What drives cyber security investment? Organizational factors and perspectives from decision-makers

Jennie de Vries

System engineering, Policy Analysis and Management, Technical University Delft, Delft

What drives cybersecurity investment? Organizational factors and perspectives from decision-makers

One of the leading perspectives from literature is that decisions about investments should be made based on a comprehensive cost-benefit analysis and on a cyber-risk assessment. However, many organizations do not undertake this sophisticated analyses due to the lack of available data about costs, benefits and the impact and likelihood of attacks. This study tries to increase the understanding of this decision-making process, and how organizational factors and individual perspectives influence this process. The Global Information Security Survey has been subjected to a latent class analysis to find investment strategies and organizational factors that influence these. Four different investment strategies were identified and mainly differ in their initial investment and change in the coming twelve months. Organizational factors that influence these investment strategies are size, revenue, type (public/private) and budget and other factors as regulation, management awareness, incidents and type of risks. We used the q-method to investigate underlying perspectives from decision-makers. Four different perspective were found and differ in their focus on concerns, resilience, hierarchy and flexibility.

Keywords: cybersecurity; investment; decision-making; perspectives; risk-management

Introduction

In April 2011, one of the biggest data breaches in corporate history 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 (Shackelford, 2012). 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.

With the 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. The awareness of managers in organizations that could be affected by cyber-attacks 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, and in response organizations are improving their defences from very basic level in the '70 to more sophisticated, robust and formal processes nowadays (EY, 2016).

However, in practices it seems very difficult to determine the continuously evolving cyber risks and to determine to what criminals we must protect ourselves from (Berg et al., 2014). 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).

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.

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 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:

(1) What drives cybersecurity investment?

(1.1) What cybersecurity investment strategies exist in practice?

(1.2) What organizational factors influence these cybersecurity investment strategies?

(1.4) What are individual perspectives from decision-makers on cybersecurity investment strategies?

(1.3) Can these investment strategies be explained from the perspectives of decision-makers?

The structure of this article is as follows: first the research methods will be explained to answer the research questions. Thereafter information about decision-making process of cyber investment

strategies is discussed. Then the results of the analyses will be explained. Finally, it will provide a conclusion, discussion, recommendation and critical remarks.

Research methods

Latent class analysis

The first sub question: "What cybersecurity investment strategies exist in practice?" and the second sub question: "What organizational factors influence these investment strategies?" will be answered with the result of the Global Information Security Survey (GISS). 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. And this survey is used because it is one of the largest surveys conducted, since information about cybersecurity and investments is relative scarce.

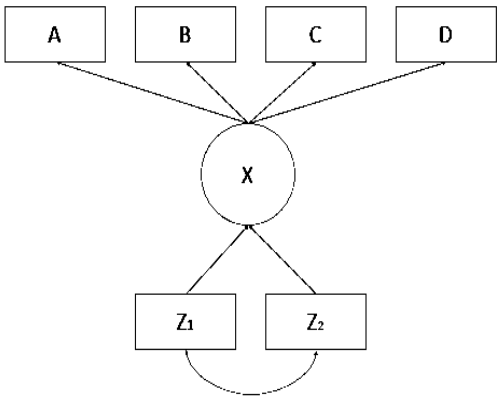

Figure 2. Latent class model

This dataset will be subjected to a cluster analysis. 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). The latent class analysis (LCA) will be used to identify clusters. This analysis has several advantages over traditional clustering techniques (Magidson & Vermunt, 2002): it uses probability-based classification, variables do not have to be standardized and variables can be of mixed scale types. In addition, LCA is not as sensitive to missing data as traditional analysis and LCA uses statistical tests to determine the number of clusters instead of determining the number of clusters upfront (Magidson & Vermunt, 2002).

Figure 2 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 LCA is used. The indicators are dependent variables that are used to define or measure the latent classes. An example indicator to find investment strategies 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. 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 indicators and covariates used in the final model are discussed in the result section: investment strategies.

Q-methodology

The third sub question: "How 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. 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 decision-makers on cybersecurity investments. 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). 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). A detailed description of the steps is discussed in the result section: perspectives from decision-makers.

