPR" (S45 3, 0, -5, **-4**). However the respondents mentioned that the regulation does not only have a positive impact on security. They agree with: "Many spend a lot of effort on complying with regulations and this detracts from efforts to develop effective security capabilities. For example a security professional is now putting effort in assuring that the door to his data centre is of a certain thickness, rather than working on more effective security measures" (S41 2, -3, -2, **2**). This indicates that the respondents agree with the idea that regulation sometimes misses its purpose. Many respondents see regulation as a checklist that does not contribute to actual safety. What probably will help according to the respondents is when organizations actually get fines when they do not comply with regulation. They

do not think that the GDPR should be an incentive to invest in cybersecurity resulting from the loading to the statement: “Because of the GDPR we are going to invest in the minimum measures required which we would not do otherwise” (S42 0, 0, 0, **-3**).

A typical risk assessment consist of the context establishment, risk identification, risk analysis, risk evaluation and risk treatment. During the first step an organization determines its assets it wants to protect. The respondents in this group highly agree with the statement: Organizations should base their cybersecurity on their assets and not on something else” (S1 -1,-1, 0, **4**). Thus, it appears that this is the only group that is considering the first step of the risk assessment. And thus is the only group which starts with the identification of their assets. The respondent, however, indicate that there is a major problem in the preparation of risk assessments. Namely the lack of complete and correct information. They agree with the statement: “Cyber risk assessments are typically made without information about the probabilities of the outcomes, the consequences and the likelihood of occurrence” (S21, 0, 1, -3, **3**). Despite the fact that information is missing they do try to perform a comprehensive cost-benefit analysis, because an investment in security must result in benefits. (S37 -2, -5, 1, **2**). This extensive cost analysis also makes it clear that some measures are too expensive. Because the respondents highly agree to the statement: “Complete prevention of security breaches is technologically impossible and, in some cases even undesirable because of high costs” (S24 0, 4, -1, **5**). Too high costs could be one of the reason that organizations may choose to accept the risk. The respondents agree to the statement: “The existence of a vulnerability does not always mean it must be remediated. The organization may choose to accept the risk (S22 -2, 4, 3**, 4**).

Interesting is the following statement: Our organization is not an interesting target for cyber criminals, so we have nothing to worry about (S31, -2, -3, -5, **1**). Maybe this is because they base their security on their assets, and believe that there assets are not attractive to cyber criminals. Or because a cyber-attack would probably not lead to the loss of business and clients or impact their reputation as the respondents highly agree to the following two statements: “Failure to properly secure and protect confidential information can lead to the loss of business and clients and is our biggest concern” (S4 2, -1, 4, **-4**) and “Our reputation is our largest asset. It takes 20 years to build a reputation and five minutes to ruin it. Therefore reputational damage is a disaster to our organization” (S38 3, -2, 0, **-4**).

Table 8 - factor loadings per statement

Category framework	#	Statements	I	II	III	IV
Context establishment						
Assets	1	Organizations should base their cybersecurity on their assets and not on something else.	-1	-1	0	4
	2	It is very difficult to determine the cyber risks due to the fact that threats continue to evolve.	4	-1	-3	0
Confidentiality	3	An employee or hacker who leaks vital information to a competitor is our biggest concern	-3	-3	5	0
	4	Failure to properly secure and protect confidential information can lead to the loss of business and clients and is our biggest concern	2	-1	4	-4
Integrity	5	Integrity is more important than the availability of the systems. For example we want to keep some information secret and that has priority number one.	1	-5	-1	4
	6	Half the battle is won when your company’s leadership stresses the importance of company data and its integrity	2	1	4	1
Availability	7	Back-ups and disaster recovery plans are too costly	-4	-4	1	1

	8	A day without operating systems can cause major financial damage to our organization	-1	3	-3	2
Cyber risk identification						
Human threats	9	Social engineering is becoming increasingly advanced and is one of our biggest concerns, and therefore requires awareness at all levels within the organization.	5	-3	2	-1
	10	Careless or unaware employees are the weakest link in the security system. Cyber security awareness training can be a part of the solution.	1	1	5	3
System and technology failure	11	I think that an unpatched system is operating with a weak spot just waiting to be exploited by hackers.	5	0	-1	-2
	12	Applying patches takes too much time and resources	-4	-2	1	1
Failed internal processes	13	The biggest problem is the awareness of the board. The top management is underestimating the cyber risks and not willing to invest	-1	2	3	-3
	14	Cyber risk management should be part of the whole risk management	4	0	0	3
External events	15	Risk management is challenging because of interdependencies among firms. Therefore suppliers and third parties may be a serious risk to our cyber security due to their bad security	3	0	3	-3
	16	Unavailable systems due to physical external causes such as fire, floods etc. is a serious danger. We must have a high uptime.	2	-4	1	-2
Cyber risk assessment						
Part of risk	17	We invest in technologies like firewalls, intrusion detection, encryption etc. Although these technologies may reduce security vulnerabilities and losses from security breaches, it is not clear how much we must invest in IT Security	-1	1	2	-1
	18	Some security risks we simply do not know or cannot imagine therefore we cannot be 100% safe	3	2	0	2
	19	With the best protection and security measures in place we are nearly 100% safe	-5	-2	2	-5
Focus on likelihood and consequences	20	We only take risks with high likelihood and major consequences into account	-4	2	3	-1
	21	Cyber risk assessments are typically made without information about the probabilities of the outcomes, the consequences and the likelihood of occurrence	0	1	-3	3
Focus on acceptable risk level	22	The existence of a vulnerability does not always mean it must be remediated. The organization may choose to accept the risk	-2	4	3	4
	23	Acceptable risk levels should be set by management and based on the business's legal and regulatory compliance responsibilities	1	4	-1	-2
Focus on measures to take	24	Complete prevention of security breaches is technologically impossible and, in some cases even undesirable because of high costs.	0	4	-1	5
	25	It is not complicated to prevent the impact of ransom ware such as wannacry, some technical basics such as back-up and	1	2	-4	1

		awareness of your employees should be enough to avoid impact.				
Treatment strategy						
Risk mitigation	26	One does not have to take measures for risk that are not probable to the company	1	2	-1	1
	27	Only taking mitigation measures is enough to cope with cyber risk	-5	1	-3	0
Risk transfer	28	Insuring is always an economic trade-off. The costs of cyber insurance must be lower than the possible impact.	0	3	2	-2
	29	Cyber insurance can function as a replacement for sound cyber-security and cyber resilience practices	-3	0	-4	-1
Risk avoiding	30	An organization has to avoid risk as much as possible, for example do not store personal data that is not necessary to store	0	5	-2	-3
	31	Our organisation is not an interesting target for cyber criminals, so we have nothing to worry about	-2	-3	-5	1
Risk acceptance	32	Incident response and resilience is more important than trying to prevent attacks from happening	-3	5	-1	-1
	33	Accepting all risk is not possible due to regulation. For example it might be legally required to protect certain data.	2	3	-2	-2
	34	We didn't have a breach this year, so we don't need to ramp up investment. And if nothing happened this means that our security is good.	-3	-4	-2	0
External factors						
Breach or incident response	35	A breach or incident could have positive effects too, such as more awareness, as long as the impact is not too big.	4	-1	-2	3
	36	I am concerned that we do not have enough budget, the right team with the right knowledge and the latest technology available	-1	-1	2	0
budget	37	We perform a comprehensive cost-benefit analysis, because an investment in security must result in a benefits	-2	-5	1	2
	38	Our reputation is our largest asset. It takes 20 years to build a reputation and five minutes to ruin it. Therefore reputational damage is a disaster to our organization.	3	-2	0	-4
reputation	39	A cyber-attack can seriously damage our company's reputation.	0	0	4	-1
	40	We do not work with personal data so we do not have to invest in cybersecurity measures	-2	-2	-4	-5
Rules and regulation	41	Many spend a lot of effort on complying with regulations and this detracts from efforts to develop effective security capabilities. For example a security professional is now putting effort in assuring that the door to his data centre is of a certain thickness, rather than working on more effective security measures	2	-3	-2	2
	42	Because of the GDPR we are going to invest in the minimum measures required which we would not do otherwise.	0	0	0	-3
	43	As long as my cybersecurity is at least the same or better than my competitors, attackers will choose a party with less security and I will be safe	-2	1	0	0

Client requirement	44	Our business relationship demand our organization to have certain hardware, software, policies or procedures. Our client requirements are therefore a strong incentive to invest in our cybersecurity	1	3	0	0
	45	organizations are forced to be aware and invest because of the fines they may face from the GDPR	3	0	-5	-4
	46	ISO 27001 is an outdated standard. Nowadays it is not just about the technical approach to cyber security	0	-2	1	5
	47	I have lack of confidence in the company's level of security	-1	-1	1	2

5.6.6. Similarities between perspectives

The respondents also have some similarities in the way they think about a topic, for example they all disagree or agree to a statement and therefore have similar factor loadings. The statements are selected based on the joint agreement or disagreement. All statements should be positive or negative. See table 9 for factor loadings per statement.

The first similarity lies in the importance of a company's leadership. Every factor loads positive on the statement: "Half the battle is won when your company's leadership stresses the importance of company data and its integrity". Still a number of issues complicate the risk management-oriented cybersecurity, and support and awareness from the company's leadership is the only way to ensure that cyber security is addressed well throughout the whole organization (Bailey, Kaplan, & Rezek, 2014) . Another issue is that cyber risks are difficult to quantify. Multiple respondents mentioned that is was hard to communicate the urgency about risks to the top management, because they were unable to quantify the risks and needs. More engagement from the top management could make it easier to make decisions about the spending on security. And finally if the top management acknowledge the importance of cybersecurity this is easier to create awareness throughout the whole organization at all levels (Bailey et al., 2014). It is not a similarity, but what is interesting is that the awareness of the board is not a problem in all organizations as can be seen in different loadings to the statement: "The biggest problem is the awareness of the board. The top management is underestimating the cyber risks and not willing to invest" (-1, 2, 3, -3).

The second similarity is that the respondents agree with the idea that cybersecurity is often treated as separate business issue, however cybersecurity touches every business process. What can be noticed is that every factor loads positive or neutral on the statement: "Cyber risk management should be part of the whole risk management the respondents". Company's leadership is also a way to achieve this.

The third similarity is that the respondents agree that it is not possible to be a hundred percent safe, whatever one invest or does and that all organizations are an interesting target for cyber criminals (although some might think they are not). There are many issues that make hundred percent security impossible. One issue that is mentioned by the respondents are the end-users. The reason why some do not load as high as others is the second sentence of the statement. Another issue is the complexity of systems. This is not covered in a statement, but mentioned by the respondents as one of the main reasons why hundred percent safety is impossible to obtain.

The fourth similarity is that the respondents all load negative to the statement: "We do not work with personal data so we do not have to invest in cybersecurity measures". All respondents agreed that having personal data stored should not be the only incentive to invest in cybersecurity. This statement suggest that one does not have to invest if one does not work with personal data. However, there should be, according to the respondents, many more incentives to invest. It is huge mistake to think one does not have to invest in security if one does not store personal data (Lord, 2016). The stories that make headlines are the ones about theft of credit card data or personal information. As a result companies that do not store personal data often believe that they are not an interesting target (Henry, 2015). But all organizations have

information of value: so not having personal data stored does not mean one should not invest in cyber security.

The last similarity is that the respondents all load positive or neutral to the statement that client requirements are a strong incentive to invest in cybersecurity. And three of the four factors load positive to the statement that third parties may be a risk due to their bad security. Organizations mostly think about their own security but often forget that security incidents or major breaches also could happen via third parties. Certain standards or certification that everyone should meet or have, could help achieving better supply chain security and could ensure that at least a certain level of data security is being met (Lord, 2017).

