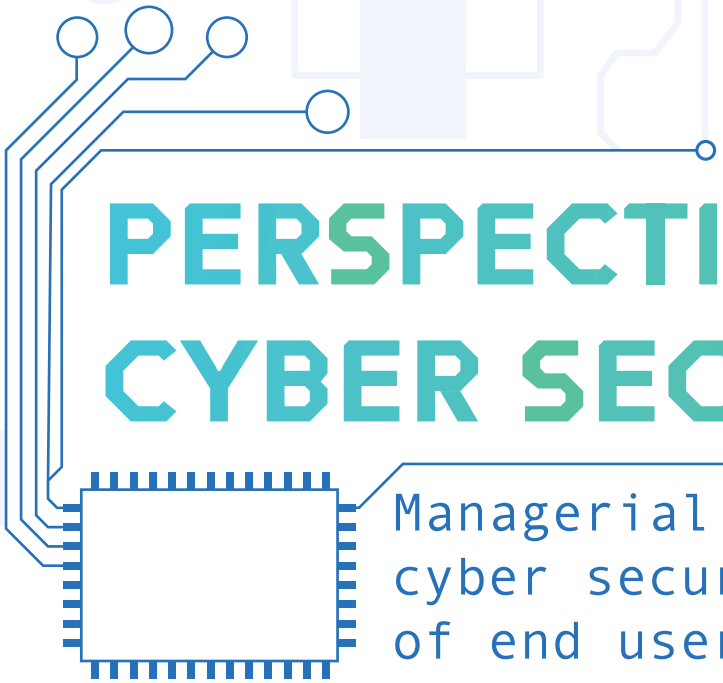


PERSPECTIVES ON CYBER SECURITY

Managerial perspectives on cyber security and the role of end user awareness

Maarten van Meijeren
March 2016
Master Thesis

TU Delft

Front image made by Fabian van Hoffen

https://www.faabdesign.nl/

Perspectives on Cyber Security

MANAGERIAL PERSPECTIVES ON CYBER SECURITY AND THE ROLE OF END USER AWARENESS

By

Maarten van Meijeren

In partial fulfilment of the requirements for the degree of
Master of Science in Management of Technology (MoT)
Delft University of Technology

Graduation Committee:

Chairman
Prof. Dr. M.J.G. van Eeten
Professor, Faculty of Technology, Policy and Management, TU Delft

First supervisor
Dr. Ir. M. Kroesen
Assistant professor, Faculty of Technology, Policy and Management, TU Delft

Second supervisor
Dr. Ir. W. Pieters
Assistant professor, Faculty of Technology, Policy and Management, TU Delft

TU Delft

Summary

With the development of the Internet, risks connected to being online started to emerge as well. These cyber risks, and specifically those in the domain of cyber security in an organisational context, are central to this thesis. Broadly, one can distinguish between four different sources of operational risks in the domain of organisational cyber security: actions of the users, system- and technology failures, failed internal processes, and external events.

Technical risks and measures are part of the established elements of cyber security; they are used as a first step in the cyber security approach. The discussion in cyber security mainly takes place in the human factor literature on the role of the human in cyber security. A dominant perspective in human factor literature focusses on human as the weakest link in the cyber security chain, mostly due to the inexperience and lack of expertise of the users. Following logically from this perspective, low expertise errors can be prevented by enhancing end user cyber security awareness, thereby reducing the cybersecurity risks.

Hence, the main perspective in literature focusses solely on humans as weakest link and only recognizes increasing awareness as a possible solution. However, it seems to be rather one-sided to believe there is only one crucial risk and one approach for such a broad problem as cyber security; in the end, there is an array of risks and mitigation means connected to cyber security other than just the awareness of users.

Such a one-sided perspective raises several questions. First of all, are there, next to the perspective mentioned above, other perspectives regarding cyber risk and cyber security in literature? Additionally, is the dominant perspective in literature also dominant in organisational practice? In other words, do responsible actors in an organization think that end user actions are the most important risk? Managers, who are identified as responsible actors, are responsible for an organization; hence for its cyber security. However, there is almost no knowledge available on managerial approaches and perspectives towards cyber security. It is thus imperative to know what the perspectives on cyber security of managers in the field are.

Since end user awareness has an important role in the dominant perspective in literature, it is important to check if that is reflected among managers in the field. Therefore it is explicitly included in the research. The main research question of this thesis is formulated as follows:

“What are the managerial and scientific perspectives regarding (organizational) cyber security and the role of end user awareness therein?”

In this thesis, a perspective on cyber security is defined as a subjective viewpoint on how to deal with cyber risks. Each perspective provides a coherent story by integrating a perception of cyber risk. In addition, how to deal with cyber risk and key elements of cyber security are included. In short, the perspectives in this thesis narrate how to approach cyber security and what the focus should be. End user awareness can be, but is not necessarily, part of a perspective on cyber security.

To embed this thesis in the existing framework of scholarly efforts, a typology of cyber security is laid out. By means of a literature review, various relevant dimensions are distinguished: cyber risks, risk management strategies, mitigation means and cyber security awareness.

To answer the research question, two separate methods are used. A literature review is used to derive scientific umbrella perspectives from literature; the Q-method is used to uncover shared perspectives from 40 managers in the field.

The perspectives derived by means of the literature review are mainly drawn from perspectives identified by Herley (2009). The first is: *Perspective I – The human is the weakest link.* According to this perspective, humans are 'lazy' and lack knowledge of security; therefore, they are bound to make mistakes. These errors form the most important risk for cyber security, which can be solved by educating the users and increasing their awareness.

Perspective II – Usability of security. In contrast to the first perspective, this perspective believes the end user is not to blame. Rather, the systems are too complex to use and therefore users make mistakes. It is not end user awareness, but security software development based on a user's functioning, that is the solution. This is called user-centered security software.

Perspective III – Economic perspective. This perspective believes the number of incidents is based on falsehoods, which frighten users. The consequences of cyber risks are said to be exaggerated, as well as the positive consequences of the security measures. Organizations should focus on cost-benefit considerations not based on falsehoods of impact and productivity. Consequently, the organization has a more profitable situation and the end users are not bothered with useless security measures.

Complementary, for the Q-method, 40 managers from diverse organisations ranked 48 statements related to cyber security. The specific rankings (or configurations) of these statements represent the perspectives of managers on cyber security. Within the Q-method, these individual perspectives form the unit of analysis. Through factor analysis, shared umbrella perspectives among the managers are revealed. The perspectives derived from managers in the field by means of the Q-method are as follows:

Perspective I – Clear in recognizing risks, inconclusive about measures. Although managers recognize that the cyber security situation in their organization can be improved, they are inconclusive about if, and which measures should be taken. Cyber security measures seem to be of low priority in most organizations.

Perspective II – Awareness as primary means in a strong avoidance strategy. The focus of these managers is on cyber risk mitigation and risk avoidance to the highest extent. Every possible measure can be taken to reduce the risk as much as possible. However, the focus is on the mitigation of the risk of human actions. This is done by raising awareness throughout the organization.

Perspective III – Economic considerations as base for cyber security decisions. The managers following this perspective are aware of cyber risks. Risks are real and managers have to deal with them based on economic considerations. A balance between cyber security and profit is sought, in which money is the key factor in deciding on cyber security.

Perspective IV – Cyber security is a matter for experts. These managers believe IT is a pillar of their core business. To retain their cyber security, appropriate measures have to be taken. The managers consider cyber security as a matter for experts, since experts have the knowledge which measures are best to implement in such a complex field.

The perspectives in the field have a high correlation and are thus partially similar. Only the main distinguishing characteristics for the perspective are named; therefore, similarities such as the same preference for risk mitigation and technical measures are less explicitly present in the description.

The comparison of the field perspectives and literature perspectives is based on the dimensions of the earlier described typology; resulting in differences and similarities. The first literature perspective and the second field perspective both strongly focus on the human as weakest link and awareness as solution. The third literature perspective and the third field perspective both underline economic

arguments in the security considerations. The field perspectives one and four are different from literature; literature perspective two is not recognized among managers.

All perspectives in both fields focus on human and technological risks, as well as risk mitigation and technological oriented means. The most important difference between literature and the field is that all field perspectives find awareness important, while literature perspectives II and III do not. One could state that awareness is dominant in the field perspectives. In addition, the field perspectives include more elements of the typology in their perspectives.

The results of this thesis are scientifically relevant; when put in dialogue, the field perspectives can be an enrichment to the perspectives from literature. Besides, the shortcomings of the perspectives regarding the typology can be leads for new perspectives. The managerial perspectives can also be a starting point for new managerial education programs.

However, the reader should bear in mind in that this thesis contains limitations. The perspectives differ in nature; the literature perspectives are developed by experts, which is not guaranteed for the field perspectives. In addition, awareness has a large focus in the statements, the results could differ if awareness was only marginally included. In addition, the statements are subject to interpretation of the respondent.

Conclusively some recommendations are made. For organizations, it is recommendable to avoid a narrow perspective on cyber security only focussing at one risk crucial risk and one solution. This prevents one-dimensional cyber security measures. To foster plural perspectives, discussions can be facilitated among the responsible and relevant actors of cyber security: end users, IT personnel and the managers themselves.

For the managers themselves, the perspectives can be used to reflect on their own perspective regarding cyber security. How does one's own perspective relate to other perspectives? In addition, the typology in this thesis can be a guidance for taking cyber security decisions.

Acknowledgements

I would primarily like to thank my first supervisor Dr. Maarten Kroesen, for his guidance, insightful comments and his friendly support during this thesis. When I had questions about my research, he steered me in the right way. His feedback and useful suggestions were an important addition to this thesis. Also, I would also like to thank my second supervisor, Dr. Wolter Pieters, for his critical view and his eye for detail. Furthermore, I would like to thank Prof. Michel van Eeten for his enlightening additions to the content of this thesis.

In addition to the graduation committee, I would like to thank Yasin Chalabi and Hiscox for the time I spent in Amsterdam. I had a great time in an encouraging environment.