Decision-making process cybersecurity investments

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, so 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, P.w, 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).

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.

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, Solhaug, & Stolen, 2015). Figure 5 is based on this NEN standard. This seems a very transparent and objective process, however the decision making regarding cybersecurity are based on subjective decisions. In addition, within this 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? As can been seen in figure 5, the cyber risk management process is complex. During cyber-risk management and assessment multiple decisions are made. 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.

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 (Fielder et al., 2016) and can only cover vulnerabilities, or organizations that only invests in their cybersecurity to comply with rules and regulations (Kovacs, 2014), or organizations only fear reputational damage (Almann & Kelly, 2008). Or organizations need to comply with client requirements (Michael P. et al. 2006), or do the same kind of investments

as their competitors (Almann & Kelly, 2008). And finally organizations could only invest after a breach or incident has happened.

This figure (1) shows how the decision-making process regarding cybersecurity could look like in practice and includes all aspect that could influence this investment strategy. This framework will be used to select variables from the GISS dataset to include in the analysis. And to create an equal number of statements per aspects which forces to select statements from one another and makes the q-set broadly representative.

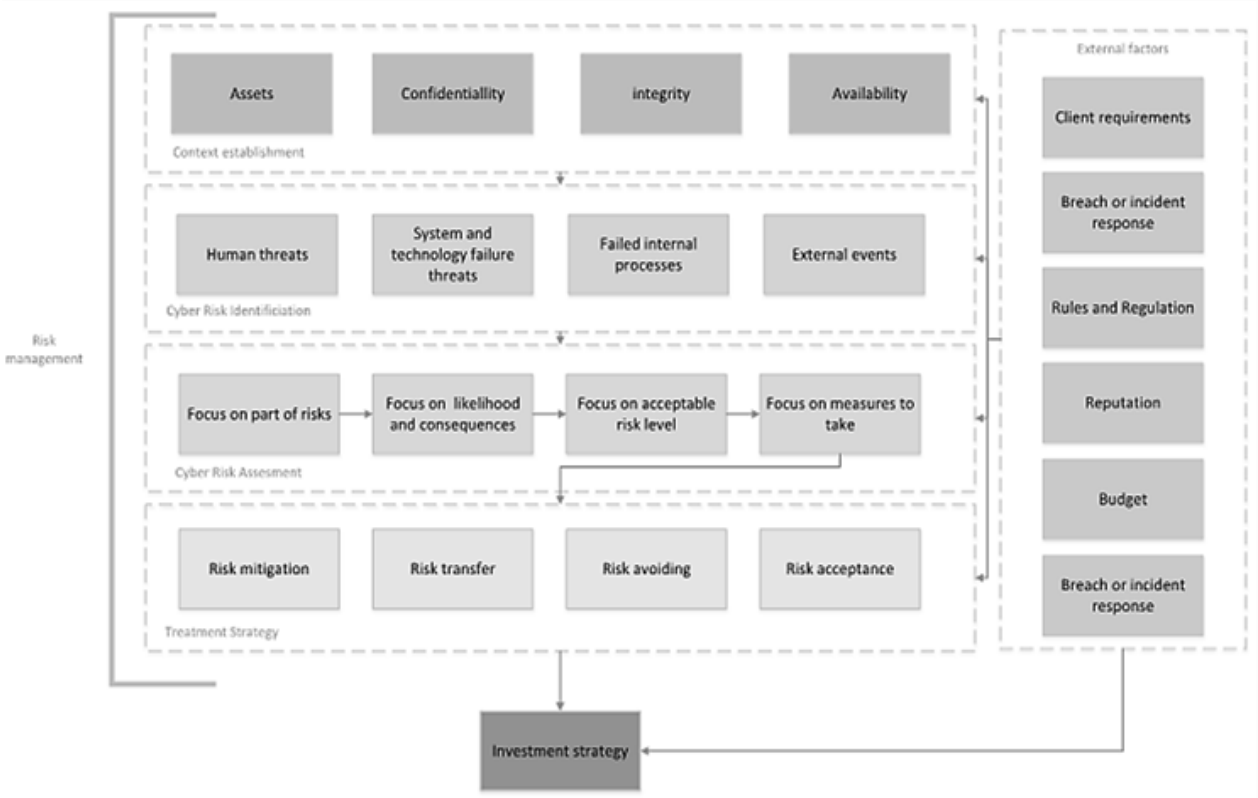

Figure 1 – Decision-making process cybersecurity investments

Investment strategies

To be able to assess whether organizations have different investment behaviour the latent class analysis is used. This section is to explain the methodology in more detail, the included indicators and covariates, and to describe the final model and the results.