Table 9 - factor loadings similarities between statements

	Statement with similar factor loadings	I	II	III	IV
S6	Half the battle is won when your company's leadership stresses the importance of company data and its integrity	2	1	4	1
S18	Some security risks we simply do not know or cannot imagine therefore we cannot be 100% safe	3	2	0	2
S41	We do not work with personal data so we do not have to invest in cybersecurity measures	-2	-2	-4	-5
S32	Our organisation is not an interesting target for cyber criminals, so we have nothing to worry about	-2	-3	-5	1
S14	Cyber risk management should be part of the whole risk management	3	0	0	3
S44	Our business relationship demand our organization to have certain hardware, software, policies or procedures. Our client requirements are therefore a strong incentive to invest in our cybersecurity	1	3	0	0
S10	Careless or unaware employees are the weakest link in the security system. Cyber security awareness training can be a part of the solution.	1	1	5	3

5.7.Conclusion

What can be concluded is that four different perspectives are found with the q-method. Within these four different perspective there are several factors that could explain the certain perspectives regarding cybersecurity investment behaviour. In the first group there is a concerned perspective. This perspective is characterised by its concern about unknown risks and social engineering. Most of the respondents in this perspective were from small and public organizations. In the second group there is a resilient perspective. This perspective is characterised by its focus on risk avoidance, incident response and resilience. In this perspective there is no difference between respondents from small and large organizations, but there were more respondents from private companies. In the third group there is a hierarchical perspective. This perspectives is characterised by its focus on the management and the unawareness of their employees. In this perspective the respondents were mostly from large private companies. The fourth group has a flexible perspective. This perspective is characterized by aversion towards rules and regulation and its focus on the risk assessment. In this perspective the respondents were mostly from small private companies.

6. Synthesis

This chapter is to answer the research questions, to discuss the results in a broader context, give recommendations and discuss limitations of this research and ideas for future research.

6.1.Conclusion

This section is to answer the research questions

1. *How is the cybersecurity investment decision-making process described in literature?*

Common in literature is that cybersecurity investments should be based on a comprehensive cost-benefit analysis or on a comprehensive risk assessment. Most methods try to estimate the best feasible decision and state that organizations must make a trade-off between the costs and benefits of investments. However, in cybersecurity the lack of reliable data is one of the main reasons that these economic methods are of limited use. The lack of reliable data can be due to multiple reasons: the constantly changing cyber threat environment or to the uncertainty about the probabilities of risk to the reluctance towards public sharing of information of attacks and the associated costs for organizations. These problems with the lack of reliable data lead to under or overinvestment in cybersecurity. To support decision-making in cybersecurity and to deal with uncertainty and complexity in decision-making, organizations acknowledge that cyber risk management is a way to support investment decisions. It is used to structurally deal with cyber risks and to manage it. It is important to correctly identify, characterize and understand risks. However, within the evolving cyber threat environment this can be slightly more difficult in practice than is described in theory. Thus, in considering the decision-making process regarding investments, it is expected that investments are influenced by organizational characteristics but also by the individual perspective of the decision-maker within that organization. Organizational factors that could influence the investment as described in literature could be the budget and size of an organization, but also external factors such as its reputation, client or third party requirements, rules and regulation or it could be influenced by a breach or an incident.

As mentioned above, within organizations there are individuals that actually make the decision how much to invest in cybersecurity and how to allocate the resources. In considering risk management, these individual decision-makers could fall back on typical psychological decision-making theories. Decision-making theory explains the way one thinks about risks and how one 'should' rationally choose from risky options. The prospect theory is a well-known decision-theory if it comes to making decisions that involve risks. In dealing with cyber-risk there are some biases people can be susceptible to. People may overweigh outcomes, show risk seeking behaviour, tent to choose measures with certain outcomes although these might not be the best measures, and people tend to overweigh and overestimate probabilities of rare events. Therefore it is expected that these decision-makers have an individual perspective on cybersecurity investments and these perspective could influence the investment strategy too. The question that remains is whether these decision-making effects exist in practice within the individual perspectives of decision-makers. In addition decision-makers are probably influenced by the organization they work as well. Several factors are researched with the q-method.

2. *What cybersecurity investment strategies exist in practice?*
3. *What organizational factors influence these investment strategies?*

Four types of investment strategies were found in practice. Within these four groups there are several factors that could explain certain investment behaviour. In the first group there are two factors. First the budget constraints are identified as a major concern and could explain the investment behaviour. Second is the factor that no incidents with serious financial damage happened that could explain that investment are not felt as necessary. In the second group the regulation has been indicated a major concern and could explain the investment behaviour. In the third group the risk identification could explain the investment behaviour. Within this group all types of risks have a very high priority. Lastly the fourth group the type of industry and the associated client requirements which makes that security receives a high priority could explain the high investment. See figure 19 below.

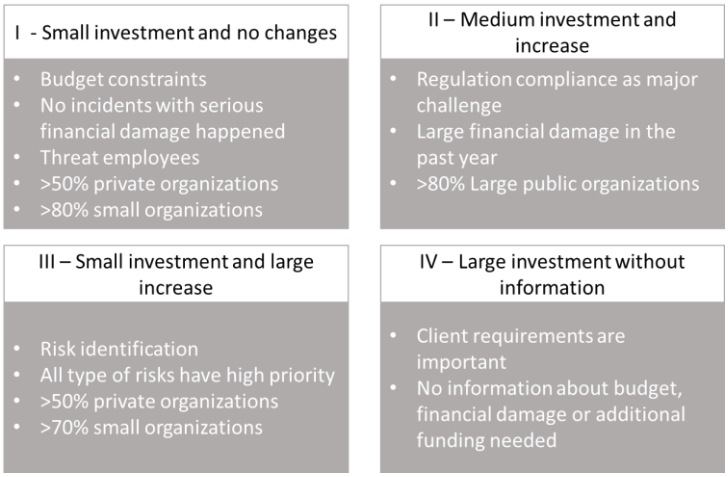

Figure 19 - Conclusions investment strategies

So, four types of investment strategies were found in practice with the latent class analysis. The main differences between the strategies is the starting investment and the change of this investment in the coming 12 months. These differences can be explained from the effect of organizational factors. The first significant organizational factor that influences the investment strategy is the type of organization categorized in public or private organizations. The second investment strategy that has been identified, consist for more than 80 percent of large public organizations. The other investment strategies consist for more than 55 percent of private organizations. So it can be concluded that for large public organizations one type of investment strategy has been found.

Second organizational factor that significantly influence the investment strategy is the budget of an organization. This is as expected in the literature: a smaller budget means smaller investment and vice versa. However the amount of organizations that have budget constraints is really high. In the first class almost 70 percent indicated that their main challenge is budget constraints and in the other classes this is almost 50 percent. The question that remains is if these constraint are due to the difficulties in assigning the costs, and especially the benefits, derived from cybersecurity? Or is it due to the difficulties in performing a risks assessment and convince the board about the needed investments? Or is it because of the externalities that are associated with cybersecurity investments? Or is it because of the lack of awareness of the board? What is also interesting, is that almost 60 percent of the first three investment strategies indicate that their main challenge is the lack of resources. Only the third investment strategy does not indicate this as a major challenge, but this seems obvious since their investment is very high.

The third and fourth organizational factors that significantly influences the investment strategy are the total revenue and the size of a company. This is, however, quite common sense. These organizational factors probably influence the initial investment. The bigger a company, or the higher the revenue, the higher the initial investment. For example, in the first strategy there is a small initial investment and more than 80 percent of this class is a small organization. With the latent class analysis, only absolute numbers are included, to really understand this relation the latent class analysis should have been performed with relative numbers. What is interesting is the difference in the change of budget for the coming 12 months. Both the first en third investment strategy include a large percentage of small organizations, but they differ in their change of budget in the coming 12 months. So this is probably influenced by other factors.

What is interesting is that the type of industry does not significant influence the cluster membership of the investment strategies, which is something that was expected upfront. The reason that this factor does not significant influence the cluster membership could be that almost 25 different industries were included.

Besides the organizational factors that are included in the latent class analysis there were also factors related to risk identification and external factors included. These factors are, however, linked to organizational factors. First external factors are the type of risks. Four type of cyber risks were used in the latent class method to predict the classes. Only two of the four cyber risks do significant influence the cluster membership. These are the threat of actions of people and the threat of failed internal processes. In all clusters almost 40 percent identified the threat of actions of people as high or even highest priority. And in all clusters almost 80 percent consider a careless employee as most likely source of attack. This indicates that employees are seen as a major risk in all clusters and confirms what is said about employees as the weakest link in the system in literature.

Second external factor that significantly influences the investment strategies are rules and regulations. The question whether fragmentation or regulation compliance is the biggest challenge or not to an organization significantly influence the cluster membership. Interesting is that within the cluster with almost 80 percent public or governmental organizations, 30 percent considers compliance with rules and regulations as a major challenge. Within the other clusters with mostly private organizations, this is around 15 percent. This could indicate that rules and regulation is not the major driving force as is thought in literature. What can be concluded is that public organizations are more driven by rules and regulations than private organizations. What is interesting is that the two strategies with an increasing budget for the coming 12 months have a higher percentage of organizations that had financial damage between 100.000 US Dollars and 1 million US Dollars than the other two investment strategies. Especially the class with the most public organizations included, has a high percentage of organizations with financial damage the past year. One might argue that public organizations have been more attacked and therefore have more financial damage, however this is probably not likely. Another reason might be that public organizations feel obliged to report incidents and are more likely to share information about incidents and finances than private organizations. As mentioned in literature research, private companies are not willing to share this information due to lack of economic incentives. Interesting is that the class with the highest investments has the highest percentage of organizations that do not know whether they had incidents that resulted in financial damage. What can be concluded is that in all classes there is, to a certain extent, incident response behaviour.

The third external factor that influences the investment strategy is the executive awareness or support. The percentage that indicates this as one of their major challenges is the lowest in the second class and thus the group with most public organizations. Within the other classes the percentage that indicates this as one

of their major challenges is around 30 percent. What can be concluded is that lack of executive awareness or support is an overall problem and can exist in all types of organizations.

4. *What are individual perspectives from decision-makers on cybersecurity investment?*
5. *Can the identified investment strategies be explained from individual perspectives of decision-makers?*

What can be concluded is that four different perspectives are found with the q-method. Within these four different perspectives there are several factors that could explain the certain perspectives regarding cybersecurity investment behaviour. In the first group there is a concerned perspective. This perspective is characterized by its concern about unknown risks and social engineering. In the second group there is a resilient perspective. This perspective is characterized by its focus on risk avoidance, incident response and resilience. In the third group there is a hierarchical perspective. This perspectives is characterised by its focus on the management and the unawareness of their employees. In this perspective the respondents were mostly from large private companies. The fourth group has a flexible perspective. This perspective is characterized by aversion towards rules and regulation and its focus on the risk assessment. See figure 20 below.