I would also like to thank the respondents who have willingly shared their precious time during the process of interviewing for this thesis. Without their participation and input, the research could not have been successfully conducted. Special thanks to Dré Lameir, who provided me with connections in his network; this speeded up the search for respondents dramatically.

Finally yet importantly, I want to thank my family, girlfriend and friends for their never-ending support through the process of writing this thesis. Finishing my thesis would be a lot harder without them!

Maarten van Meijeren

Contents

List of figures

List of tables

List of acronyms

CBS	Centraal Bureau voor de Statistiek, Dutch governmental organization for statistics.
FUD	Fear, Uncertainty and Doubt. Strategy that scares people to perform certain actions, based on falsehoods (Florencio et al, 2014).
MKB/SMB	Midden- Klein Bedrijf, Dutch for Small and Medium Enterprises
P-sample	The set of selected individuals participating in the Q-method. Full explanation in Chapter 4, step 2.
Q-set / Q-sample	The set of selected statements that have to be ranked by the individuals from the P-sample. The Q-set is based on the aspects of the typology in this thesis.
Q-sort	The actual process of ranking the Q-set by the individuals from the P-sample; Step 4 in Chapter 4.
Z-scores	Normalized factor scores for each of the statements

Chapter 1: Problem statement and research questions

Introduction

Over the last years, the impact and frequency of cyber incidents has increased severely. There are many public examples; one of the examples is the widely covered hack of Sony (Robb, 2014). Accompanying numbers are clear; in February 2014, 360 million hacked accounts of Internet users were offered at illegal online marketplaces. Moreover, an indication shows that as many as 80% of all the US companies suffered from financial losses due to data and computer breaches (Greisiger 2010; Saini et al 2012). McAfee's (2014) estimate of the total impact of cyber incidents counts up to 400 billion dollar. In short, one could say the frequency and impact of cyber incidents are increasing; hence, there is an enhanced risk of being victim of a cyber incident.

Risk is according to Jones (2005) "The probable frequency and probable magnitude of future loss, or in other words how frequently something bad is likely to happen, and how much loss is likely to result". This is a general definition of risk; however, it can be specified on cyber risks. Cebula et al (2014) distinguish four different sources of risk that threaten the cyber security of organizations. These are actions of users, system- and technology failures, failed internal processes, and external events.

Technical risks and measures are part of the established elements of cyber security; technical risks and solutions were part of the 'first wave in cyber security' (Von Solms, 2000) and the necessity of technical measures is therefore commonly accepted (Colwill, 2009). The discussion in literature is more about the human factor. In this field, there is discussion about what the important risks and best approaches are. A dominant perspective in human factor literature focusses on human as weakest link; even stronger, this perspective on cyber security sees the 'risk of end user actions' as a crucial risk (Liginlal et al, 2009). The numbers of Liginlal show that over a four-year period, an increasing trend is visible in frequency of human errors. The total amount of cyber incidents caused by user errors, nearly reached 80%. In line with this number, Kevin Mitnick argued that the human side of cyber security is overlooked and consequently that humans form the weakest link in the security chain (Spencer, 2015).

Human errors happen due to inexperience and the lack of expertise (Stanton et al, 2005) of a user. These low expertise errors can be prevented by end user cyber security awareness, according to Liginlal et al (2009) and Stanton et al (2005). In addition, Turle (2009) explicitly states that organizations can avoid people- or user risk by training and cyber security awareness.

The preceding perspective only focusses on human as weakest link and one awareness as only possible solution. It seems to be one-sided to believe there is only one crucial risk for such a broad problem as cyber security; in the end there are much more risks for cyber security than user actions. Hackers cannot be stopped by awareness, just like an internet interruption. The same holds for the proposed solution, is awareness really the only solution to decrease the risk of user actions?

Apparently, categories of risk, such as: external risks and risks regarding failed internal processes are all marginal risks. This perspective might seem unlikely. It raises the question, whether there are, next to the perspective mentioned above, other perspectives regarding cyber risk and cyber security.

In addition, the risks are about an organizational context, while perspectives in literature are usually not connected to a specific environment. Responsible actors in an organizational context are managers, who dictate the policies and who can influence the functioning of an organization. Amongst the tasks in the organization, managers also have the responsibility to take care of cyber security. Managers have the responsibility for the measures taken; the question is if the focus in practice is also on end user awareness or whether there are any deviating perspectives? In other words, to what

extent are the perspectives in literature reflected among responsible actors? Because there is a dominant perspective in literature, it is likely that the same particular perspective influences the perspectives in the field; awareness is likely to be a dominant topic in the field as well.

In this thesis, a perspective[1] on cyber security is defined as a subjective viewpoint on how to deal with cyber risks. Each perspective provides a coherent story by integrating a perception of cyber risk. In addition, how to deal with cyber risk and key elements of cyber security are included. In short, the perspectives in this thesis narrate how to approach cyber security and what the focus should be. End user awareness can be, but is not necessarily, part of a perspective on cyber security. In addition, the end user in this thesis is defined by "*the person who will eventually use a product*"[2]. For cyber security, product means for example IT systems. In an organizational context, person will generally mean employee.

Regarding the managerial cyber security perspectives, not much research has been conducted among managers in the field. Research in the field of managerial perspectives regarding cyber security is non-existent according to Choi et al (2006). Several sources confirm this, which are also stated in the relevance section. There is almost no knowledge available on managerial approaches and perspectives regarding cyber security.

This leads to the conclusion that there is a need for research regarding common managerial thought on cyber security and the role of end user awareness in cyber security. It is imperative to know what the opinion of managers in the field is; what is their point of view or perspective regarding cyber security?

To know what the differences and similarities between the perspectives of managers and scientific literature are, the perspectives have to be compared. The reference point for the perspectives will be derived from scientific literature. By comparing the perspectives from the field and literature, differences and similarities can be revealed.

In addition, there is a need for a clear definition of cyber security and its dimensions. Therefore, what cyber security means and contains is necessary to investigate as well. The same holds for the context of managers. What are their possibilities to increase the security in an organization? What is the role of end user awareness? The typology including these topics will be derived from literature and has the function to guide the comparison of perspectives as well.

In this research, the perspectives of managers regarding cyber security are investigated and compared to scientific perspectives. A proper method is needed to capture a person's subjectivity. After having obtained field data, the results will be compared to the view on cyber security derived from scientific literature.

Relevance

This research treats the perspectives of managers regarding cyber security and end user awareness. This is relevant in academic terms, for there is a research-gap. Also for society, the results can be used to improve managerial awareness. Commercially speaking, the results can be used in order to adapt products on managerial perspectives.

[1]Perspectives are viewpoints of persons regarding a topic, which is of subjective nature. (http://www.merriam-webster.com/dictionary/perspective)
[2]http://www.merriam-webster.com/dictionary/end user

Scientific

In science, this is a new theme: very little is known about managerial perspectives regarding cyber security and end user awareness. This is acknowledged in the literature; Choi et al (2006) report negatively about the efforts made by science: the research regarding the role of managerial cyber security awareness on cyber security is 'non-existent'. Tsohou (2010) also notes that the managerial perspectives on cyber security are not researched thoroughly. In addition, Häussinger (2015) suggests investigating more on the managerial cyber security awareness related to the actions taken in cyber security. Literature indicates that there is only little known about the perspectives regarding cyber security, but literature also shows the importance of knowledge about managerial perspectives. The perspectives can for example be used as a starting point to develop improvement programs for managerial cyber security awareness (McCoy and Fowler, 2004).

However, information lacks about what a managerial perspective on cyber security is. Choi et al (2006) ask why, what, and how managerial decision makers should be educated about information security. Without this perspective regarding cyber security, it is difficult to expect better cyber security.

In this thesis, insight in managerial perspectives regarding cyber security will be given. This will be done by investigating, categorizing and analysing the actual managerial perspectives on cyber security and end user awareness. The perspectives will be compared to views taken from scientific literature. The managerial perspectives can also help to understand what the role of end user awareness in cyber security is. In addition, the results can be a reference point for managerial awareness improvement programs. Besides, the derived perspectives can help fostering an understanding of other managers and departments, as well as to improve one's managerial cooperation.

Societal

The possible contribution to society is based on publishing information that is useful for organizations to improve their cyber security. For example, the importance of managerial awareness is shown by Okenyi and Owens (2007); they consider managerial perspectives as a prerequisite to security policies and strategies; the perspectives are a guide to develop security-training strategies, which will eventually contribute to a cyber-secure organization. By publishing the perspectives, prerequisite information is available from which organizations can benefit.

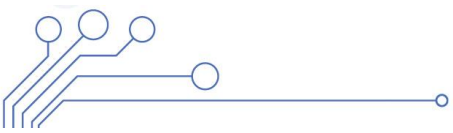
Secondly, a slightly different example; awareness at a management level is key to an effective policy-making. In the end, management sets out the occupations of its personnel (Vroom and von Solms, 2002). The results can enrich the current literature perspectives, because known perspectives can be completed with elements found in the field. The results can also cause an improved understanding of the management's perspectives on cyber security by other relevant employees. This mutual understanding can then again further cooperation.

Commercial

Knowledge about the perspectives of managers regarding cyber security is also relevant to commercial organizations, for example insurers.

To better address their customers and increase their cyber security, insurers want to have a better understanding of the perspectives of cyber security in management. For optimal adaptation, commercial parties need to know how managers think about cyber security. What is important in the current cyber security approach and how can commercial parties contribute?

Relevance for insurers is two-folded: on the one hand, the results lead to a better understanding of the customer. Better understanding of the customer means that product targeting can be improved and specified on the customer. In addition, the products can eventually be adapted to the customer.



On the other hand, insurers can help improve the awareness among management. The perspectives can be a starting point for the educational program. The knowledge in education can be connected to what managers already know; therefore, 'gaps in knowledge' can be completed. High cyber security awareness implies a high level of cyber security. Better security implies lower chance on damage, which means less chance on a recovery payment by the relevant insurer. For the insurer it can be profitable to help improve the cyber security of customers.