The LCA model consist of indicators, latent classes and covariates. Based on the risk management process five different categories that could have a significant influence on the investment behaviour can be included in the model. These categories 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 data and thus variables in the GISS dataset the following categories, besides organizational characteristics, are included: cyber risk identification and external factors. The other dimensions are not covered in the GISS dataset. 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.

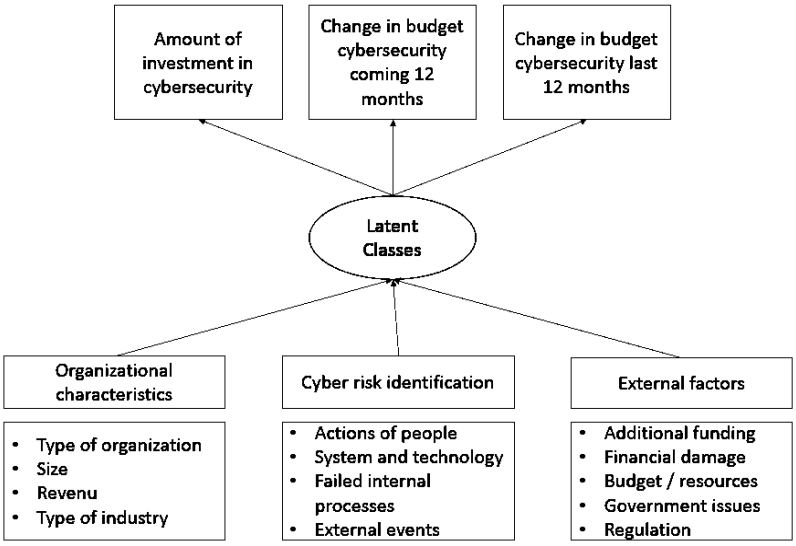

Figure 1 - latent class model

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 is first estimated without any covariates, see table 3 in the appendix for the outcomes of this estimation. Several methods exist to determine which models fits best. The first 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. Generally when the p-value is smaller than 0.05 the model provides an adequate fit and is most parsimonious. Using this criteria the best model is given by model 4, the 4-cluster model with a p-value of 0.01.

So, the latent class analysis is performed with four models. To test the significance of the indicators and the active covariates the Wald test is used. 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 in the appendix, with a confidence level of 93 percent, there rae 11 out of 15 covariates that significant affect cluster membership. These are: the threat of actions of people, the threat of failed internal processes, lack of resources, budget constraints, lack of executive awareness or support, fragmentation compliance or regulation, total revenue, type of

organization, additional funding needed for cybersecurity and the total financial damage past year due to cyber incidents.

So the outcome of the latent class analysis shows that there are four classes different from each other and are well interpretable. Table 1 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 2 in appendix. The four classes are discussed below including some distinguishable characteristics of the respondents per class.

Group I - Small investments 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 constrains was one of the main obstacles of reasons that challenge the information security contribution and value to the organization. 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 almost 40 percent has small to no financial damage due to a cyber-attack. This could indicate that if damages to an organisation are small to none, they are not driven to increase their budget.

Group II – 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 explain why this group will increase their spending. What is interesting is that this group contains of for almost 80 percent public organizations. It can be concluded that public organizations are more driven by rules and regulations than private organizations.

Group III – 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.

Group IV – Large investment and no 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.

This table shows the outcome of the latent class analysis and shows the different four classes and the percentages of respondents belonging to that cluster per indicator. Table 5, which includes the covariates, is shown in the appendix.

Table 1 - 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**

Individual perspectives

The next step of this study is to identify individual perspectives of decision-makers and how these might influence or explain the investment strategies found in the abovementioned analysis. To be able to capture individual perspectives of decision-makers the q-method is performed. The q-method consist of six steps, namely: the concourse, the selection of the q-sample, the selection of the p-set, the q-sort and the correlation and factor analysis.