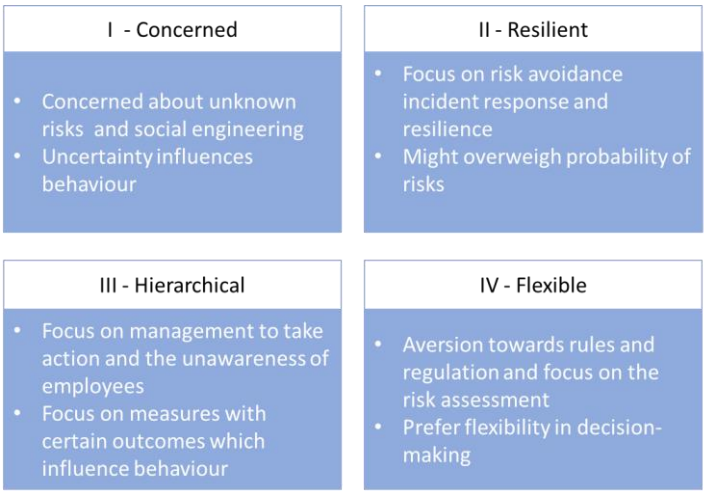

Figure 20 - conclusion perspectives

The question that remains is that if certain decision behaviour or biases as described in literature can be seen in the perspectives from practice. The first perspective is based on concerns, and if outcomes are not certain people tend to behave differently. People rather choose something with a certain outcome, than something with a higher utility but with an uncertain outcome. This concerned behaviour and uncertainty in the cyber environment could influence the investment behaviour. People might choose to invest in security measures with certain or measurable outcomes for example, instead of measures that might be a better option but have uncertain outcomes. So it can be concluded that due this concerned behaviour their might be some influences from decision-making biases in this perspective. The second perspective is based on resilience due to the fact that the respondents rather try to avoid risks and put focus on incident response and resilience than take proactive actions. What might have influenced this perspective is the fact that these respondents could overweigh the probability of risks happening and therefore focus on incidents response, because they might think that an incident will almost certainly happen. The third perspective is characterized by its focus on the management and the unawareness of the employees. This can be seen as a focus on tangible effects. The focus on the awareness of the employees and therefore reducing the probability of an incident can be felt like as a win. People rather choose something with a certain outcome,

so this perspective could be influenced by the idea that people rather choose something with certain outcomes and therefore put focus on employees. It is not clear if decision-making biases influence in the fourth perspective. However, this perspective could influence investments because they prefer flexibility in decision-making and focus on performing a risk assessment. They also mention that performing a risk assessment and corresponding cost-benefit analysis is difficult due to the lack of reliable information. As a result this could lead to over or under investment and therefore could influence the investment strategy.

The final question that remains is if and how an organization influences an individual perspective? Differences between perspectives of respondents from public and private companies and small and large companies is researched with the q-method too. However, due to the low number of respondents, the relation between these organizational factors and the type of perspective a respondent belongs to is not significant. This could, however, mean two things. First is that there is no significant relation and that individual perspectives are not influenced by these companies' characteristics, even if the number of respondents is higher in further research. This means that individuals who make decisions are not influenced by these organizational characteristics such as size and sector, but are influenced by the other factors. However, with the latent class analysis the influence of those two organizational factors does significantly influences the cluster membership. So this could also mean that the number of respondents is just too low to say anything about this relation.

What drives cybersecurity investment?

It can be concluded that multiple factors drives the cybersecurity investment of an organization. First are the factors related to the cyber risk identification, namely the threat of actions of people and social engineering and the threat of failing internal processes that influence the investment strategy. Second are the factors related to the executive awareness or support, this is also related to lack of resources and budget constraints and influence the investment strategy. Third, are the factors related to regulation and fragmentation compliance, these factors could influence the investment strategy but many question the effectiveness of regulation. And finally factors related to organizational characteristics influence the investment strategy, these are the total revenue, the type of organization (public/private), the size of a company and the total financial damage due to a cyber-attack in the past year. So this means that one cybersecurity investment strategy does not fit all. Organizations and individuals have different needs. The practical consequences for this conclusion is that there are different strategies for different target groups. Since the particular clusters are known, one could divide organizations and individuals into these clusters and can act from these perspectives.

6.2. Discussion

First of all, compared to literature the results from the field show additional value. This additional value lies mainly in the combination of the two different methods used to find different types of investment strategies, organizational factors that influence investment strategies and to find individual perspectives from decision-makers regarding cybersecurity investments. With the first research method a large dataset had been analysed (over 1700 respondents). Large datasets about investments, financial situations and organizational factors in cybersecurity are scarce. However, personal perspectives were not included in this dataset, therefore the second research method has been used, namely: the q-methodology. The q-method was to find individual perspectives of decision-makers and this results in an explanation about a population of perspectives. A disadvantage of this method, however, is that results are not an explanation about a population of respondents. This means that with the results of the q-method one cannot say anything about a certain population. But with the Global information security survey dataset one could say something about the population. Therefore this combination shows additional value.

In literature most investment strategies are discussed as cost-benefit analyses and risks assessments. The cost of the investment should be lower than the compared benefits and the investment should be based on an extensive cyber risk assessment. Multiple researchers propose economic models that determine the optimal amount of investment. The results are however, that not many organization determine their investment strategies based on a comprehensive cost-benefit analysis. Instead of investigating the optimal level of investment or trying to improve models or methods that estimate costs and benefits of security measures, this study analysed investment strategies in the first place, organizational factors that influence these strategies and personal perspectives that influence the investment strategies.

A similar study from Rowe and Gallaher, as mentioned in the literature study, conducted interviews to determine the decision-making process regarding cybersecurity investments. They have put focus on the type of internal and external information that is used in this decision-making process. This study, with the global information security survey and the interviews adds more external and internal organizational factors that influence this investment strategy. Where Rowe and Gallaher focus on information, this study includes how types of risks, availability of resources, the budget, executive awareness, revenue, size, number of employees, financial losses due to cyber incident and types of organizations and industries influence this investment strategy. In addition it combines these factors with personal perspectives. Rowe and Gallaher consider two types of strategies: proactive and reactive. Proactive puts emphasis on prevention, while reactive, puts emphasis on responding to known threats. This study build upon that with more different kind of strategies and factors that influence these strategies. However, there still needs to be more research about the role of decision-makers within companies, so who makes decisions and for example how much influence does a CISO has within an organization? And how much does the investment strategy influence the actual implementation, and who determines the implementation strategy and can this person influence the investment strategy too?

6.3. Limitations

Although meaningful results are found from the analyses, there are some limitations too. A few things are notable in the latent class analysis and the use of the Global Information Security survey dataset. The sample composition from the GISS is worldwide and a relatively large part of the respondents is from the financial sector, this could mean that the strategies are biased. However, the factor type of industry does not significant influence the cluster membership in the LCA, therefore the impact of this limitation is not expected as very large. Within this survey the type of organization is categorized in private, public and government or non-profit. However this is not very clear distinction. It is not clear what is meant with the difference between “public” and “government or non-profit”. However, it is not expected that this has a large impact on the outcomes of this study. In addition is the size of company categorized in small and medium companies as less than 1000 employees and everything above as large companies. However according to international standards a small company has less than 50 employees, a medium sized company has between 50 and 249 employees and a large sized company has greater than or equal to 250 employees. The size of a company does significantly influence the investment strategy, so it would be interesting if small and medium companies are categorized more specifically, and to investigate if it still significant influence the investment strategy. Furthermore, the dataset does not cover all aspects that were discussed in the literature research, namely: the context establishment, the risk assessment and the risk treatment strategy. So the list of factors that significantly influence cluster membership is not extensive: it could mean that more factors could influence the cluster membership. Since these factors are not included in the analysis, their effect on the investment strategies stays unknown. The factors that are not included are from the following categories from the risk management decision framework: the context establishment, the risk assessment and the risk treatment strategy.

In addition, as already mentioned in the conclusions, with the latent class analysis only absolute numbers are included, this has a great impact on the types of investment strategies. If relative numbers would have been used, probably different strategies would be found. So this is really something that needs to be considered in future research. For example, the conclusion that the size of organization influences the investment strategy: the larger an organizations the higher the investment is relatively common sense. If relative number would have been used this conclusion might be different.

A few things are also notable in the perspectives derived with the q-method. First of all, some respondents may have shown some socially acceptable behaviour, due to the sensitive information some statements entail. This could mean that some respondents may have shown an 'ideal' perspective, instead of what the company is actually doing. Some respondents mentioned they have lack of confidence in the company's level of security or in the awareness of the board, but just put statements about this topic on neutral. Another example what might have been socially accepted behaviour are the differences between how the interviewees think and behave and what the company actually does. The respondents might have ranked the statements to a socially acceptable result, however socially acceptable behaviour is not made explicit, therefore the impact on this study is not expected as big. Secondly, the number of respondents for this method was relatively low, as has already been mentioned in the conclusions. Due to this low number, there is no significant relation found between the organizational factors and the perspective a respondent shares. Thirdly, there are some statements that were actually two statements in one statement and therefore difficult to interpret. For example, some respondents agreed with the first part of the statement and disagreed with the second part of the statement. However, after some additional explanation the statements were clear to the respondents.

6.4. Recommendations and future research

The recommendations are based on the conclusions and discussion.

One cybersecurity investment strategy does not fit all. Organizations and individuals have different needs. The practical consequences is that there are different strategies for different target groups. Since the particular clusters are known, one could divide organizations and individuals into these clusters and can act from these perspectives. For example, large public organization can be classified in the second investment strategy, characterized by several drivers such as compliance with rules and regulations. With this knowledge specific advice can be given. So based on the investment strategies and perspectives one could classify any organization within one of the investment strategy classes or in one of the perspectives. However, more research is necessary whether this model can be used to make predictions about organizations that fit within one certain class. For example one half of the dataset can be used to create the model and the other half can be used to validate if predictions are correct. It is also interesting to make a distinction between proactive and reactive strategies as mentioned in the discussion and to determine how these types of strategies influence the investment strategy.

In addition more research is necessary into the effect of organizations on individual perspectives. This is to answer the questions whether certain perspectives only consist in certain organizations based on organizational factors or not. For example, the fourth perspective is characterized by its aversion towards rules and regulations. It is interesting to know whether this perspective is more common in one particular organization or not. One investment strategy is, for example characterized by the number of public organizations and by the challenge to comply with rules and regulations. It would be interesting to know if the perspective mentioned above is connected with that type of organization.

Based on investment strategies, their drivers and the individual perspectives it might also be possible to classify the groups in terms of level of security. The level of security can be expressed in a level of maturity. The maturity level can be useful in guiding an organization in the process towards the highest possible maturity level. It can also be used to evaluate an organization's current status of security. So these maturity models can help in determining where organizations currently stand and can help in developing security programs and processes to effectively prevent, detect, respond to, and recover from cyber-attacks. Multiple models exist, a model based on cybersecurity is the community cyber security maturity model from White (2007). Within this model each maturity level indicates the type of threats and activities being addressed at that level. However, the combination of the strategies and perspectives with the maturity level of safety needs more research.

As mentioned in the conclusions the budget constrains is one of the key drivers in cybersecurity investments. But why are these budget constraints in place? What remained from the conclusions are the questions if the budget constraint are due to the difficulties in assigning the costs and especially the benefits derived from cyber security? Or is it due to the difficulties in performing a risks assessment and convince the board about the needed investments? This could be the case since, many respondents mentioned that it was often difficult to explain how security spending benefit the business to the management. As a result the management may hesitate to invest in cybersecurity measures. What is important here is that the management can address the issue by making the cybersecurity issue part of the overall risk management of the business. More research is needed into the reasons behind budget constraints.

As mentioned in the conclusions the financial damage is the highest in public organizations. The question that remains is: if this is really the matter or do other, and especially private, organizations do not share this information? One of the main issues for decision-making is this lack of reliable information and lack of resources. The government can intervene in the market if there is market failure and this could for example be: imperfect information (Rowe & Gallaher, 2006). Therefore the government could play a role in providing information about threats, risks, costs and benefits and impact of incidents. It could help in the collection of data on cost-effective information, but also in providing resources for extra research in this topics. One could also say that rules and regulations are important in the issue with information sharing. But as mentioned in the conclusions rules and regulations are not the major driver for all organizations, especially not for private organizations.