Research questions

The research questions focus on perspectives regarding cyber security and the role of end user awareness. Therein, the role of end user awareness is important, because a lack of end user awareness is perceived to be an important cause of cyber risk. The perspectives that will be found are likely to cover more characteristics. These characteristics will have differences and similarities with perspectives in literature; the results will be compared. Resulting in the following questions:

What are the managerial and scientific perspectives regarding (organizational) cyber security and the role of end user awareness?

1. *What are the perspectives regarding cyber security and the role of end user awareness in scientific literature?*
2. *What are the perspectives of managers regarding cyber security and the role of end user awareness in practice?*
3. *What are the differences and similarities between the preceding perspectives from literature and practice?*

Conceptual framework

To start, the current situation of the different dimensions is simplified in figure 1. The field of cyber security is until now in the thesis unstructured, which is presented by the 'cloud'. The relation of all kinds of concepts as risks and risk management strategies is not specified.

A manager or scientist perceives the different kinds of concepts in the field of cyber security in a specific manner; as, what is important in cyber security, which elements are included in cyber security and how should cyber risk be treated? The personal perception of a relevant actor results in perspective of preferences and importance of certain elements in cyber security. These preferences are the basis for actions.

The field of cyber security need to be structured, which will be done in the typology. The perspectives of managers and science have to be investigated. For both fields hold that common perspectives need to be found. It is not about individual perspectives, but shared perspectives among managers.

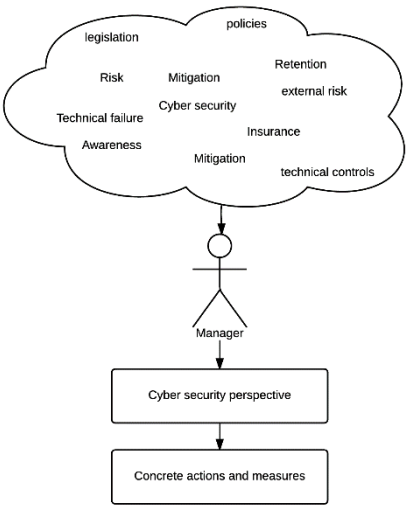


Figure 1 Conceptual framework of an individual manager (the 'cloud' contains random concepts in cyber security)

Methods

Literature review

The first question treats the perspectives in scientific literature. To derive these perspectives a literature review has to be performed. An investigation of relevant literature about cyber security and end user awareness is needed to answer the first research question. Literature will be gathered via scientific search engines like Scopus, Web of Science and Google Scholar. Many search terms can be used: awareness, human weakest link, usability, usable security software, user-centered security, information security, security governance, perspectives, cyber security, risk management strategies, IT, security, retention, organizational hierarchy, management and combinations of the keywords above.

The same holds for the typology of cyber security and end user awareness. What are cyber security and end user awareness? This will be investigated through a literature review as well.

Q-method

Capturing umbrella perspectives of managers is of an explorative nature in this thesis. Perspectives are up front unknown and have to be found. In order to find perspectives from the field, qualitative methods can be used. A face-to-face interview is a common used method to record the perspective of a respondent. However, interviewing a respondent is unstructured and subjective (Hollway and Jefferson, 2000). It is subjective in such a way that the researcher selects perspectives; while a different researcher can select other perspectives. In an unstructured interview, there is no methodological guarantee for selection of the 'right' perspectives.

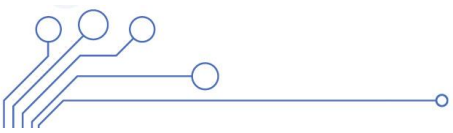
A method that deals with this subjectivity in a structured way is the Q-method. In the Q-method, a respondent ranks statements in one topic; the ranking of the statements represents the individual's perspective on the topic. An individual perspective forms the unit of analysis; by factorization, umbrella perspectives among the individual rankings are revealed. The aspects of this reasoning are briefly described next.

To be clear, the definition of 'perspective on cyber security' slightly differs in the Q-method. The configuration of statements about cyber security is the particular perspective. The statements form a coherent story (as perspective is defined) about the risks, how to deal with risk and the dimensions of cyber security; since these topics are included in the statements. Therefore, the ranking of statements is considered as perspective.

First, the Q-method catches subjectivity of respondents in a systematic manner (Brown, 1980). The Q-method allows subjectivity for the respondents, because the respondents rank pre-defined statements from their own point of view; therefore, the respondent applies his or her own opinion to the statements. In addition, the interviewer can ask the interviewee for the reasons how he ranked certain statements. This in order to uncover the underlying argumentation.

Thus, the configuration of statements represents the individual's viewpoint. The statements derive meaning from the relation to other statements (Dryzek & Berejikian, 1993). This is called the 'gestalt principle' as coined by Watts & Stenner (2005). According to Robbins and Krueger (2000), the Q-method can uncover perspectives or positions in a certain debate. In this thesis, it will be used in exploring the perspectives regarding cyber security. In addition, the Q-method is used systematically, because the pre-defined statements are for every respondent the same.

Last, the rankings (individual perspectives) of all the respondents can be factorized. Factorizing the results will cluster the population of different perspectives in umbrella perspectives (Watts and



Stenner, 2005). The structured way of using this method and the statistical analysis of the rankings, will result in a transparent and replicable way of recording and analysing subjectivity. Thomas and Baas (1992) already proved that by doing two tandem studies.

The Q-method is suitable for this thesis, because Q is a replicable way of capturing subjectivity of respondents. The individual perspectives of the respondents are combined in common perspectives through transparent statistical methods, which categorize the perspectives from the field. This is exactly what is needed to answer research question 2.

Target group

As the introduction and research questions already stated, the target group of this research consists of managers. Managers execute the roles that are described by Mintzberg (1975). Mintzberg writes these roles have more impact when they are performed on a higher level. The division of different management levels, explained by Simmering (2006), shows top-, middle- and lower management. Managers who are in the top- and middle management usually have much influence on the operations of the company; thus, also on dividing budgets and on the development of policy in order to manage cyber security on a high level. Lower management has too little influence on cyber security on an organizational scale.

In selecting managers for this research's sample, the following demands have been put in place:

- Managers can be in charge either of an IT-department or another department;
- A manager is part of the middle- or higher/top management;
    - In case of small size organizations, the owner is the top of management.

Examples of relevant managers are thus: managers in the board of directors, the owner of a small organization, a member of the management team or middle management like service managers and so forth.

Domain

For the Q-methodology, it is important to select managers who differ in perspective based on a certain factor (Brown, 1980). For example, it is likely that managers who have to deal with a lot of IT have a different perspective on cyber security than managers who do not work with IT at all. Therefore, factors who can possibly cause a difference in perspective have to be identified.

It is assumed that two important factors can influence the perspective of the manager, the importance of IT for the organization's business and the size of the organization. IT can be used as primary and secondary resource, a difference in focus on cyber security is expected. A web shop is expected to have different (better) cyber security measures than a butcher in a small village.

The size of the company can be cause for the difference in institutionalization of the measures taken. A small organization owner is responsible for every decision taken about cyber security; in a large organization, the responsible manager has to act on cyber security. A large organization is likely to have policies made by experts and complied with by employees. For a small organization, the policies and procedures have many overhead costs.

Both dimensions are thus expected to have influence on the perspective of individual managers in an organization. Therefore, the managers are ideally evenly selected from dimensions as presented in table 1.

Table 1 Dimensions for selection of managers

	Small size organization	Large size organization
IT as secondary resource	Limited focus on cyber security. Not recorded in policies and procedures.	Limited focus on cyber security. Measures are institutionally recorded in policies etc.
IT as primary resource	Strong focus on cyber security. Not recorded in policies and procedures.	Strong focus on cyber security. Measures are institutionally recorded in policies etc.

Comparison

In order to answer research question three, the comparison of the perspectives from the two different methods will be based on a parallel principle (Francis, 2013). As stated in figure 2, first the data collection and individual analysis of the literature review and Q-method is conducted. Thereafter, the comparison of the perspectives from both fields have to be performed. The comparison will be based on the elements from the typology that will be laid out in chapter 2 of this thesis. The comparison is based on differences and similarities of individual elements in the typology and their mutual relations.

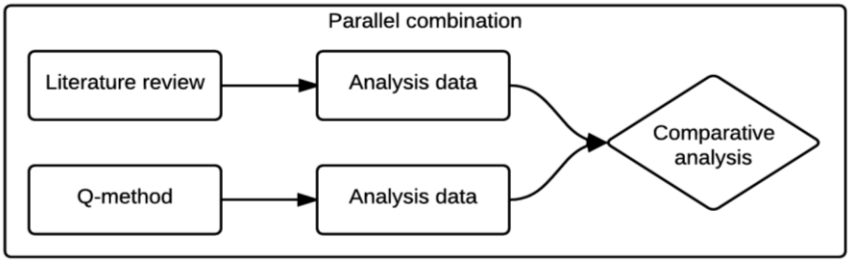


Figure 2 overview of the methodology to compare the perspectives from literature and the field

Structure of report

In the next chapter, the theoretical explanation of the relation of managers and cyber security will be investigated. A typology will be constructed based on the dimensions found in literature; this typology will be the guidance for the division of statements to select the Q-set. In addition, the typology will be used to guide the comparison of perspectives from literature and perspectives from the field on all aspects of cyber security. Chapter 2 is about typology of cyber security and cyber security awareness to guide chapters 3 and 4.

Chapter 3 has as goal to find an answer on the first research question, what are the perspectives in literature regarding cyber security and end user awareness. This chapter is closely related to the second chapter, since both are based on a literature review. In the second chapter it is about the different and separate dimensions of cyber security; the third chapter is about the literature perspectives (coherence of different dimensions) on cyber security and end user awareness.

Chapter 4 is about the perspectives from practice, or in other words the execution of the Q-method. The explanation and execution of the Q-method are merged. Which contains, the concourse, selection of Q and P set, the Q-sort and the factor analysis. In addition, the results will be explained based on the results gained in the Q-method procedure. Chapter 4 finds an answer to the second research question; what are the perspectives of managers regarding cyber security and end user cyber security awareness in practice?