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 six interviews, literature research and from news blogs or fora. The statements represent the best possible extent of perspectives regarding cybersecurity investments. The framework which is presented above in the cyber risk management section is used to structure the topic of decision-making in cybersecurity investments. Each of the categories that has been covered by the framework, is to be covered by the statements. Per category approximately ten statements are included, which resulted in 185 statement in total. 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.

Selection of the 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 presented in the section: Cyber risk management, 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 6 in de the appendix.

Selection of the p-set and the q-sort

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. 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. The private sector has a lot of 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. Therefore it is expected that this influence the perspectives.

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. The function of the respondents 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. 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 4. 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 typically is. Other distributions would lead to the same outcomes (Exel & Graaf, 2005).

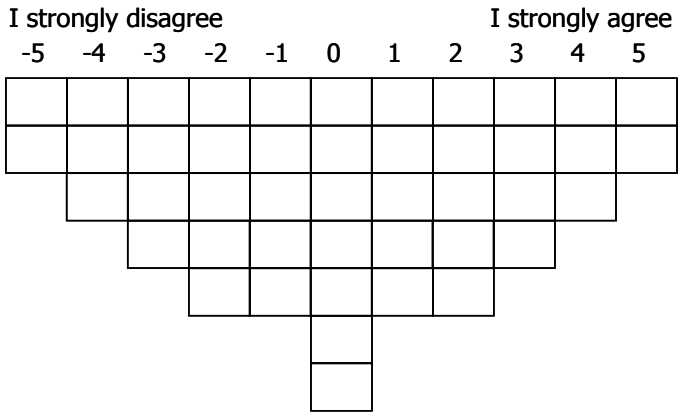

Figure 2 - forced distribution to sort statements

Correlation and factor analysis

As mentioned above, 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 study 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.

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. To maximize the amount of respondents on a factor different factor loadings were used. When the factor loading is set at 0.45 the amount of respondents is maximized. So therefore this factor loading is used, with a significance of 0.05, see table 5 in the appendix.

Interpretation of the results: perspectives from decision-makers

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 (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. See the table 2 for the statements with the biggest differences and table 6in the appendix for the factor scores for all statements.

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 and it is characterised by its concern about unknown risks and social engineering. The second perspective is characterised by its focus on risk avoidance, incident response and resilience. In the third group there is a hierarchical perspective and it 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.

The question that remains is if certain decision behaviour or biases as described in literature can be seen in the perspectives from practice. As mentioned, people rather choose something with a certain outcome, then something with a higher utility but with uncertain outcomes. This behaviour might be visible in the first perspective, since it is focused on concerns. And might be visible in the third perspective, because it is focussed on the unawareness of the employees. This can be seen as something which is tangible and therefore some sort of certainty. People are also tempted to overweigh the probability of uncertain events. This behaviour might be visible in the second perspective since they are focussed on resilience and incident response. This could indicate that they overweigh certain events and think that incidents will certainly happen and therefore focus on response instead of proactive actions.

Another question that remains is if and how an organization influences an infidel perspective. So can the investment strategies be explained from individual perspectives? 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.

Table 2 - Statements with the biggest differences between factors

	Statements with different factor loadings	I	II	III	IV
S30	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
S25	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.	1	2	-4	1
S9	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
S5	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
S4	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
S3	An employee or hacker who leaks vital information to a competitor is our biggest concern	-3	-3	5	0
S1	Organizations should base their cybersecurity on their assets and not on something else.	-1	-1	0	4
S2	It is very difficult to determine the cyber risks due to the fact that threats continue to evolve.	4	-1	-3	0
S45	Organizations are forced to be aware and invest because of the fines they may face from the GDPR	3	0	-5	-4
S46	ISO 27001 is an outdated standard. Nowadays it is not just about the technical approach to cyber security	0	-2	1	5
S38	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
S36	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
S21	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

Conclusion

Common in literature is that cybersecurity investments should be based on a comprehensive cost-benefit analysis or on a comprehensive risk assessment. 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. 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. 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.