To address the issue that rules and regulations do not drive cybersecurity investments for all organizations, there could be another role for the government, namely to better control on the compliance of regulation. Regulation is something that can provide incentives to enhance cybersecurity for organizations. However, the results show that multiple respondents are not sure whether regulations are an efficient way to increase cybersecurity. Regulation could increase the overall level of security, but the respondents mentioned that an one size fits all solution does not lead to efficient solutions. Regulation alone is not enough to create a basis of cybersecurity. The control on the compliance is considered very important. Examples of activities or level of security that should be met are very difficult since cyber security is not just something that can be achieved through a checklist, however the threat of legal actions from being out of compliance should be a lot higher. Based on the results, there were mixed feelings about the regulation regarding cyber security, many question whether it is efficient or not and that compliance can be very costly. Regulation can be more prescriptive, but then again, the question remains if this lead to more security and the respondents mentioned that this lead to high compliance costs. Therefore regulation could be more flexible and it should give organizations the flexibility to choose amongst solutions which fits their budget and it should give organization to ability to see it as a baseline for security and organizations should be flexible in how to select their measures.

As mentioned in the conclusions the lack of executive awareness highest in private organizations. In general the management involvement is important, since cybersecurity is more than just an IT problem. Organizations should at least implement a proactive strategy, which means investing in enhancing their cybersecurity, but also an integrated and holistic risk management strategy is proved to be important. In addition, organizations may choose to implement cyber insurance, however this needs more research, since the usefulness is still questioned. In addition there still needs more research about the role of decision-makers within companies, so who makes decisions and for example how much influence does a CISO has within an organization? And how much does the investment strategy influence the actual implementation, and who determines the implementation strategy and can this person influence the investment strategy too? And more research is needed to determine the efficiency of security measures which could make it easier to determine where to allocate ones resources.

6.4.1. Recommendation for GISS

Finally there are some recommendations for improvement of the global information security survey:

- Include personal questions to combine organizational factors and perspectives from individual decision-makers.
- It is important to determine in advance what one wants to analyse from this dataset and create variables that are nominal, ordinal, interval and ratio in accordance. Then it is easier to conduct analyses.
- Include questions that determine who makes decisions regarding cybersecurity investments and what information is used to make these decisions. For example, how much influence has the CISO in this decision-making process?
- Include questions about cyber risk management. For example, to what extend is cyber risk management included in the organization? Then it can be determined to what extend cyber risks management is used in practice compared to in theory.
- In the GISS It is not clear what is meant with the difference between “public” and “government or non-profit”. This needs to be specified.
- Large amount of the respondents is from the financial sector, this might give a biased representation. Try to include more different sectors in the GISS.
- The size of company categorized in small and medium companies as less than 1000 employees and everything above as large companies. However according to international standards a small company has less than 50 employees, a medium sized company has between 50 and 249 employees and a large sized company has greater than or equal to 250 employees. So this could be more specified in the GISS.
- Include questions about proactive and reactive strategies. Then this can be used to research the relation between strategy, investments, organization and decision-makers.

7. References

Almann, L., & Kelly, J. J. (2008). CRS report for Congress - Economic Impact Cyber-Attacks. *Policy Review*, 39+. https://doi.org/Article

Bailey, T., Kaplan, J., & Rezek, C. (2014). Why senior leaders are the front line against cyberattacks | McKinsey & Company. Retrieved August 3, 2017, from http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks

Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10–11), 706–719. https://doi.org/10.1016/j.telpol.2009.09.001

Berg, J. Van Den, Zoggel, J. Van, Snels, M., Leeuwen, M. Van, Boeke, S., Koppen, L. Van De, … Bos, T. De. (2014). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. *NATO STO/IST-122 Symposium in Tallin*, (c), 1–10.

Bisogni, F., Cavallini, S., & Trocchio, S. D. I. (2011). Cybersecurity at European Level: The Role of Information Availability. *COMMUNICATIONS & STRATEGIES, 81, 1st Q*, (2010), 105–125.

Bojanc, R., & Jerman-Blazic, B. (2008). Towards a standard approach for quantifying an ICT security investment. *Computer Standards & Interfaces*, *30*(4), 216–222. https://doi.org/10.1016/j.csi.2007.10.013

Cebula, J. J., & Young, L. R. (2010). A Taxonomy of Operational Cyber Security Risks CERT ® Program. Retrieved from http://www.sei.cmu.edu

de Wit, J. (2015). *Research Proposal*. Technical University Delft.

Dynes, S., Goetz, E., & Freeman, M. (2008). Cyber Security: Are Conomic Incentives Adequate? *International Federation for Information Processing*, *253*, 15–27.

European Commission. (2017). What is an SME? Retrieved June 1, 2017, from http://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

Exel, J. Van, & Graaf, G. de. (2005). Q methodology : A sneak preview. *Social Sciences*, *2*, 1–30. Retrieved from http://qmethod.org/articles/vanExel.pdf

EY. (2016). *EY's 19th Global Information Security Survey 2016-17*. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/%24FILE/GISS_2016_Report_Final.pdf

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

Gordon, L. (2007). Incentives for Improving Cybersecurity in the Private Sector : A Cost-Benefit Perspective Benefits Derived from Cybersecurity Investments, 1–9.

Gordon, L. a., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L., Loeb, M. P., & Sohail, T. (2003). A Framework for Using INSURANCE FOR CYBER-RISKMANAGEMENT. *Communications of the ACM*, *46*(3), 81–85. https://doi.org/10.1145/636772.636774

Henry, S. (2015). Top 5 Cybersecurity Mistakes Companies Make and How to Avoid Them ». Retrieved August 3, 2017, from https://www.crowdstrike.com/blog/top-5-cybersecurity-mistakes-companies-make-and-how-to-avoid-them/

Johnson, J. G., & Busemeyer, J. R. (2010). Decision making under risk and uncertainty. *Wiley Interdisciplinary Reviews: Cognitive Science*. https://doi.org/10.1002/wcs.76

Johnson, S. (2017). Social engineering attacks: Is security focused on the wrong problem? Retrieved August 4, 2017, from http://searchsecurity.techtarget.com/feature/Social-engineering-attacks-Is-

security-focused-on-the-wrong-problem
Kahneman, D. (2011). *Thinking , Fast and Slow (Abstract)*. *Book*. https://doi.org/10.1007/s13398-014-0173-7.2
Kahneman, D., & Tversky, A. (1979). Kahneman & Tversky (1979) - Prospect Theory - An Analysis Of Decision Under Risk.pdf. *Econometrica*. https://doi.org/10.2307/1914185
Kaufman, L., & Rousseeuw, P. J. (2005). *Finding Groups in Data: An Introduction to Cluster Analysis*. *Wiley-Interscience* (Vol. 33). https://doi.org/10.1007/s00134-006-0431-z
Kovacs, E. (2014). Global cybersecurity spending to reach $76.9 billion in 2015: Gartner. Retrieved April 19, 2017, from http://www.securityweek.com/global-cybersecurity-spending-reach-769-billion-2015-gartner
Li, P., Mao, Y., & Zdancewic, S. (2003). Information integrity policies. *Proceedings of the Workshop on Formal Aspects in Security & Trust (FAST)*, 53–70. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.9762&rep=rep1&type=pdf
Lord, N. (2016). Data Security Experts Reveal the Biggest Mistakes Companies Make with Data & Information Security | Digital Guardian. Retrieved August 3, 2017, from https://digitalguardian.com/blog/data-security-experts-reveal-biggest-mistakes-companies-make-data-information-security
Lord, N. (2017). Supply Chain Cybersecurity: Experts on How to Mitigate Third Party Risk | Digital Guardian. Retrieved August 3, 2017, from https://digitalguardian.com/blog/supply-chain-cybersecurity
Magidson, J., & Vermunt, J. K. (2002). Latent class models for clustering: A comparison with K-means. *Canadian Journal of Marketing Research*, *20*(1), 37–44. https://doi.org/ISSN: 1614-1881
Magidson, J., & Vermunt, J. K. (2004). Latent class models. *The Sage Handbook of Quantitative Methodology for the Social Sciences*, 175–198. https://doi.org/10.3102/0091732X010001305
Meijeren, M. (2016). *Perspectives on cyber security*. Technical University Delft.
Meulen, N. Van Der. (2015). Investeren in Cybersecurity. Retrieved from https://www.wodc.nl/images/2551-volledige-tekst_tcm44-602708.pdf
Michael P. Gallaher, Brent R. Rowe, Alex V. Rogozhin, A. N. L. (2006). Economic analysis of cyber security. *Air Force Research Laboratory*, (July), 110.
NCSC. (2016). Europese richtlijn voor cybersecurity aangenomen | NCSC. Retrieved April 24, 2017, from https://www.ncsc.nl/actueel/nieuwsberichten/europese-richtlijn-voor-cybersecurity-aangenomen.html
Neil, N. F. and M. (2012). The Need for Causal, Explanatory Models in Risk Assessment 2.1, 31–50.
Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' behavior towards IS security policy compliance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–10. https://doi.org/10.1109/HICSS.2007.206
Refsdal, A., Solhaug, B., & Stolen, K. (2015). *Cyber-Risk Management*. SpringerBriefs in computer science. https://doi.org/10.1007/978-3-319-23570-7
Roeser, S., Hillerbrand, R., Sandin, P., Peterson, M., Trautmann, S. T., & Vieider, F. M. (2012). *Handbook of Risk Theory*. *Handbook of Risk Theory*. https://doi.org/10.1007/978-94-007-1433-5
Rouse, M. (2017). What is confidentiality, integrity, and availability (CIA triad)? - Definition from WhatIs.com. Retrieved March 16, 2017, from http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA
Rowe, B. R., & Gallaher, M. P. (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. *The Fifth Workshop on the Economics of Information Security (WEIS06)*, 1–23.
Rue, R., Pfleeger, S. L., & Ortiz, D. (2007). A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making. *Workshop on the Economics of Information Security, 2007*, (2003), 1–23. Retrieved from http://weis2007.econinfosec.org/papers76.pdf
Sahlin, P. N.-E. (2012). Unreliable Probabilities, Paradoxes, and Epistemic Risks. In *Handbook of Risk Theory* (pp. 477–498). https://doi.org/10.1007/978-94-007-1433-5
Sales, N. A. (2013). Regulating Cyber-Security. *Northwestern University Law Review*, *107*(4), 1503–1568.
Schneier, B. (2008). The psychology of security. In *Lecture Notes in Computer Science (including subseries*

Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (Vol. 5023 LNCS, pp. 50–79). https://doi.org/10.1007/978-3-540-68164-9_5

Shackelford, S. J. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*(4), 349–356. https://doi.org/10.1016/j.bushor.2012.02.004

Shim, W. (2010). INTERDEPENDENT RISK AND CYBER SECURITY : AN ANALYSIS OF SECURITY INVESTMENT AND CYBER INSURANCE By Woohyun Shim Communication Arts and Sciences – Media and Information Studies ABSTRACT INTERDEPENDENT RISK AND CYBER SECURITY : AN ANALYSIS OF SECURITY INVES.

Singer, P.w, Friedman, A. (2014). Cybersecurity and Cyberwar. *Igarss 2014*, (1), 1–5. https://doi.org/10.1007/s13398-014-0173-7.2

Siponen, M., Pahnila, S., & Mahmood, A. (2007). Employees' adherence to information security policies: An empirical study. *IFIP International Federation for Information Processing*, *232*, 133–144. https://doi.org/10.1007/978-0-387-72367-9_12

Soo Hoo, K. J. (2000). How much is enough? A risk management approach to computer security. *Ph.D. Dissertation, Stanford University, USA*, (June), 99. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.4127&rep=rep1&type=pdf

Vermunt, J. K., & Magidson, J. (2005). Latent Gold 4.0 User's Guide, 256.