Once the perspectives are analysed, the comparison of research question three can be made. Chapter 5 is exactly focusing on the question what the differences and similarities between the preceding

perspectives from literature and practice are. The results of the preceding Chapters 3 and 4 will be used. The comparison is made based on the dimensions of the typology developed in Chapter 2.

Lastly, Chapter 6 sums up the results and draws the conclusions. The conclusions are based on the preceding research questions answered in chapters 3 – 5. In addition, a discussion about the results is presented; accompanied by a critical reflection on how this research has been conducted. Conclusively, recommendations are made.

Chapter 2: Typology

Introduction

The typology in this chapter is constructed for two main purposes. First, cyber security will be discussed to explain dimensions of cyber security and end user awareness. At the same time, it functions as a guidance for the comparison between the perspectives from literature and the perspectives from the field for research question 3. Second (and already a little ahead), the typology of cyber security provides a division of dimensions and elements that can help to divide statements in the Q-set. How this works, will be explained later. In addition, the typology functions as an overall framework for this research. The typology is constructed through a literature review.

The research questions regarding define three aspects: managers, cyber security and end user awareness. First, the relation between managers and cyber security in an organization is explained. What can a manager do in an organizational context to improve cyber security? The next step is about cyber security, what does literature state about cyber security and the role of end user awareness therein.

Cyber security will be explained in different dimensions: risks, risk management, mitigation and end user awareness. Chapter 2 will mainly focus on the concept of cyber security in literature, thereby the role of end user cyber security awareness in cyber security.

Management perspectives

First, the managerial component of the research question has to be clarified. How are managers relevant actors for the cyber security in an organization? The manager can help to improve cyber security and end user cyber security awareness in different ways. Therefore, it is necessary to know what roles and positions the manager can have. As said, the manager can help, but it is not a golden formula to improve end user awareness. Security policies and strategies need to be followed to be successful, compliance has role in that.

Relevant roles

As stated before, the end user is seen as an employee in the organization. Employee and end user will be used next to each other. In addition, end user awareness and end user cyber security awareness will mean the same. Next the possibilities of the manager to increase cyber security.

The manager has some tasks that can influence the enhancement of cyber security. The manager can lobby for more resources to improve awareness; it is possible to divide budgets in favour of mitigation means, IT resources and awareness improvement programs. He can give the right example in cyber secure behaviour, monitoring behaviour to check what the awareness situation is, and the manager can spread information how to deal with the security policies. In addition, a manager can decide on technical measures to use; for example, invest in firewalls or DDoS protection.

In the further sections in this thesis, dividing budget, developing policy and management support will be mentioned. Management support means that management is in favour of a certain topic and is willing to contribute to this. So, management support for cyber security means that management is willing to provide budget and time, to improve cyber security in the organization. Management has to understand the goal and importance of improving cyber security, before they can fully contribute (Choi et al, 2006).

Organizational structure

The possible roles of the manager are explained, but the manager is also acting in an environment. The higher the position in the organizational structure, the higher the impact of the decisions. In the organization, there are different layers of management, which have different responsibilities. This is called a hierarchical organization structure (Meehan, 2010) the managers in the different layers have different tasks. Simmering (2006) is describing three different layers of management: top or higher management, middle management and lower management.

The tasks of the top management consist of controlling and overseeing the complete organization (Boundless, 2015). The top management is responsible for the company goals and strategic approach. The middle management is responsible for the execution of the organizational plans that are developed by the top management (Simmering, 2006). Therefore, these managerial layers are relevant for this thesis. However, the involvement of lower management regarding cyber security is limited and therefore excluded in this thesis.

The roles and possibilities that managers have according to Mintzberg (1975) can be applied on different layers in the management hierarchy. When the roles are on a higher level in the hierarchy, the impact of the decisions made by the relevant role are also higher.

Compliance

That managers set policies or give employees tasks does not mean that these are executed correctly. One can simply forget to do what one is commanded to do, or obligated by policy. Compliance is *conformity in fulfilling official requirements*[3]. The main issue is that commands or policies do not mean that they are executed like ordered. It can conflict with an employee's personal goals, such as efficient working, which can be made more difficult by security policies (Bulgurcu et al, 2011). It is also hard to be fully compliant, fulfil checklists with security requirements can turn into a goal in itself. Some aspects can be forgotten or the whole of regulations can just be too comprehensive (Spears and Barki, 2010).

Compliance is only briefly denoted, because it is only to mention that management support and managerial awareness do not imply cyber security is improved. Cyber security is a complex process, there are many papers on establishing a successful security awareness program (McCoy and Fowler, 2004; Peltier, 2005; Domingeuz et al, 2010). Management has the possibilities to deal with cyber security and end user awareness; however, the measures do not ensure improvement.

In the preceding section, the relation of the manager cyber security is explained. A manager has many possibilities to improve the security; the higher the position of the manager, the more impact his decision has. However, it is not a golden formula, because employees do not necessarily obey the rules and commands of a manager. Next, the other important aspects, namely cyber security and end user awareness will be discussed.

Cyber security

The other important components in the research question are cyber security and end user awareness. End user awareness is identified as one of the mitigation means to improve the cyber security. Awareness is like a final step in a decision chain for cyber security; risks of user actions need to be mitigated, therefore awareness can be used. Cyber security does not consist merely out of end user awareness as means to mitigate a wide range of cyber risks, but many other possibilities as well. In this chapter, the dimensions and possibilities in cyber security will be explained. Therefore, a typology of

[3] http://www.merriam-webster.com/dictionary/compliance

cyber security will be laid out; the use of this typology is an overall guidance framework for this thesis. The identification of relevant aspects of cyber security starts with the definition of what cyber security contains.

To define cyber security in this thesis, the definition of the International Telecommunication Union (ITU, 2009; part of the United Nations) is used. The comprehensive ITU definition says: *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability, Integrity (which may include authenticity and non-repudiation) and Confidentiality"*

The ITU definition mentions many different entities concretely. Important are the objectives: Availability, integrity and confidentiality. Also notable, the ITU definition does not explicitly focus on remediation of cyber incidents, but on prevention. This is because the focus is on retaining the objectives, not on restoring to a safe situation.

Different aspects can be derived from this definition of cyber security. First, why protection is needed; it is about protecting against *cyber risks.* Second, the manners in which cyber security is reached; this includes tools, concepts, guidelines etc. these *manners* are focussing on *decreasing the risk*, or decreasing the probability on an incident. Third, *risk management* is also in the list of means to mitigate the risk; which can be true, but management is on a different level than the other means; risk management is about the choice to mitigate risk or choosing another way to deal with risk (Bolot and Lelarge, 2008). Therefore, three aspects are distinguished in the definition of cyber security: *protecting against cyber risks, risk management* and *mitigation means*.

Lastly, *End user cyber security awareness* is an important aspect as well. Since awareness is perceived as important means to mitigate cyber risks in a dominant paradigm in literature. Therefore, end user awareness is part of the focus in this thesis.

The four different aspects are all aspects important for cyber security resulting in a decision chain; the decision chain is presented in figure 3. The levels indicate the steps in the decision process. The flow is top down; because first, one has to know what the risks are, then one can manage the risks, for example by mitigation. Last, awareness as a mitigation means.

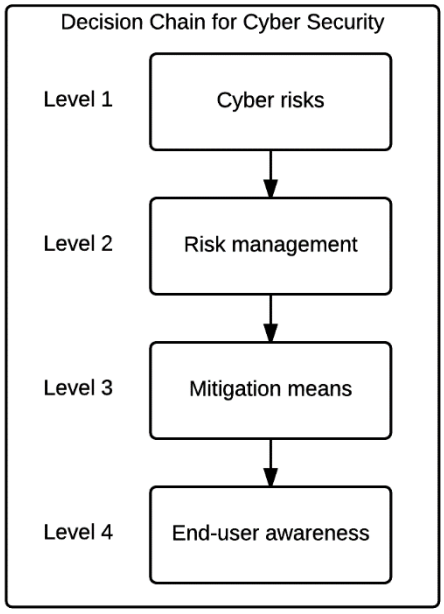


Figure 3 Decision chain for cyber security, with end user awareness as a mitigation means.

However, this is not the only possible path through the levels to reach cyber security. To find out what other possibilities are, each level has to be investigated. The typology for cyber security will consist of four levels; based on the four important aspects previously explained.

Level 1 – Cyber risks

The first level of the typology is cyber risk. In this section, the meaning of risk will be explained according to Jones (2005) and the division of risk categories will be explained according to Cebula et al (2014).

1.1. Risk definition

Recalling the definition of risk in the Factor Analysis of Information Risk (FAIR) by Jones (2005). Jones describes risk as "*The probable frequency and probable magnitude of future loss*". There are two important components: *Loss event frequency* and *probable loss magnitude*. A loss event is an event in which harm is inflicted to, for example, an organization; the loss event is in this thesis called a (cyber) incident. The aspects of risk are displayed in figure 4. The incident frequency is the probable frequency, in a certain timeframe, that an incident occurs. The probable loss magnitude is the expected loss that an incident causes. In other words, risk is the estimation of how often something bad happens and what the estimated impact is of future loss.

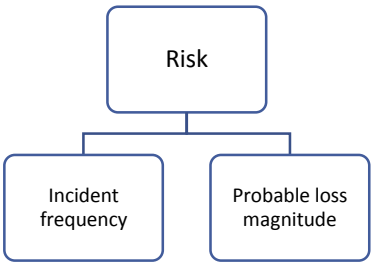


Figure 4 Risk equation (Jones, 2005)

An important part is a level 'deeper' in the risk equation tree (figure 5). An incident depends on two factors: *threat event frequency* and a *vulnerability*. This is important for the understanding of risk in total; an incident depends on a threat and a vulnerability. Jones defines a threat is "anything that can result in harm" and a vulnerability as a "weakness that may be exploited". An example: a hacker is a threat to an organization, because it can steal sensitive information. The hacker can only steal information if he breaks through security, which can through a vulnerability. In other words, the threat can only do harm if there is a vulnerability. This is important, because threats are only risks if the threats 'are stronger' than the vulnerability.