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. One of the key drivers is the budget of an organization and the lack of resources. It is unclear if this is due to incomplete information, or lack of awareness. For large public organizations the key driver is the need to be compliant with rules and regulations and the high financial damage. This could indicate incident response as a driver. The financial damage is the largest in public organizations, however the question remains if this is really the case or are public organizations more obliged to report incidents? The size and revenue of an organization significantly influences the investment strategy, however 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. Within all cluster almost 40 percent identified indicate that the threat of actions of people is a major concern. This can be seen as an important driver. Interesting is that the type of industry does not significantly influences the cluster membership.

In addition four different perspectives from decision-makers are found. 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 and it is characterised by its concern about unknown risks and social engineering. The second perspective is characterised by its focus on risk avoidance, incident response and resilience. In the third group there is a hierarchical perspective and it 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.

Recommendation and future research

One cybersecurity investment strategy does not fit all. Organizations and individuals clearly 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 and to determine how these types of strategies influence the investment strategy.

In addition more research is necessary into the effect of organizations on individuals and therefore the effect on the perspectives. This is to answer the questions whether certain perspectives only consist in certain organizations based on organizational factors or not.

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. 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? 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 really the matter or do other, and especially private, organizations do not share this information? The government's role could be 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 regulation is important in the issue with information sharing and can support this issue. 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 regulation does not drive cybersecurity investments, the respondents see another role for the government, namely to better control on the compliance of regulation.

In addition there 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?

Discussion

The additional value of this study 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 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.

In literature most investment strategies are discussed as cost-benefit analyses and risk 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 organizations 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.

Rowe and Gallaher did a similar study and conducted interviews to determine 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 industry 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 builds 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?

Although meaningful results are found from the analyses, there are some limitations that need to be discussed. A large part of the respondents from the sample composition from the GISS are from the financial sector, however this factor did not significant influenced cluster membership. In addition some variables were not clear or not correctly categorized or some variables were missing that were discussed in the literature research. This means that the list of factors that could influence the investment strategy is not extensive. If these factors are included in a next study other

investment strategies could be found too. The effect of these factor stays unknown in this study. These factors are from the categories: the context establishment, the risk assessment, the risk treatment strategy. 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.

A few things are also notable in the perspectives derives with the q-method. First some respondents may have shown some socially acceptable behaviour and may have shown an "ideal" perspective, however this is not made explicit thus the impact of socially acceptable behaviour is unknown for this study. Secondly, as mentioned above, the number of respondents for this method was relatively low. Due to this low number, there is no significant relation found between the organizational factors and the perspective a respondent shares.

References

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

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.

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

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

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

Kahneman, D. (2011). *Thinking , Fast and Slow (Abstract)*. *Book*. https://doi.org/10.1007/s13398-014-0173-7.2

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

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
Meijeren, M. (2016). *Perspectives on cyber security*. Technical University Delft.
Michael P. Gallaher, Brent R. Rowe, Alex V. Rogozhin, A. N. L. (2006). Economic analysis of cyber security. *Air Force Research Laboratory*, (July), 110.
Neil, N. F. and M. (2012). The Need for Causal, Explanatory Models in Risk Assessment 2.1, 31–50.
Parsons, B. (2017). The home of cyber security best practice: public or private sector? Retrieved May 2, 2017, from http://www.securitynewsdesk.com/the-home-of-cyber-security-best-practice-public-or-private-sector/
Refsdal, A., Solhaug, B., & Stolen, K. (2015). *Cyber-Risk Management*. SpringerBriefs in computer science. https://doi.org/10.1007/978-3-319-23570-7
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.
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
Singer, P.w, Friedman, A. (2014). Cybersecurity and Cyberwar. *Igarss 2014*, (1), 1–5. https://doi.org/10.1007/s13398-014-0173-7.2
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

Table 3 - Model estimation latent class analysis

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

Table 4 - Wald test latent class analysis

	Indicators	**Wald**	**P-value**
	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

Table 5 - 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

Table 6 - Varimax analysis respondents included

	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		

Table 7 - statements for q-method

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 awareness of your employees should be enough to avoid impact.	1	2	-4	1
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