Watts, S., & Stenner, P. (2005). Doing Q methodology: theory, method and interpretation. *Qualitative Research in Psychology*, *2*(1), 67–91. https://doi.org/10.1191/1478088705qp022oa

Appendices

Appendix A - Literature research

Search engine / source	Terms used / Title

Google Scholar	• "Cybersecurity'' in combination with:
	  ○ decision making
	  ○ investment strategy
	  ○ risk management
	  ○ incentives
	• Cyber risk management
	• Risk management
	• Decision making theory
	• Cyber risk evaluation
	• Cybersecurity
	• Q-method/Methodology
	• Decision making under uncertainty

TU Delft library	Cyber risk management
(de Wit, 2015) used as a source	"Handbook of risk theory" (Roeser et al. 2012)
Meijeren, M (2017) used as a source	• Cebula, J., Young, L., & Popeck, M. (2010). *A Taxonomy of Operational Cybersecurity Risks*. *Advances in Information Security*. • Choi, N., Kim, D., & Goo, J. (2006). Managerial Information Security Awareness' Impact on an Organization' s Information Security Performance. • Brown, S. . (1993). A primer on Q methodology. Operant Subjectivity. *Operant Sub/ectlvlty, 1*

Appendix B - Latent class analysis: Model estimation

		LL	BIC(LL)	Npar	L^2	BIC(L^2)	df	p-value	Class.Err.	L2 reduction
Model1	1-Cluster	-8135,45	16419,6	20	1630,56	-1544,37	427	7,50E-140	0	
Model2	2-Cluster	-7812,21	15929,27	41	984,0845	-2034,7	406	6,50E-50	0,0078	39,65
Model3	3-Cluster	-7606,78	15674,55	62	573,2222	-2289,42	385	1,40E-09	0,0965	64,85
Model4	4-Cluster	-7533,47	15684,08	83	426,6096	-2279,89	364	0,013	0,1428	73,84
Model5	5-Cluster	-7489,97	15753,22	104	339,6015	-2210,75	343	0,54	0,1392	79,17
Model6	6-Cluster	-7456,84	15843,1	125	273,3396	-2120,87	322	0,98	0,138	83,24
Model7	7-Cluster	-7435,88	15957,34	146	231,4298	-2006,64	301	1,00	0,1477	85,81
Model8	8-Cluster	-7420,55	16082,82	167	200,7727	-1881,15	280	1,00	0,2104	87,69
Model9	9-Cluster	-7410,43	16218,72	188	180,5276	-1745,25	259	1,00	0,2198	88,93
Model10	10-Cluster	-7402,8	16359,6	209	165,2634	-1604,37	238	1,00	0,285	89,86

Appendix C – Latent class analysis: GISS questions included

Questions	Answer options
Q1. What is your organization's total annual spend on information security (approximately, including people, process and technology costs)? (Select one)	Less than US$1 million Between US$1 million and US$2 million Between US$2 million and US$10 million Between US$10 million and US$50 million Between US$50 million and US$100 million Between US$100 million and US$250 million More than US$250 million Don't know
Q3. Which of the following describes the change in your organization's total information security budget in the coming 12 months? (Select one)	Will increase by more than 25% Will increase between 15% and 25% Will increase between 5% and 15% Will stay approximately the same (between +5% and 5%) Will decrease between 5% and 15% Will decrease between 15% and 25% Will decrease by more than 25% Don't know
Q4. How much additional funding is needed to protect the company, in line with management's risk tolerance? (Select one)	0-25% 26-50% 51-75% 76 -100% Over 100% Don't know
Q5. How likely is it that any of the following events would encourage your organization to increase your information security budget in the coming 12 months? (Select one response for each topic)	Discovery of a breach with, apparently, no harm done Discovery of a breach that resulted in the attackers impacting the organization A DDoS attack A cyber attack on a major competitor A cyber attack on a supplier M&A activity A physical loss of confidential corporate information on a mobile device A physical loss of customer information on a mobile device Other (please specify) (text response for other)

Q7. What information in your organization do you consider is the most valuable to cyber criminals? (Select the top 5 you consider most valuable for your organization, and rank them from 1 as the most valuable, to 5 as less valuable)	Customer personal, identifiable information Customer passwords Research and development (R&D) information Information exchanged during mergers and acquisition (M&A) activities Patented Intellectual Property (IP) Non-patented IP Senior executive/Board member personal information (inc. email accounts) Company financial information Supplier/vendor identifiable information Supplier/vendor passwords Corporate strategic plans Don't know Other (please specify)
Q8. Which threats* and vulnerabilities** have most increased your risk exposure over the last 12 months? (Rate all of these items, with 1 as the highest priority, down to 5 as your lowest priority)	Vulnerability — outdated information security controls or architecture Vulnerability — careless or unaware employees Vulnerability — related to cloud computing use Vulnerability — vulnerabilities related to mobile computing use Vulnerability — related to social media use Vulnerability — unauthorized access (e.g., due to location of data) Threat — cyber-attacks to disrupt or deface the organization Threat — cyber-attacks to steal financial information (credit card numbers, bank information, etc.) Threat — cyber-attacks to steal intellectual property or data Threat — espionage (e.g., by competitors) Threat — fraud Threat — internal attacks (e.g., by disgruntled employees) Threat — malware (e.g., viruses, worms and Trojan horses) Threat — natural disasters (storms, flooding, etc.) Threat — phishing Threat — spam Threat — zero-day attacks
Q9. Who or what do you consider the most likely source of an attack? (Select all that apply)	Malicious employee Careless employee External contractor working on our site Customer Supplier Other business partner

	Criminal syndicates State sponsored attacker Hacktivists Lone Wolf hacker Other (please specify) (text response for other)
Q34. What are the main obstacles or reasons that challenge your Information Security operation's contribution and value to the organization? (Select all that apply)	Lack of skilled resources Budget constraints Lack of executive awareness or support Management and governance issues Lack of quality tools for managing information security Fragmentation of compliance/regulation Other (please specify) (text response for other)
Q39. What is your estimate of the total financial damage related to information security incidents over the past year (this includes loss of productivity, regulatory fines, etc.; the estimate excludes costs or missed revenue due to brand damage)? (Select one)	Between $0 and $100,000 Between $100,000 and $250,000 Between $250,000 and $500,000 Between $500,000 and $1 million Between $1 million and $2.5 million Above $2.5 million Don't know Had no information security incidents that resulted in any financial damage

Appendix D - Q-method: Summary interviews

Interview 1: Expert cyber security from governmental organization

Budget as constraint for cybersecurity

According to M 10 percent of the ICT budget must be spend on cybersecurity. However in practice it is difficult to convince the director that this budget is needed. It is very difficult as a security officer to argue the needs, because it is not always present or tangible. The needs become clearer once a breach has happened. But then you are too late. So to argue that one needs to invest at least 10 percent of the budget on cybersecurity is tough. And why not 20 percent or 30 percent? This too is a difficult question and almost impossible to know.

The question many directors have is to what are you protecting yourself from? Because if nothing happens does that mean that your security is perfect or that nothing is happening or has happened? And as a security officer it is your job to translate the technical part about attacks to the directors and convince them that attacks do happen and that budget for cybersecurity is needed. But this is rather difficult. The only thing that is rather clear, is the assets you want and need to protect.

The tangibility of assets determines investment

According to M. tangible assets ensure that security gets more priority. For example, with the government the assets are mostly about personal information and a loss of personal information is less tangible than the loss of 2 million US dollar. With private parties on the other hand the financial losses are much more tangible. Another example is that of Rijkswaterstaat which must protect the critical infrastructure in the Netherlands. If there is an open sluice this could have major physical consequences. Or the Belastingdienst, if here is a loss of money this could have major consequences for the society. Therefore these governmental organisations give cybersecurity a higher priority and invest more. So security becomes greater as the tangibility of what you want to protect is greater. However M. also states that more investment does not mean better security. Money is not the objective, but smart investments is. According to M. organizations only invest in their cybersecurity if no security could lead to monetary loss.

Only investments after breach

M. states that many organizations only invest in their cybersecurity after a breach has happened. As an example M. mentioned the latest cyber-attack: 'Wannacry'. After this attack multiple organizations' eyes have been opened. Organizations only take action if something has happened such as loss of monetary value, income loss, unavailability of systems, income loss or penalties for privacy. It must have financial impact before organizations do something about their cybersecurity.

The difference between the private sector and the government is the type of impact. In the private sector it is mostly about monetary loss and with governments it is more about reputation and political damage.

Protection of core assets as driver

The Ministry of Security and Justice invest in their cybersecurity to protect their core values, personal credentials, the interest of external parties and extern countries. It needs to protect their own business processes. The protection in place depends on which assets the ministry has. And according to M. all organizations should base their cybersecurity on their assets and not on something else.

Regulation as driver

However as M. states many organizations only invest in their cybersecurity because of regulation and are not willing to do extra security. As a government, you cannot force parties to invest more in their security. Large companies however do understand their own interest and invest what is needed. However SMEs are increasingly difficult and as a government you cannot enforce that. You can, however, point out the risks

they are facing. But cannot force to invest in cybersecurity. So companies do what regulation tells them to do, and as a government it is difficult to push them to do more.

In addition M. mentioned the following: “Everything is okay, so why would I invest?” as an example why professionals do not invest in their security.

Money as driver

Money is the key driver why organizations invest in their cyber security. There are some differences between large companies and SMEs. SMEs do not have the same amount of money to invest and rather not invest if not needed, and probably will wait until a breach happens. Banks are mostly motivates because clients need to be satisfied, unsatisfied clients means no money. For large organizations as Shell and ASML knowledge is also important. But knowledge is in the end also money. Energy sectors are morally more responsible, because they are partly government.

The largest leaks are within the healthcare. The intentions of the healthcare sector are very good and are willing to do invest, but simply do not have enough money for cybersecurity. Regulation is getting stricter so now the need to invest.

The governments’ motivation is less about money and more about the responsibility raised by politics. But the problem within the government is the lack of money available for cyber security. Only when something happens money will become available.

Interview 2: Expert cyber security from private organisation

Media attention and privacy regulation

According to J there are two main drivers that make people more aware of the cyber risks they could face. The first is the many media attention that cyber-attacks are getting today. Secondly is the privacy legislation that compels companies which are handling personal data to implement a certain level of security. If companies fail to do so, they may face fines. So first people were quite unaware of the risks they were facing but because of these two factors people became more aware of cyber risks and are actually going to do something about it. So media attention and regulation are one of the key drivers for people to invest. Because if one does not comply with rules and legislation one could face tremendous fines. In particular J mentioned the GDPR as an important driver.

Best practice approach

J mentioned that companies compare themselves to their competition and partly determine their cybersecurity investment strategies on what the competition is doing. This approach is simply said: the same kind of investment as your competitors. Small SME companies do not pursue the security of banks but compare themselves with others in the same industry and must definitely be one of the bests. If competitors are doing less, they might face bigger risks. Companies actually think as long as my cybersecurity is better than my competitors then I will be safe. However, you should always pursue a minimum level of cyber security regardless of what others do.

Risk management and money

Depending on the size of a company risk management is used to address cyber risks. Large companies have probably more budget available and face bigger risks compared to smaller companies. Another important aspect that J mentioned is the impact of a cyber-attack. As the impact grows, more investments will be made. Or at least cybersecurity will be at a higher priority. He mentioned that if the dependency on the availability of the systems grows, cyber security will perceive a higher priority.