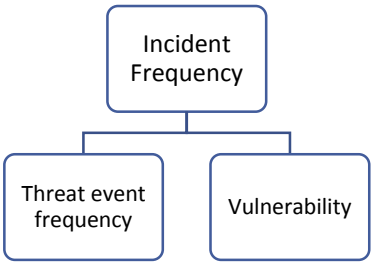


Figure 5 Left-hand side of the risk equation (Jones, 2005)

This applies on the next section in which different risks are categorized by Cebula et al (2014). The issue is these risks are only risks in a particular situation. For example, in figure 6, point 2.1.1 is only a risk if for example too little hardware capacity results in harm. To make it more concrete: if a web shop does not have enough capacity to process all orders on 'Black Friday', revenue can be lost; a situation in which harm is inflicted. Therefore, one can conclude that the risks stated in figure 4 are threats; they are only risks when there is a vulnerability. In this thesis it is assumed that the threats described by Cebula et al (2014) 'are stronger' than the relevant vulnerabilities; thus, are defined as risks.

1.2. Division of risks

The risk division of Cebula et al (2014) is already mentioned in the introduction, but now explained in more detail. The four different classes consist of *actions of people, systems and technology failures, failed internal processes, and external events.* Those different classes are defined to help identifying the applicable risks in an organization. By identifying and classifying those risks, a relevant risk management approach can be made.

To make it more concrete, for every class an example is provided: In *actions of people,* a threat can be clicking on a malicious link, resulting in an installed virus that has negative impact. So, there is a probability of occurring and a probability of negative impact; according to the definition, those components together form a risk. For a *failure in systems and technology,* an example is antivirus detection software failing to identify a virus or other malicious software. In *internal processes, failure*

is the lack of personnel to monitor organizations network on threats. *External events* can have negative influence due to fire in a datacentre or power cut due to lighting strikes.

It is not likely to classify a certain risk in more than one class; Cebula et al (2014) describes the risks in very detailed way. An overview of the detailed division is displayed in figure 4. An effect that actually is possible is cascading; risks can trigger other risks in different classes. The example given in the Cebula paper is the failure of security configurations; the configurations can be too stringent or too loose. This is classified as a risk of *systems and technology*, however this risk can be caused by inadvertent or deliberate user behaviour. The latter is classified as risk class: *actions of people (or end users).*

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
			4.4.3 Fuel
			4.4.4 Transportation

Figure 6 Taxonomy of cyber risks by Cebula et al. (2014).

The division of the different risks is useful, for example to define different approaches to manage the risks. A concrete example: a risk on a DDoS attack demands another approach than the risk on data loss. The division of risks provides a level in the typology to divide the risk and the possibility to couple it to an approach. It also provides an organized overview of the possible risks.

The different classes of cyber risk will help this thesis to identify the different cyber risks managers distinguish. The first level of the typology will be the division of different cyber risks (figure 7).

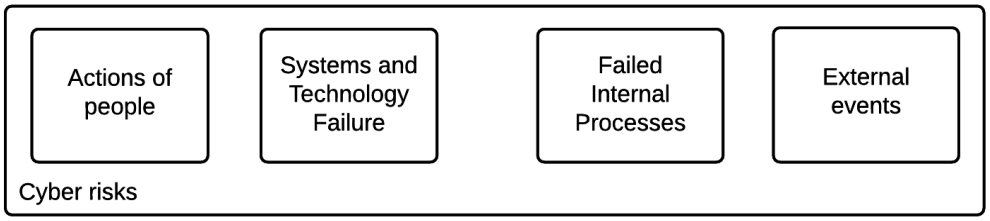


Figure 7 Level 1, risks in the cyber security typology

Level 2 – Risk management

The second level in the typology framework is about risk management. In the introduction, cyber security awareness is mentioned as a way to reduce cyber risk. Reducing risk is called mitigation; however, mitigation is not the only way to deal with risk. To regard the complete cyber security perspective of a manager, an overview of all possibilities to deal with risk will be given.

There are four ways of dealing with risk according to Bolot and Lelarge (2008): avoiding risk, retaining risk, self-protecting and mitigating the risk and transferring risk. The classification of the risks needs explanation. Every classification will be explained briefly on meaning and applicability.

2.1. Avoiding risk

Avoiding risk is a very rigorous option resulting in complete safety. Stoneburner et al (2002) define risk avoidance in the following way: "*To avoid risk by eliminating the risk cause and/or consequence*". This definition implies two ways of avoiding risk, proactively and reactively. Proactively avoiding risk is taking away the cause of the risk; an example is to cut the Internet off from an endangered systems. Reactively avoiding the risk can be illustrated by disconnecting a (part of a) network when it is attacked.

Bolot and Lelarge (2008) consider proactive avoidance as an infeasible option to the deal with cyber risk. By eliminating the cause, namely the Internet, the main functionality disappears, namely connectivity. A simple example, an end user not using the Internet is not at risk, but without the advantages of Internet. Internet usage is implying cyber risks; when the advantages of the Internet are used, the risks are present as well.

Reactive avoidance is not a feasible option as well. When a network or computer is disconnected in case of an attack, there is no connectivity available anymore. Connectivity is one of the main goals of the Internet. Example of a system requiring high availability is the Global Positioning System (GPS). In the definition of cyber security, the three main important goals to retain are Availability, Integrity and Confidentiality. Availability is lost when an avoiding risk approach is used which is not desirable.

2.2. Retaining risk

Retaining risk means that the risk will not change, however the way a company deals with the risk changes. Instead of reducing the risk an economic consideration is made; this consideration consists of assessing the financial consequences of an incident following from the risk. An organization can decide that own reserves of money are large enough to deal with the probable consequences of the risk. Risk retention is a way of self-insurance[4]. The financial reserve reduces the impact of the cyber incident, because the consequences are already budgeted (Becker & Ehrlich, 1972). A company can decide that they have enough reserves, but risk retention is not allowed in case the organization has stored personal information of customers.

However, privacy authorities dictate guidelines for protection of personal data. These privacy authorities also actively check organizations, on proportionality of the safety measures to reduce the risk and guarantee the safety of personal information. Obviously, hospitals need to protect their data stricter than online shops have to. If the measures are not proportional for the data stored, the authority can charge fines for the violations. Risk retention is in the Netherlands thus not allowed for organizations storing personal information. Another example, governmental organizations have to act according to their own BIR norm[5]. This norm obligates governmental organizations to have appropriate security measures according to the BIR classification.

[4] http://www.investorwords.com/19202/risk_retention.html
[5] http://wetten.overheid.nl/BWBR0022141/geldigheidsdatum_09-09-2015

Retaining risks completely is *legally* only possible in certain situations in which no personal data is involved. Some legal regulations also require strict security measures. Retaining risk is also only possible when the organization has enough financial reserve, exactly the consideration in the first paragraph of this section; a probable high impact, demands high reserves. That is only possible when there is enough reserve available.

2.3. Mitigating risk

Mitigation and self-protection against the risk is practically reducing the risk. Reducing the risk can be done in two ways; Becker and Ehrlich (1972) describe reducing the chance of the probable loss and Stoneburner et al. (2002) describe reducing the impact of the probable loss. Just like the both aspects of the definition of risk by Jones (2005), Jones explains mitigation as control. The probability on loss events have to be controlled by decreasing the probability of occurring; Jones agrees with Becker and Ehrlich (1972).

According to Jones (2005), the forms in which control can be performed are policy, process or technology; Cherdantseva and Hilton (2013) add legal options for control. In the ITU definition there are many options given that are part of one of the preceding forms. Namely the *"collection of tools, policies …."* describes the different forms by the ITU. Jones (2005) is on a more abstract level, but the concept is the same.

The nature of mitigation is described by the purpose. There are three different purposes regarding control (Jones, 2005): prevention, detection and response. This can be applied on different aspects of risk, namely: loss event, threat event and vulnerability. On each of the categories, the three different purposes can be applied (figure 8). So, a vulnerability can be prevented, detected and responded to. A structure can be distinguished; this structure is presented in figure 6. The structure explains that a loss event can be prevented by preventing, detection or responding to a vulnerability or threat event. Which is completely in line with the definition of cyber security of the ITU. The detection and response on a loss event are also in the scope of control.

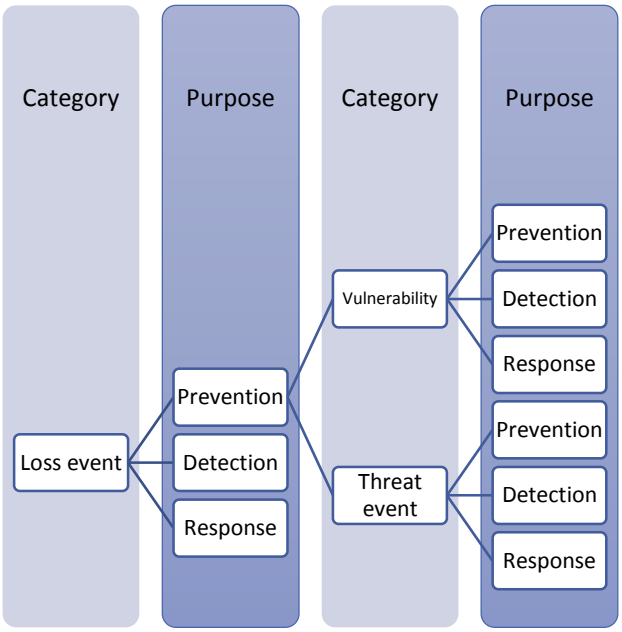


Figure 8 control category and purpose dimensions (Jones, 2005)

In this thesis, there is a focus on loss event prevention, in line with the definition of cyber security by ITU. The most important reason is that the objective of information security is retaining the availability, integrity and confidentiality. These actions can be taken by an organization, which is not yet hit by cyber incidents and can thus always be performed to lower the probability for a loss event to occur.

Mitigation is an important strategy in risk management; it is also explicitly stated in the definition of cyber security. This strategy will be discussed deeper in a further section. It will also be part of the cyber security framework introduced in this chapter.

2.4. Transferring risk

The last option to discuss in the scope of risk management is the transference of risk. Transference of the risk is transferring the responsibilities relating to the risk, to a third party. Third parties are for example insurance companies who are willing to take the risk and the possible consequences, but in exchange for a premium. The choice 'to insure or not' depends in general on what the expected cheaper option is. Is it worth taking the risk of a big loss versus paying a relative small premium without any risk?

By having economic incentives relating to cyber insurance products, the Internet can be made safer (Majuca et al, 2005). Insurers are a knowledge hub for risks, vulnerability analysis and prevention strategies. Security audits before contracting insurance are common, resulting in knowledge about weaknesses in the organization. Such audits influence the premium for insurance and are in that way a powerful mechanism to increase the network safety according to Lelarge and Bolot (2009).

A summary of the previous part is that cyber insurance has through economic incentives a positive influence on the safety in the cyberspace. This is however not specified, how does the cyberspace become a safer place? This is done through mitigation of risk; the economic incentives cause increased use of mitigation measures. Mukhopadhyay et al. (2013) shows that insurance is interesting as a complementary mean next to security. The advice of Shackelford (2012) is even more precise: organization should first invest in cyber security by installing firewalls, include encryption, and invest in intrusion detection and other means for protection. Siegel and Sagalow (2002) explicitly indicate that insurance is not feasible without the first line of defence like security software, products and tools.

The mitigation methods will reduce, but not fully eliminate risks. Insurance can be an interesting addition to cover the residual risk from the mitigation measures. Bolot and Lelarge (2008) state that there is no fool proof way of identifying and detecting risks. False negative and false positive incident reports can be gaps in security; another issue is the constant battle of better security and better worms. The struggle of how to get around security (Vojnovic & Ganesh, 2005). Completely eliminating the risk in cyberspace is not possible due to the 'messy humans' (Odlyzko, 2003); even when they are non-malicious users.

Thus, insuring cyber risk has two major components: the economic incentives coupled to insurance boost the cyber security measures taken and insurance is covering the residual risk. Insurance can be used as an additional approach to mitigation. Result is a maximal covered risk approach.

The risk management layer consists of four different approaches how to deal with risk: avoiding, retaining, mitigating and transferring the risk. In the typology the same division will be used, which results in the following figure (figure 9).

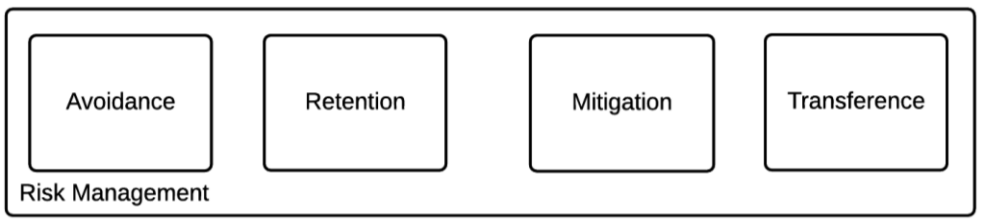


Figure 9 Level 2, risk management in the cyber security typology

Level 3 – Mitigation

In the field of mitigation in cyberspace, many options exist to reduce the cyber risk. According to Cherdantseva and Hilton (2013) four main categories to reduce cyber risk can be distinguished: technical oriented means, human oriented means, legal means and organizational means to reduce risk. All of the categories will be briefly explained.

3.1. Technology oriented means

Venter and Eloff (2003) provide an overview of the technological focussed information security means. This paper is focussed on technology for information security, but it can also be interpreted wider; the technologies are also applicable on the protection of the user's assets and other entities defined in the ITU definition of cyber security.

The technologies investigated and categorized by Venter and Eloff (2003) are divided in two main categories: proactive and reactive security technologies. Proactive security measures are about prevention; preventing the risk from an actual occurrence of the risk. Reactive security measures are focussing on the possible reaction after an incident. In other words, when an attack occurred or a breach happened, the actions to cure or solve the problem are reactive measures.

The main division is subdivided in three categories; those categories are the same for proactive and reactive measures. The three categories consisting of network, host and application level. The network level is 'a system of connected computers to share information', consisting of hosts. A 'host' is on the level of a single computer, which can be part of a network. The application level is on single application or single computer programs. In the displayed figure 10, the possibilities for technology protection are stated. Although the paper is from 2003 the protection methods are the same; only the content and development of individual methods has changed.

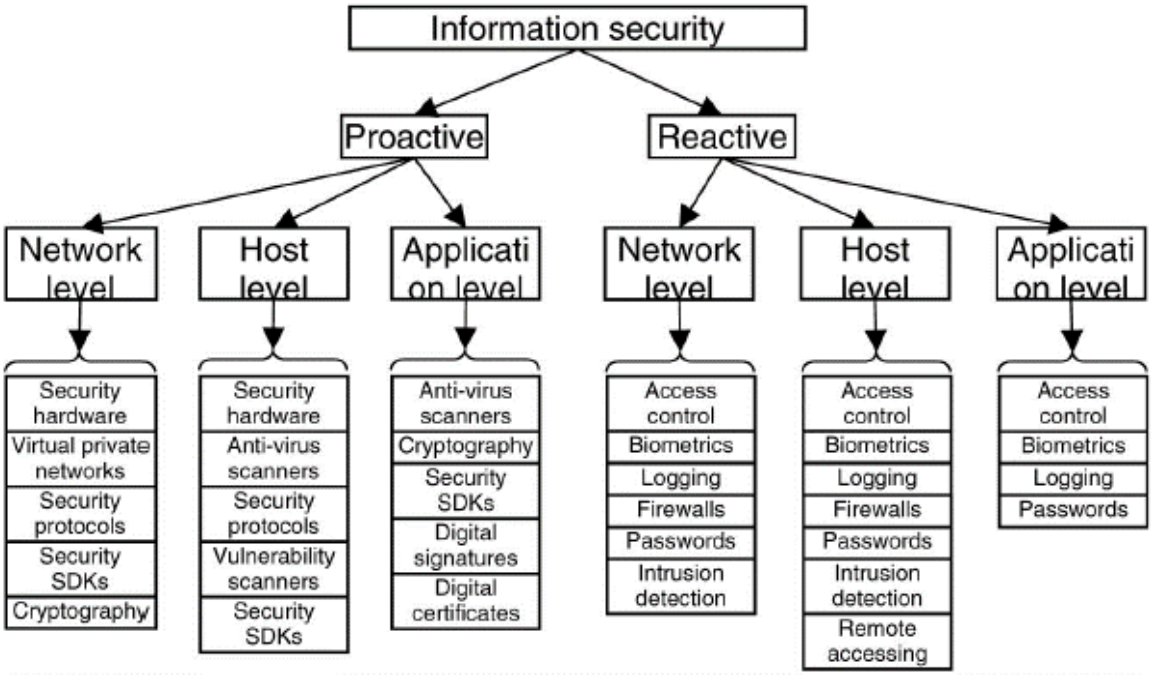


Figure 10 Complete overview of security methods categorized by Venter and Eloff (2003)

3.2. Human oriented means

The human oriented means consist of four important pillars described by Wilson and Hash (2003). Those pillars are awareness, training, education and certification. According to Cherdantseva and Hilton (2013), there are more factors as ethics, policy and rewards. The meaning of awareness in cyberspace is complex and will not be discussed in this part. Therefore, the term awareness will be used to the meaning according to Wilson and Hash (2003) only *temporarily* to illustrate the meaning. Since awareness has a large role in cyber security, it is described in a separate level in the typology: Level 4.

3.2.1.Awareness, training and education

Cyber security awareness needs to contribute to changing behaviour or strengthen good security behaviour. The Wilson and Hash paper defines awareness as 'knowing about issues relating to cyber risk', like possible infections and possible solutions. Awareness can be raised by paying attention to a certain topic and showing the importance of it, in this case cyber security. Presentation about awareness stimulate users to recognize security problems and act according to the situation. Awareness is just about focussing the user's attention on the cyber security issue, so that the user is aware of the situation. Awareness according to Wilson and Hash (2003) consist of only knowing risks, for example that a virus can infect your computer.

Training differs from awareness in the goals it has; the goals of training are to produce needed skills and competencies to act in a specific situation (Wilson and Hash, 2003). In the training, the goal is to master the skills and competencies to, for example, delete a virus on an infected computer.

Education is integrating the knowledge, skills and competencies for several specific situations that can be trained. This combination is one common body of knowledge about cyber security situations and how to act accordingly. Education is resulting in security specialists and professionals. Validating those skills and competences can be done by certification; it ensures a certain level of skill and competences.

Summarized, Wilson et al. (1998) describe the situation in different terms: awareness is about knowing 'what is cyber security'; training is 'knowing how cyber security is performed' and education is knowing 'why is cyber security performed'. In terms that are more formal, it is about information about-, knowledge of- and insight in cyber security, which can be validated by certification.

In the papers discussed in this section, awareness is seen as knowing what cyber security is. In literature, many definitions of awareness are stated. In addition, awareness is perceived more important by a dominant perspective in literature; therefore, level 4 in the typology will discuss awareness further.

Cherdantseva and Hilton (2013) also discussed policies and rewards. Rewards is according to them: simply rewarding people who made the right choices in cyber security behaviour. Policies relate to employees and cyber security rules. By being compliant to the policies the employees can be more cyber secure. Policies have overlap with organizational means, which will be discussed next.