J mentioned that money is an important driver for cyber security investments. It is important that the security professionals are able to show that an incident could lead to monetary loss, loss of customers,

reputational damage etc. If the security professionals fails to do so, the top management will probably not be motivated to invest in security. The benefit need to exceed the cost and therefore the cost-benefit analysis is an important aspect.

J mentioned that in multiple organizations systems are being protected in the same way, despite the fact that the risk classification is not the same for both the systems. It may therefore happen that data that does not require protection get the same security as data that needs high protection. This could be a waste of investment. It is therefore better to distinguish between systems that need to be well protected and systems that need less security. So it is important to invest wisely, although this is difficult.

Interview 3: Expert cybersecurity from private organisation

I have seen a lot more organizations who are concerned about advanced attack than you would see five to six years ago. Nowadays you see much more attacks that have become more sophisticate, for example on behalf of states, and these attacks are doing more harm. So A. mentioned that nowadays the consequences of being attacked are greater. Attacks are much more common in the daily news and it affects much more organizations. Combined with the upcoming privacy laws and penalties, the risk for organizations are becoming much more tangible. What you saw with cyber-attacks, was that the odds were very unclear and the impact was unclear too. Now the likelihood of an attack becomes clearer due to more information that is available.

He mentioned that many organizations struggle with managing configurations and assets. It is very important that an organization knows what their critical assets are. Therefore is risk management and risk assessment are two very important things a company should do in order to protect itself from cyber-attacks. On the other hand, with risk management the costs and benefits should be considered too. What risks do you accept as an organization and what not?

With multiple organizations budget becomes less of a constraint. The budget is considered as less important. This is probably due to the fact that the awareness regarding cybersecurity and cyber risks has grown. However it is still unclear in what measures one has to invest. More investment does not mean better security. A mentioned that probably less investment would lead to better security because it is all about prioritization. What you see in practice is that a lot of organizations invest in protecting the entire organization while you could only secure a small part of the organizations as well. For example, organizations are protecting information that is publicly available. Then you lose a certain amount of your budget to useless investments.

Interview 4: CISO from government

Cyber threats are becoming increasingly advanced and happening more often. Therefore incident response is becoming more important. A good incident response plan has to be ready in case of an attack happens. It Is not a question if an attack will happen, but when. Cyber-attacks are increasing because many systems are the same. Therefore it is important to implement different type of systems: divide and conquer. This mono-culture is a threat in cybersecurity. If one uses only one system, an attacker only needs one virus to enter the entire system. So spreading risks is very important.

Cybersecurity need to be seen as a process and not as a state. One have to constantly manage cyber risks and determine the cyber threat environment due to the fact that it is constantly changing. Therefore cyber risk management needs to be a dynamic process in order to understand the cyber threat environment, but also to determine what measures one needs to take. Everything that seems safe today does not have to be safe tomorrow. What you see is actually an asymmetrical battle between cyber criminals and security of systems. An attacker only needs one vulnerability, but the defender must keep the whole systems safe. As a result, cybersecurity developments are incredible fast. That means that you should have an organizations that has some degree of flexibility. To respond quickly to new threats that might occur. But this is (especially

for the government) difficult. Within the government a lot is being standardize but this doesn't help flexibility.

H mentioned that the larger your organizations the more difficult it gets to ensure the desired rate of response in times of failure. For example with wannacry, one does not have that much time. Another issue is that software vendors deliver patches under a very high time pressure. This indicates that patches are not always good and might contain bugs. Therefore, some organizations first want to test the patches, and of course this takes time. And this time is something you do not have with outbreaks such as wannacry.

Interview 5: CIO from private organisation

We are working on a cybersecurity department, also as service to customers. So this means that there is definitely awareness. The cybersecurity for bridges and other industrial project are as important as cybersecurity is to banks.

Cyber-attack could definitely damage our reputation. I think that reputational damage has a larger impact than if the systems are down for a couple of days.

I believe that at least 95% of the hacks are because of human error. There will always be someone who does something wrong, clicks on the wrong link etc. Awareness training could help but still it is difficult to make people understand cybersecurity and to create more awareness. Regarding cyber security regulation I think that regulation lacks behind.

Interview 6: CISO from private organisation

Social responsibility, Reputation and Regulation

We are entirely focussed on the healthcare sector which includes mental health care, nursing and hospitals. So apart from all business risks we have a big social responsibility. If something goes wrong with one of our main clients the consequences can be very big. So the main driver to us is this social responsibility and the social impact cyber incidents could have.

Second most important driver is our reputation. If one of our clients get hacked it directly influences our reputation. In practice companies will not directly leave after reputational damage, but customers will leave in the long run if your reputation has been damaged once. In cybersecurity trust is hard to gain but easy to lose.

Third is the regulation regarding privacy and personal data. Multiple clients are trying to comply with the coming GDPR in May 2018. However, the action is still quite limited. What would help if a large penalty would occur in the health sector, probably then there will be more action in the health care sector.

What also helps is the media attention data breaches are getting nowadays. It helps to highlight attention, however attention is needed not only for the protection of personal data but for cybersecurity as a whole. I think that if you manage to secure the personal data, then the organisational overall security is likely to be good as well. So this privacy regulation is an important driver. But keep aware of the fact that protection of personal data is not the only thing that matters, there is much more than that.

We determine what needs to be protected but we will not define different types of data. All data needs the highest protection, because all data is rather personal and sensitive. So it does not matter to make a distinction.

J mentioned that the ISO standards are just checklists and not rocket science. So everybody can comply with those standards. The most important thing is the awareness of the board. There are still managers who do not think cyber security is necessary, even in our company J. mentioned. For example, a phishing campaign is very expensive, and difficult to convince the effectiveness towards the board of the company. The board needs to consider the profits throughout the whole organisations and in cybersecurity profits

are very difficult to make tangible. So budget could be a constraint if it not clear how much to invest, and not clear what the efficiency of measures is. However, efficiency of measures is very difficult to determine.

Back-ups and recovery plans

Back-ups and recovery plans are the most important thing to have. Some companies do not worry because for multiple years in a row nothing has happened to them. But nowadays it is not clear if you have been attacked or not. And a company only needs one accident to ruin its reputation. J mentioned that he cannot image that companies do not have back-ups because it cost too much. If this is the case, back-ups are not on your priority list.

J mentioned that a cyber-attack could have positive effects too, if the impact is not too big. For example, more awareness of your employees. Humans are the weakest link in the system, so awareness is very important.

Appendix E – Q-method: Selection statements

Context establishment

In the category context establishment there are four sub categories. The first statement regarding the sub category assets is based on how cyber risk assessments should be done in theory. In theory it is important to start with the identification of ones assets. Therefore this statement is selected. Statement number two is selected because this is the main opinion of the interviewees: they mention that they often find it very difficult to perform risk assessments due to a changing threat environment. Information security is often explained as the protection or preservation of three key aspects of information: availability, integrity, and confidentiality as mentioned in chapter three. What the interviewees mentioned is that the focus of a manager could be on one of these aspects and that for example, one of the aspects is more important than another. Therefore these statements are included, to capture the perspectives that one of the aspects is more important than others. See table 10 for an overview of the statements.

Nr.	Category framework	Statement
	Context establishment	
1	Assets	Organizations should base their cybersecurity on their assets and not on something else.
2		It is very difficult to determine the cyber risks due to the fact that threats continue to evolve.
3	Confidentiality	An employee or hacker who leaks vital information to a competitor is our biggest concern
4		Failure to properly secure and protect confidential information can lead to the loss of business and clients and is our biggest concern
5	Integrity	Integrity is more important than the availability of the systems. For example we want to keep some information secret and that has priority number one.
6		Half the battle is won when your company's leadership stresses the importance of company data and its integrity
7	Availability	Back-ups and disaster recovery plans are too costly
8		A day without operating systems can cause major financial damage to our organisation

Table 10 - statements about context establishment

Cyber risk identification

In the category of cyber risk caused by human threats there was amongst the interviewees two main opinions: humans are the weakest link in the security system and social engineering is becoming increasingly advanced. In the category system and technology failure many mentioned that the availability of the system due to technical failure can have huge consequences. What is striking about the interviewee's responses is that they indicated that patching systems is one of the biggest problems that cause system failure. Therefore these two statements have been chosen, which both focus on patching systems. In the category failed internal processes the interviewees showed very clearly that one of the biggest problems is the awareness of top management. Many have difficulty in convincing the board of the necessary investments but also convincing them about the risk they face.

In the section external events the most common risk is that of external events such as fire, floods, power failure etc. This is covered in one of the statements. The other issue that was mentioned by the interviewees is the interdependency amongst firms. Suppliers or third parties could be a serious risk

to ones organizations, due to their insufficient security. This is covered in the second statement. (see table 11 for an overview of the statements)

Nr	Category framework	Statement
	Cyber risk identification	
9	Human threats	Social engineering is becoming increasingly advanced and is one of our biggest concerns, and therefore requires awareness at all levels within the organization.
10		Careless or unaware employees are the weakest link in the security system. Cyber security awareness training can be a part of the solution.
11	System and technology failure	I think that an unpatched system is operating with a weak spot just waiting to be exploited by hackers.
12		Applying patches takes too much time and resources
13	Failed internal processes	The biggest problem is the awareness of the board. The top management is underestimating the cyber risks and not willing to invest
14		Cyber risk management should be part of the whole risk management
15		I have lack of confidence in the company's level of security
16	External events	Risk management is challenging because of interdependencies among firms. Therefore suppliers and third parties may be a serious risk to our cyber security due to their bad security
17		Unavailable systems due to physical external causes such as fire, floods etc. is a serious danger. We must have a high uptime.

Table 11 - statements about cyber risk identification

Cyber risk assessment

The main opinion that emerged is that risk assessments are made without sufficient information about risks. This means that decisions to invest are made on the basis of incomplete information. Therefore the statements need to cover the impossibility of complete information (See table 12). In the category part of risk the interviewees mentioned that it is often not clear how much one should invest in security and they indicated that is very difficult to estimate the risk one is facing. In the second category some interviewees mentioned that they only takes risks into account with a high likelihood or with major consequences, this is covered in one statement. And the second statements covers the main opinion about incomplete information. The third category is the focus on acceptable risk level, what the interviewees mentioned is that acceptable risk levels should be set by the management. The main opinion the interviewees had in the category measures to take, is that a basic security level is not very difficult to obtain. Some technical basics such as a firewall, back-ups and awareness throughout the whole organizations could be enough to avoid most of the cyber-attacks. This is covered in both the statements. See table 7 for an overview of the statements.

Nr.	Category framework	Statement
	Cyber risk assessment	
18	Part of risk	We invest in technologies like firewalls, intrusion detection, encryption etc. Although these technologies may reduce security vulnerabilities and losses from security breaches, it is not clear how much we must invest in IT Security
19		Some security risks we simply do not know or cannot imagine therefore we cannot be 100% safe
20		With the best protection and security measures in place we are nearly 100% safe

21	Focus on likelihood and consequences	We only take risks with high likelihood and major consequences into account
22		Cyber risk assessments are typically made without information about the probabilities of the outcomes, the consequences and the likelihood of occurrence
23	Focus on acceptable risk level	The existence of a vulnerability does not always mean it must be remediated. The organization may choose to accept the risk
24		Acceptable risk levels should be set by management and based on the business's legal and regulatory compliance responsibilities
25	Focus on measures to take	Complete prevention of security breaches is technologically impossible and, in some cases even undesirable because of high costs.
26		It is not complicated to prevent the impact of ransomware such as wannacry, some technical basics such as back-up and awareness of your employees should be enough to avoid impact.