3.3. Organizational oriented means

Other means for protection lie in the organizational factor. Organizational factors should also contribute to a safe environment. Organizational oriented means are characterized by administrative activities to enhance and maintain a secure environment where security measures can be effectively implemented and managed (Cherdantseva and Hilton, 2013); examples of organizational factors are security policies and procedures, strategy, audits and compliance. Management develops policies and procedures; the end user has to be compliant to them. For strategies, earlier is stated that management is responsible for the development. Organizational means are usually developed by

management. Procedures and policies are an example of overlapping administrative activities and management involvement. Therefore, the policy pyramid is highlighted next.

3.3.1. Organizational policies and procedures

As mentioned before, managers in any layer can use policies and procedures to implement their vision in the organization. The policies and procedures help to guide the subordinates to reach the company goals. ISO 9000 describes the differences among the terms and these are elaborated by Besterfield (2009). Besterfield describes the terms based on a so called 'documentation pyramid', this pyramid is presented in figure 11. There are four layers in the pyramid, top down policies, procedures, work instructions and records. The higher in the pyramid, the more abstract the documentation.

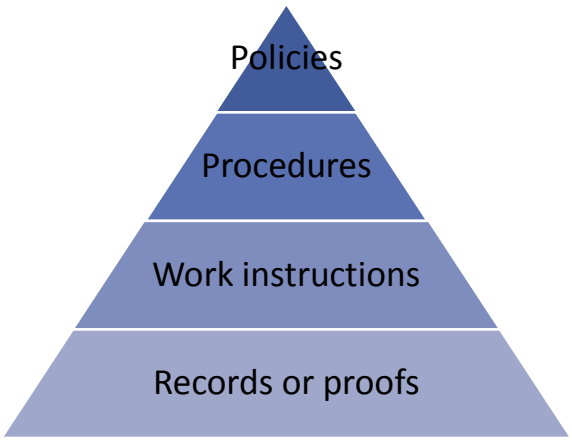


Figure 11 Documentation pyramid according to Besterfield (2009)

The core of a policy is described by Besterfield as "*what* will be done and *why*". Procedures describe *when* the task has to be performed, *who* it performs. In other words, the methods and strategies to implement the policies described. The procedures are more detailed than the policies. The work instructions is focussing on the detailed description *how* a job is performed. Proof should show that policies and procedures are actually respected.

Concrete examples and templates of security policies are provided by the SANS security policy resource[6]. Examples for policies are password policy and clean desk policy. Password policy is a measure to improve password strength; the password has to be stronger, thus each employee has to change his password. The new password has to be of a minimal length and contain symbols, capitals and numbers. Clean desk policy consists of leaving the user's desk empty behind. In this way, no crucial and sensitive information can accidentally be found by people who are not allowed to see this information.

There is not always a very clear distinction between organizational and human oriented means. There can be overlap; both are for example relating to policies, since policies, measure have organizational and human characteristics: employees should comply to policies and procedures, while management develops the policies.

3.4. Legal oriented means

Legal oriented means play mainly a role when company measures do not apply anymore. It is about data protection outside a company. When information is stolen or intentionally shared, legislation can offer protection against theft and improper use.

Another issue is the legislation concerning the safety of personal data inside a company. As explained before, privacy authorities are auditing companies on the implementation of (Dutch) data laws. The legislation serves the goal of protecting the data of citizens against improper use and theft. Other examples given by Cherdantseva and Hilton (2013) are service-agreements, job contracts and non-disclosure agreements.

[6] http://www.sans.org/security-resources/policies/

Summarized, there are four main categories of means to mitigate cyber risks. Technical-, human-, organizational- and legal oriented means. Each of these means has its own specific measures to mitigate risks. For the typology, the global four categories of means to mitigate will be used. Which results in following figure 12 representing the means to mitigate risk in the typology framework.

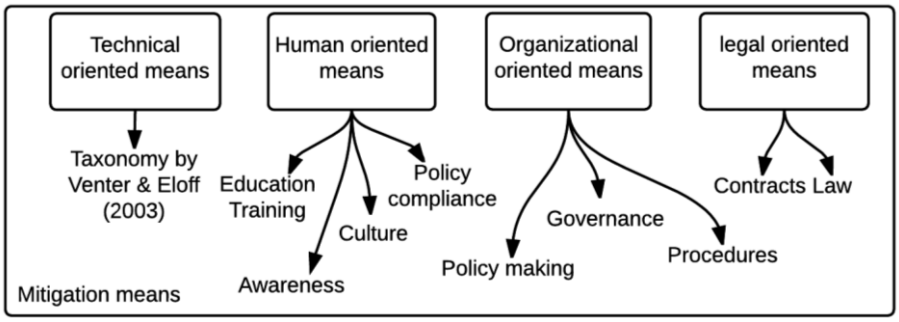


Figure 12 Level 3, mitigation means in the cyber security typology

Level 4 – Cyber security awareness

4.1. Cyber security awareness definition

In this thesis, the meaning of cyber security awareness of Wilson and Hash (2005) is used until now, but in this section, a proper investigation of literature will be performed. For cyber security awareness, many definitions are stated in literature. Most of the definitions regard information security awareness; in this thesis, cyber security is used instead of information security. Cyber- and information security are often regarded as the same; but as earlier stated in this thesis, cyber is more than only information. The means to protect stay the same; therefore, information security awareness will be regarded as cyber security awareness.

Häussinger (2015) discovered that in many papers about cyber security awareness, the definition is not clearly defined or not even defined at all. He also made a separation in definitions of cyber security awareness. The separation is based on several aspects that can be included in the definition, namely cognitive, behavioural and process aspects. For each of the aspects some examples of definitions will be given to illustrate the differences in content of the definitions. Not every definition that is found in literature is stated. Many definitions, which have almost the same meaning. Only the definitions with large differences in meaning are stated.

4.1.1.Cognitive aspect

The most elementary meaning of cyber security awareness is the cognitive aspect. This aspect is referring to the meaning of awareness by the dictionaries. The cognitive state is about 'knowing and understanding the importance of cyber security'. In other words, 'being well-informed about a certain situation or development relating to cyber security'. Those statements are directly derived from the definitions in the dictionary cited in the previous chapter.

As stated before there is no unambiguous definition of cyber security awareness. To illustrate the differences in the definitions regarding the cognitive aspect, some definitions from Häussinger (2015) are stated. Differences among the definitions will be explicitly explained.

More specific than the meaning of the dictionaries are D'Arcy et al (2009). They are in their definition more specific on what to do to minimize risks, but not what the risks are *"IS-users' awareness of security countermeasures: awareness of security-policy statements and guidelines, SETA Programs, and computer monitoring."*

The difference between risk awareness and solution awareness is emphasized by Hänsch and Benenson (2014). A definition that is including both aspects is from Straub and Welke (1998): *"Identifying and formulating problems with IS security breaches and computer disasters…"* and *"training should also make participants aware of the general effectiveness of deterrent, preventive, detective, and remedial countermeasures in lowering systems risk".*

Bulgurcu et al. (2011) take the separation one-step further; according to them, the difference in GISA and ISPA is important: *"General information security awareness (GISA) and information security policy awareness (ISPA) are the key dimensions of information security awareness. GISA is defined as an employee's overall knowledge and understanding of potential issues related to information security and their ramifications. ISPA is defined as an employee's knowledge and understanding of the requirements prescribed in the organization's ISP and the aims of those requirements."*

In this definition, the dimensions are the knowledge about cyber security and knowledge about the policies relating to cyber security. Knowledge about cyber security (GISA) also has the dimensions of *risk awareness* and *solution awareness*, made by Hänsch and Benenson. GISA does not exclude ISPA, but does not include it as well. Therefore, that means that different levels of awareness for both of these dimensions can exist.

More aspects can be included in the definition of awareness. Dinev and Hu (2007) explicitly describe entities to be aware of information assets, risks or technological issues. Hellqvist et al. (2013) focus on the explicit understanding of security policies, comparable with ISPA explained by Bulgurcu. The issue 'who is aware' is explained by Spears and Barki (2010); they emphasize the differences among different groups. One group is specifically named by Bray (2002); he is focusing on the employees. Another group is pointed out by Choi et al. (2006; 2008); they are focusing on the managers.

Overall, the differences of the definitions lie in 'what to know' and 'who have to know', but all agree on knowing of the risks and/or solution. The definitions all have in common cognitive is about a 'state of mind' of the user.

4.1.2.Behavioural aspect

The behavioural aspect is more than only a state of mind; it connects the cognitive aspect to an aspect of behaviour. Knowing about a certain situation results in acting in a certain situation. An example of a definition including the behavioural and cognitive parts is by Chaplin et al. (2011). This definition also is often cited: *"Security awareness is the extent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly."*

The largest part of this definition is referring to the cognitive part indicated by 'understanding'. Important addition to the cognitive meaning is 'act accordingly'; this addition is the behavioural part in the definition. These three words demand action in response to the understanding of the security situation.

A definition with only a small deviation is by Siponen (2000). This definition is one of the most used definitions for awareness in literature and is as follows: *"The term "information security awareness" is used to refer to a state where users in an organization are aware of - ideally committed to - their security mission".* The deviation is in the obligation to act or not. Chaplin et al. demand action conform the situation, Siponen is more careful and act accordingly in an ideal situation.

A wider definition is defined by (Kruger and Kearney, 2006) *"what does a person know (knowledge); how do they feel about the topic (attitude); and what do they do (behaviour)".* All three terms can be interpreted very broad, the definition serves like a directive with space for own interpretation.

Other definitions that indicate the behavioural aspect are 'complying to rules' (Hellqvist et al, 2013) or 'act according to your responsibilities' (Rotvold and Braathen, 2008), and 'a set of rules' (Shaw et al, 2009).

The behaviour demanded is according to what is known by the definition. If only knowledge about risks is included, one can only act to his knowledge about risks. The same holds for knowledge about solving cyber incidents.

The definitions with a behavioural aspect show that the line between behaviour and awareness is not very clear. All definitions regarding the behavioural aspect include also a cognitive aspect; there is no definition of cyber security awareness with only a behavioural aspect. Doing is only possible by knowing what to do.