Table 12 - statements about cyber risk assessment

Treatment strategy

In the statements about risk treatment strategies (table 13), complete risk avoidance is perceived as impossible but some interviewees mentioned that risk should be avoided as much as possible. In the category risk mitigation all interviewees mentioned that they try to reduce cyber risks by means of mitigation measures, but these measures alone are insufficient. Risk transference is directly linked to cyber insurance. The content of insurance is however, not always clear. Some may find insurance useless, or not interesting because it is economically not profitable or difficult to quantify. Risk could be party avoidable and could be perceived as better than recovering from incidents. Therefore the statement covers the idea that organizations should avoid risks as much as possible. The statements in the category risk acceptance distinguish several views. It is often said that 100% protection is not possible and responding to an incident is more important. However, accepting risks is not always possible due to regulation. See table 13 for an overview of the statements.

Nr.	Category framework	Statement
	Treatment strategy	
27	Risk mitigation	One does not have to take measures for risk that are not probable to the company
28		Only taking mitigation measures is enough to cope with cyber risk
29	Risk transfer	Insuring is always an economic trade-off. The costs of cyber insurance must be lower than the possible impact.
30		Cyber insurance can function as a replacement for sound cyber-security and cyber resilience practices
31	Risk avoiding	An organization has to avoid risk as much as possible, for example do not store personal data that is not necessary to store
32	Risk acceptance	Our organisation is not an interesting target for cyber criminals, so we have nothing to worry about
33		Incident response and resilience is more important than trying to prevent attacks from happening
34		Accepting all risk is not possible due to regulation. For example it might be legally required to protect certain data.

Table 13 - statements about treatment strategy

External factors

In the category breach or incident response there is one main opinion that stands out. One common idea is that many organizations only invest in security after a breach or incident has occurred and that

this is often too late. However while speaking with the interviewees, they indicated that this is not the case for them. But they did acknowledge the fact that this happens to many other organisations. The first statement covers this main opinion. Another opinion is that most interviewed are actually happy with an incident as long as it does not have too much impact, because it creates awareness.

In the category budget only a few interviewees mentioned that they determine their budget for cybersecurity through an extensive cost-benefit analysis or extensive risk analysis. Many of the interviewees were concerned they did not have enough budget available. The two statements cover these opinions. A cyber-attack can cause a lot of negative publicity due to media attention nowadays and potentially damage a company's reputation and eventually cause financial impact. The respondents mentioned that the harm done to a company's reputation can be long lasting and have serious loss of business due to the loss of trust amongst clients, suppliers and partners. These opinions are covered in the statements. There is no single rule that deals with cyber security, instead there are multiple rules and regulations that have been developed. Therefore more than two statements covers this category. One of the main opinions is that many respondents question the efficiency of the complex mixture of rules and regulation. Much has been said about the GDPR, however the respondents wonder whether this regulation will be effective or not. These topics are covered in the statements. One driver to be cyber secure could be client requirements. A potential client who is cyber secure does not want to take risk with an organizations that is not. Therefore, the respondents mentioned it could happen that a certain client requires a certain security. For example a client might require an ISO certification. This is covered in the second statement. Some respondents mentioned that they believe that attackers will choose the least secure company. As a result if their security is better than their competitor they believe, attackers will choose the other. This is covered in the other statement. See table 9 for an overview of the statements.

Nr.	Category framework	Statement
	External factors	
35	Breach or incident response	We didn't have a breach this year, so we don't need to ramp up investment. And if nothing happened this means that our security is good.
36		A breach or incident could have positive effects too, such as more awareness, as long as the impact is not too big.
37	Budget	I am concerned that we do not have enough budget, the right team with the right knowledge and the latest technology available
38		We perform a comprehensive cost-benefit analysis, because an investment in security must result in a benefits
39	Reputation	Our reputation is our largest asset. It takes 20 years to build a reputation and five minutes to ruin it. Therefore reputational damage is a disaster to our organization.
40		A cyber-attack can seriously damage our company's reputation.
41	Rules and regulation	We do not work with personal data so we do not have to invest in cybersecurity measures
42		Many spend a lot of effort on complying with regulations and this detracts from efforts to develop effective security capabilities. For example a security professional is now putting effort in assuring that the door to his data centre is of a certain thickness, rather than working on more effective security measures
43		Because of the GDPR we are going to invest in the minimum measures required which we would not do otherwise.

44		Organizations are forced to be aware and invest because the fines they may face from the GDPR
45		ISO 27001 is an outdated standard. Nowadays it is not just about the technical approach to cyber security
46	Client requirement	As long as my cybersecurity is at least the same or better than my competitors, attackers will choose a party with less security and I will be safe
47		Our business relationship demand our organization to have certain hardware, software, policies or procedures. Our client requirements are therefore a strong incentive to invest in our cybersecurity

Table 14 - statements about external factors

Appendix F – Q-method: 186 statements

Topic	Statement
Context establishment	
Assets	If my assets are tangible it is easier to invest in cybersecurity
	If an organization has its basics all organized it decreases the changes to get attacked Wie begint de basis op orde te brengen, maakt de kansen kleiner om niet getroffen te worden
	Determining your core assets and the type of protection it needs is the most important step in cyber risk management
	Without assets there is nothing to harm
	It is very difficult to determine the cyber risks due to the fact that threats continue to evolve and threat landscapes are constantly changing berg et al
	loss of personal information is less tangible than for example, the loss of 2 million US dollar, therefore tangible assets get more priority in security get
	all organizations should base their cybersecurity on their assets and not on something else
	It is better to distinguish between systems that need high protection and systems that need less protection to save money. Otherwise it may happen that data that does not require protection will be protected.
	Depending on the risks you need to invest. For example for one system the availability is most important but for another systems this is less important. Then those systems do not need the same security.
	any risk analysis must take into account legal obligations and regulatory requirements, as well as business drivers and objectives
	Our most important assets is our reputation
Confidentiality	Confidentiality of our information is as important as the availability of our systems
	Confidentiality is roughly equivalent to privacy.
	maintaining confidentiality is necessary to comply with ethical and legal regulations
	Every organization has a need to keep certain information confidential
	An employee or hacker who leaks vital information to a competitor is our biggest concern
	Failure to properly secure and protect confidential information can lead to the loss of business and clients and is our biggest concern
	Unauthorized access to a business' data is a serious threat
Integrity	Integrity is more important than the availability of the systems. For example we want to keep some information secret and that has priority number one.
	Many companies suffer from overdue maintenance. In recent years they have built new systems in which data is stored but no longer know where data is stored and whether they comply with the rules.
	Charging and misusing sensitive information is the biggest danger to our organization
	Back-up data is very important with respect to data integrity
	data integrity should be top of your mind at every stage of the data lifecycle, and already from the design and implementation phase of your systems
	Half the battle is won when your company’s leadership stresses the importance of company data and its integrity.
Availability	A day without operating systems can cause major financial damage to our organisation
	The most important thing is to keep current with all necessary system upgrades
	Fast and adaptive disaster recovery is essential for the worst case scenarios
	To prevent data loss from external occurrences, a backup copy may be stored in a geographically-isolated location, perhaps even in a fireproof, waterproof safe
	Duplicate data sets and disaster recovery plans are too costly
	Having basic backup, data-replication, and failover procedures in place is perhaps the most basic approach to server availability.
	System availability is very important. If the availability is at stake, people will invest faster.

	Backing up your data frequently and having a disaster recovery plan could help should a worse attack happen such as wannacry
	A denial of service (DoS) attack is one of our biggest concerns.
Cyber risk identification	
Human threats	Humans are the weakest link in the system
	Everyone can be a victim to cyber attacks
	Phishing is one of the biggest problems we have in our organization
	Employees are not aware of cyber risk
	The most likely source of an attack are careless employees
	Employees with bad intentions are a major treat to the cyber security of the organisation
	Social engineering is becoming increasingly advanced and therefore requires awareness at all levels within the organization.
	Social engineering is our biggest threat
	Humans are the weakest link in the security system. Cyber security awareness training can be a part of the solution.
System and technology failure threats	Outdated software is a great risk for our organization
	Unavailability of our systems due to a technical failure or cyber-attack would be a major problem and has huge consequences
	The awareness of managers about their cybersecurity has increased but not enough yet
	ISO 27001 is an outdated standard. Nowadays it is not just about the technical approach to cyber security.
	The network must be tested regularly for leaks and unevenness
	An unpatched system is, by definition, operating with a weak spot just waiting to be exploited by hackers.
	Applying patches takes too much time and resources. However it is very important.
Failed internal processes	Top management underestimates the cyber risks
	Cybersecurity is seen as an IT problem only, but need to be addressed throughout the whole organisation
	Cyber risk management should be part of the whole risk management
	I have lack of confidence in the company's level of security
	Top management differs from IT management in the field of cybersecurity which is not good
	Employees are insufficiently committed to cyber security measures and procedures
	Cyber security must be treated as any other risk
	The biggest problem is the awareness of the board. Management is still aware of the risks and not willing to invest
	In our organization there are managers who say that cybersecurity is not that important.
	Making the management aware of the risk is sometimes very difficult. This is due to the fact that these managers mainly worry about profit
	The failures that breaches characterize are a direct result of people, policies and process that are not aligned with a security-minded IT team.
	Cyber security is regarded as a board-level responsibility
External events	External events are a great risk for our organization
	Suppliers and other third parties can form a serious risk to our cyber security due to their bad cyber security
	Software from third parties may cause a cyber-risk because you can hardly check for any leakage
	Unavailable systems due to physical external cause is a serious danger, we must have a high uptime.
	Risk management is challenging because of interdependencies among firms. So security risk faced by one organization does not only depend on its own security and actions, but also on those of others
	Safeguards against data loss or interruptions in connections must include unpredictable events such as natural disasters and fire
Cyber risk assessment	
Part of risks	Some security risks we simply do not know or cannot imagine therefore we cannot be 100% safe
	Some risks are more important than other risk and are therefore get more attention

	Even with the best protection and security measures in place an organization will not be 100% secure.
	We do not make a comprehensive cyber risk assessment
	Risk management is more difficult in practice than in theory
	The standard cost-benefit analysis is almost impossible to perform
	Protection of personal data is not the only thing that matters, there is much more than that.
	Today almost every company is an IT company, which means that every company should have the cybersecurity as good as an IT company.
	Firms invest in technologies like firewalls, intrusion detection, encryption etc. Although these technologies may reduce security vulnerabilities and losses from security breaches, it is not clear to firm how much they must invest in IT Security
	Many organizations only focus on personal data, but focus is needed throughout the whole organizations' cyber security.
Focus on likelihood and consequences	If the social impact of an attack is very large cybersecurity gets a high priority
	Estimating the likelihood of occurrence is very difficult because most of the times human intent and motives are involved
	We only take risks into account with high likelihood and major consequences
	Cyber risk assessments are typically made without information about the probabilities of the outcomes, the consequences and the likelihood of occurrence
	As the impact of an attack grows, more investments will be made. Or at least cybersecurity will be at a higher priority.
	What would help if a large penalty would occur, probably then there will be more action
	Organizations are forced to be aware and invest because of the fines they may face from the GDPR
	It is important to focus on the basics: people and technology
Focus on acceptable risk level	No organization is ever completely without risk, but there are steps that can be taken to establish an acceptable level of risk that can be appropriately mitigated.
	Acceptable risk levels should be set by management and based on the business's legal and regulatory compliance responsibilities, its threat profile and its business drivers.
	Information security professionals need to serve as the intermediary between the threats and management, explaining how underlining security threats could affect business objectives so they can get the balance of security and the acceptable level of risk right.
	Ultimately the goal is for this "residual risk" to be below the organization's acceptable level of risk
	All identified risks should be evaluated to determine if they are acceptable or unacceptable
	The management should decide if it should control or mitigate the identified risks or accept the risk
	The existence of a vulnerability does not always mean it must be remediated. The organization may choose to accept the risk
Focus on measures to take	Prevention is better than cure Preventive action is better than reaction
	Better to be safe than sorry
	To eliminate threats throughout the organization, security must reach beyond the IT department
	Cybersecurity must be treated as any other risk
	Complete prevention of security breaches is technologically impossible and, in some cases even undesirable because of high costs.
	Investing in both measures and insurance to manage risks is enough
	It is not complicated to prevent the impact of wannacry, some technical basics and awareness of your employees would have been enough to avoid to avoid impact.
	Some measures just cost too much money and the efficiency is not clear
	Proper investment is difficult.
	No countermeasure can completely eliminate risk, There will always be some risk
	Preparation is key when it comes to what you can do to protect that reputation.
Treatment strategy	
Risk mitigation	Cybersecurity efforts have to focus on risk management, not risk mitigation.
	We took all measures possible to deal with the cyber risks and the residual risk need to be accepted

	One does not have to take measures for risk that are not probable to the company
	Only taking mitigation measures is not enough to cope with cyber risk
	You must properly document all of the data you store and have sufficient security.
	Every organization should imply cyber security measures to reduce risk
	It is not enough to take only preventive measures against cyber attacks
	Cyber security should be part of the primary business process
	Awareness of senior management ensures better cyber security
	Many organizations do not have their primary processes in order. In IT, primary process are the most important. This means that back-up and recovery is the most important process
Risk transfer	a cyber-security insurance to reduce the risk of financial losses is a perfect idea
	Insurance is useless, after an attack it is already too late and the damage has been done.
	Insurance is only an option if you do not have the necessary expertise and it is cost effective
	Insurance is only useful it if is economic beneficial
	Good risk management includes cyber insurance
	Insuring is always an economic trade-off. The costs of insurance must be lower than the possible impact.
	It is not clear what a cybersecurity insurance entails and what an insurance can provide
	Cyber insurance is no replacement for sound cyber-security and cyber resilience practices
Risk avoiding	Avoiding cyber risks is not possible, there will always be a residual risk
	An organization has to avoid risk as much as possible, for example do not save personal data that is not necessary to save
	Completely avoiding all cyber-related risks is not possible for an organization.
	Information risk must be elevated to a board-level issue and given the same attention afforded to other risk management practices.
Risk acceptance	Our organisation is not an interesting target for cyber criminals
	Incident response and resilience is more important than trying to prevent attacks from happening
	Accepting all risk is not possible due to regulation
	We have taken enough measures, the residual risk is negligible
	An organization does not have to protect itself from cyber risks that an organization thinks does not face.
	There is a possibility that cyber risks can be accepted if the cost of security exceeds the potential impact of the risk. It is always a well-considered decision.
	A risk cannot be accepted if it causes reputation damage
	Accepting cyber risks is not possible if it is legally required to protect certain data
	It has been good for years now, so we have nothing to worry about
External factors	
Breach or incident response	We started investing in cyber security after a breach has happened
	We didn't have a breach this year, so we don't need to ramp up investment
	Nothing will happen to us, therefore cybersecurity does not have priority
	If nothing happened this means that our security is good
	After a breach we (will) spend whatever it takes to solve the problem.
	many organizations only invest in their cybersecurity after a breach has happened
	Everything is okay, so why would I invest?
	A breach or incident could have positive effects too, such as more awareness, as long as the impact is not too big.
Budget	More investment means more security
	Because of our restricted budget we are not able to implement a certain amount security measures
	At least 10 percent of the IT budget should be spent on cyber security
	I am concerned about lack of sufficient funding needed to defend the systems
	I am concerned that we do not have enough budget, the right team with the right knowledge and the latest technology available

	We perform a comprehensive cost-benefit analysis and determine how much to invest in our security
	Investment in security must result in profits because of increased profits or reduced costs
	Money is the key driver why organizations invest in their cyber security.
	If an organizations does nothing, then more investment is useful. But if an organizations has its basic security then it is more about the effectiveness of the measures instead of more investment.
	If you cannot prove that the benefits exceed the costs, you cannot motive the top management to invest in cybersecurity
	Money is not the objective, but smart investments is.
Reputation	Reputational damage is a disaster to our organization
	The consequences of cyber-attacks can go beyond organizations' material damage such as reputational damage
	Due to media attention people are more aware of cyber risks and are going to do something about the security
	Most cybercrime incidents go unreported, and few companies come forward with information on their losses. That is not surprising given the risk to an organization's reputation and the prospect of legal action against those that own up to cyber crime
	The harm done to brand reputation can be long lasting and hard to control
	It takes 20 years to build a reputation and five minutes to ruin it
	Trust is hard to gain but easy to loose
	A cyber-attack can seriously damage our companies' reputation and most success due to human error.
	Our strong reputation is our largest asset, but just one crisis could irreversible damage our image and ruin our business
	Cyber resilience is important to maintain our reputation
Rules and regulation	A lot of companies have no idea what data they are saving
	You must keep track of what you are doing with your data at all times
	Because of the GDPR we are going to invest in the minimum number of measures required
	We do not work with personal data so we do not have to invest in cybersecurity measures
	Data protection and privacy laws are accelerating spending on IT security solutions
	Many spend a lot of effort on complying with regulations and this detracts from efforts to develop effective security capabilities. For example a security professional is now putting effort in assuring that the door to his data centre is of a certain thickness, rather than working on more effective security measures
	legislations give positive incentives to organizations to invest in cybersecurity, which they would not do otherwise
	Legislation in data privacy lags behind
	many organizations only invest in their cybersecurity because of regulation and are not willing to do extra security
	One of the key drivers is privacy legislation that compels companies which are handling personal data to implement a certain level of security. And especially the fines they can face are the key driver.
	Legislation for data privacy is not enough, there is more than personal data to protect.
	The most important thing with the GDPR is the supervision
Client requirements	Our client requirements are a strong incentive to invest in our cybersecurity
	Our business relationship demand our organization to have certain hardware, software, policies or procedures
	We do the same kind investment as our competitors. Because if we are at least at the same level attackers will choose a party with less security
	I think we have investments in security measures which might not be efficient at all.
	We have installed firewalls because firewalls are a great success in the market. However firewalls are not the most effective measure at all. There are multiple more measures that are much more effective.
	As long as my cybersecurity is better than my competitors I will be safe
	Risk management is challenging because of interdependencies among firms. So security risk faced by one organization does not only depend on its own security and actions, but also on those of others
	So apart from all business risks we have a big social responsibility. If something goes wrong with one of our main clients the consequences can be very big. So the main driver to us is this social responsibility and the social impact cyber incidents could have.

Appendix G – Q-method: Correlation matrix

Correlations

	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18
R1	1,00	0,19	0,25	,361*	,421**	,396*	0,22	,368*	,427**	,615**	,427**	0,28	0,07	,541**	,411**	0,21	,340*	-0,07
R2	0,19	1,00	,294*	,312*	0,27	0,15	0,20	0,27	0,23	0,21	0,07	0,18	0,06	0,20	0,02	,309*	0,21	0,04
R3	0,25	,294*	1,00	,422**	,567**	0,28	,493**	,511**	,404**	,407**	,456**	,435**	0,22	,313*	0,27	0,29	,669**	0,03
R4	,361*	,312*	,422**	1,00	,322*	,328*	0,29	0,27	,359*	0,26	,300*	,468**	0,03	,518**	,378**	,334*	,378**	-0,11
R5	,421**	0,27	,567**	,322*	1,00	,463**	0,22	,463**	,563**	,532**	,397**	,350*	-0,07	0,28	0,24	,554**	,645**	-0,06
R6	,396**	0,15	0,28	,328*	,463**	1,00	,309*	,322*	0,23	,619**	0,24	,416**	-0,04	,297*	,444**	0,12	,528**	-0,10
R7	0,22	0,20	,493**	0,29	0,22	,309*	1,00	0,08	,400**	,399**	,294*	0,28	0,16	,331*	,450**	-0,12	,447**	-0,17
R8	,368*	0,27	,511**	0,27	,463**	,322*	0,08	1,00	,431**	,518**	,363*	0,28	0,09	,291*	0,22	,338*	,594**	0,09
R9	,427**	0,23	,404**	,359*	,563**	0,23	,400**	,431**	1,00	,490**	,378**	0,25	0,08	,578**	,413**	,444**	,541**	-0,10
R10	,615**	0,21	,407**	0,26	,532**	,619**	,399**	,518**	,490**	1,00	,327*	,298*	-0,08	,449**	,477**	0,20	,603**	-0,03
R11	,427**	0,07	,456**	,300*	,397**	0,24	,294*	,363*	,378**	,327*	1,00	0,04	0,10	,325*	0,21	0,15	,409**	0,13
R12	0,28	0,18	,435**	,468**	,350*	,416**	0,28	0,28	0,25	,298*	0,04	1,00	0,05	,294*	,438**	0,24	,322*	-0,15
R13	0,07	0,06	0,22	0,03	-0,07	-0,04	0,16	0,09	0,08	-0,08	0,10	0,05	1,00	0,09	0,13	-0,04	0,09	0,06
R14	,541**	0,20	,313*	,518**	0,28	,297*	,331*	,291*	,578**	,449**	,325*	,294*	0,09	1,00	,606**	0,28	,369*	-,300*
R15	,411**	0,02	0,27	,378**	0,24	,444**	,450**	0,22	,413**	,477**	0,21	,438**	0,13	,606**	1,00	0,15	,325*	-,441**
R16	0,21	,309*	0,29	,334*	,554**	0,12	-0,12	,338*	,444**	0,20	0,15	0,24	-0,04	0,28	0,15	1,00	0,29	-0,06
R17	,340*	0,21	,669**	,378**	,645**	,528**	,447**	,594**	,541**	,603**	,409**	,322*	0,09	,369*	,325*	0,29	1,00	-0,10
R18	-0,07	0,04	0,03	-0,11	-0,06	-0,10	-0,17	0,09	-0,10	-0,03	0,13	-0,15	0,06	-,300*	-,441**	-0,06	-0,10	1,00

Appendix H – Q-method: Relation factor loading and organizational factors

Relation between size company and factor loading

Crosstab							
			Factor loads				Total
			factor1	factor2	factor3	factor4	
Size	klein	Count	5	3	2	2	12
		% within size	41,7%	25,0%	16,7%	16,7%	100,0%
	groot	Count	2	1	1	0	4
		% within size	50,0%	25,0%	25,0%	0,0%	100,0%
Total		Count	7	4	3	2	16
		% within size	43,8%	25,0%	18,8%	12,5%	100,0%

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	,825[a]	3	0,843
Likelihood Ratio	1,301	3	0,729
Linear-by-Linear Association	0,278	1	0,598
N of Valid Cases	16		
a. 7 cells (87,5%) have expected count less than 5. The minimum expected count is ,50.			

Relation between sector company and factor loading

Crosstab							
			Factor loads				Total
			factor1	factor2	factor3	factor4	
sector	publiek	Count	3	1	1	0	5
		% within sector	60,0%	20,0%	20,0%	0,0%	100,0%
	privaat	Count	4	3	2	2	11
		% within sector	36,4%	27,3%	18,2%	18,2%	100,0%

Total	Count	7	4	3	2	16
	% within sector	43,8%	25,0%	18,8%	12,5%	100,0%

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1,427[a]	3	0,699
Likelihood Ratio	1,996	3	0,573
Linear-by-Linear Association	0,970	1	0,325
N of Valid Cases	16		
a. 8 cells (100,0%) have expected count less than 5. The minimum expected count is ,63.			