4.1.3.Process aspect

The process aspect describes cyber security awareness as a process of raising or improving awareness; it also refers to the process to manage the activities to raise awareness. The process aspect can be described as only a process, but also cognitive and behavioural aspects can be included. Tsohou et al (2010) describes it as a solely a process: *"Awareness is an interfunctional process (check, act, plan, do) that crosses different divisional units or departments of organizations."*

Tsohou describes the process as interdepartmental in an organization; notable in this definition is there is no goal or usage named. In a different way, but also focussed on only the process aspect is provided by (Rastogi and von Solms, 2012): *"Information security awareness is a vital communication tool used by organizations to influence end-users towards compliance with information security policies and controls in the organization."*

In addition to the process aspect, the cognitive aspect can be included. (Lim et al, 2010) provides this type of definition: *"Security awareness are programs that teach employees to be conscious about information security policies and procedures."*

Differences among the definitions focus on how to shape the process, by raising awareness through programs that teach employees (Lim et al, 2010) or by booklets, stickers etc. (Spurling, 1995). Alternatively, how to achieve the improved awareness, by checking, planning, acting and doing (Tsohou et al, 2008). Central theme in this aspect is the process of improving awareness.

4.1.4.Summarized

To summarize, a flat and simplified view of the three aspects will be given; literature is more nuanced and comprehensive. Three aspects can be included in the definition of cyber security awareness according to Häussinger (2015). The cognitive aspect, which is to know about the risk and/or the solution regarding cyber security. In addition, the behavioural aspect, which is always, appears in combination with the cognitive aspect; one have to know before one can act. Last is the process aspect, which considers awareness as a process of raising and/or maintaining awareness. Ways how to do it can be defined. The cognitive aspect can be educated to a certain level, from low-level expertise to high level of expertise. The process aspect has to be continually educated to gain new knowledge, because by definition, it is always developing and never stops.

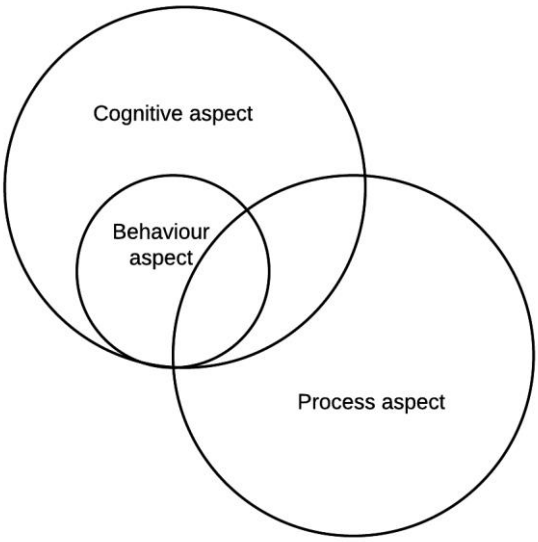


Figure 13 Possible combinations of aspects of definitions by Häussinger (2015)

4.2. Context

Besides the definition of end user awareness, awareness is used in a context. The context consists of goals of awareness, conditions for success and roles. These topics will very briefly be outlined in this section to illustrate the relevance for awareness; in the next chapter, these topics are explained more extensively.

In the possible objectives of cyber security awareness, many possibilities exist. Tsohou et al. (2008) provide an overview of different goals to be achieved by awareness: changing behaviour, developing a privacy culture and users understanding their security role.

The 'conditions intervening to success' as it is called by Tsohou (2008), represent factors that influence the success of cyber security awareness. Factors influencing the success are of a wide range: from language to complete organizational cultures. A lot of factor can influence the success, but in a different intensity; for example, when there is no budget (Casmir, 2005), it is hard to establish awareness improvement programs for employees.

Roles is already mentioned in the preceding part; Rastogi and von Solms (2012) mention different actors, like end users and organization. Spears and Barki (2010) mention users, management and IT professionals as actors in awareness.

The context of awareness consists of a few relevant topics, such as: goals, conditions and roles. These elements have to be included in the typology of cyber security. However, these elements are only described briefly. A more extensive explanation is provided in the next chapter.

4.3. Cause

In addition to the context, a lack of awareness is not always perceived as the only or crucial cause of human cyber risk. Adams and Sasse (1999) wrote a paper called 'users are not the enemy', which is a pledge not to aim on users as only cause. They claim that the user is victim of poor usability of security software; that is also the reason why the problems manifest with user interaction. According to Adams and Sasse, this unfairly indicates the human as weakest link.

Awareness as possible cause of problems is also included in the typology. It is relevant because different kinds of perspectives exist for the role of awareness in cyber security. The cause and conditions context of awareness will be explained more extensively in the next chapter. The next chapter describes the ambiguities of the conditions, there is no common view on the importance of awareness and its aspects.

Summarized

In this chapter, a typology framework for cyber security is created. This framework contains elements that embody a perspective on cyber security and the role end user awareness in scientific literature. In the first layer of the framework, several sorts of cyber risk are mentioned, namely: *actions of people, systems and technology failure, failed internal processes* and *external events.* To manage risk, several strategies are distinguished: *avoidance, retention, mitigation* and *transference.* In the orientation of risk management, mitigation is the most important strategy. This specifies different orientations on *human-, technology-, organizational-* and *legal means.* End user awareness is covered under the human oriented means. End user awareness is an ambiguous term, with aspects of *definitions, context* and *cause*. These will be explained more extensively in the next chapter.

Resulting in the complete typology framework in figure 14 on the next page.

The managerial role is not included in this framework. Recalling the conceptual framework of figure 1, the typology represents the 'messy cloud' on top. The typology is a tool for managers to structure the elements of cyber security and their mutual relation.

Managers can increase cyber security by the possibilities that provide the managerial roles (Mintzberg, 1975) stated in the first part of this chapter. Figure 14 is a visualization of the concept of cyber security and the role of end user awareness derived from literature. This concept will be used to make a division of the statements in the Q-set, which will be explained in chapter 4 relating to research question 2. Besides, this concept will be used to make the comparison of perspectives from literature and from practice for research question 3.

By investigating the literature for the typology, insight in the perspectives from literature is gained as well. The actual perspectives from scientific literature and analysis of the perspectives will be explained in the next chapter.

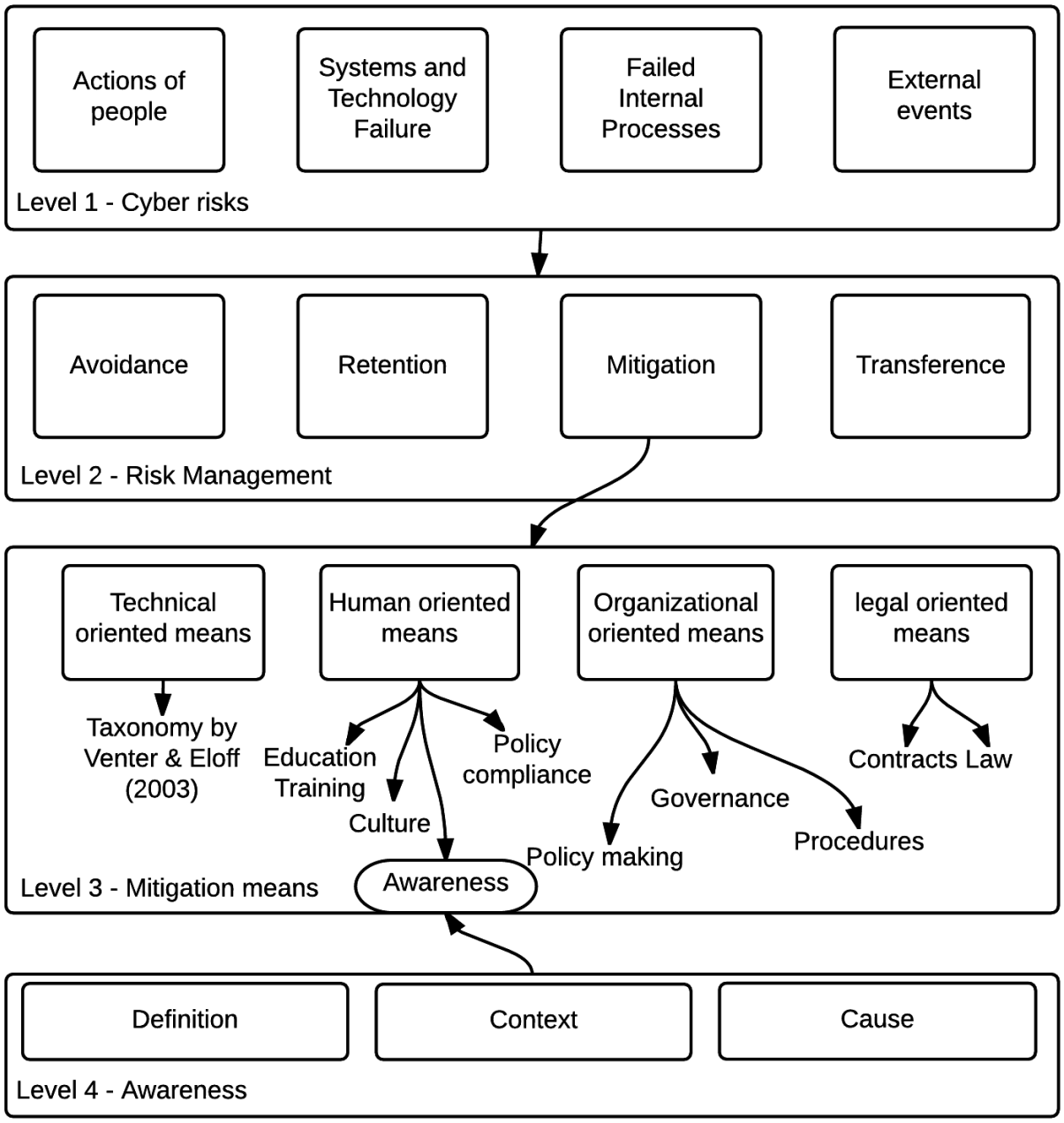


Figure 14 Complete typology framework of cyber security based on literature

Chapter 3: Perspectives from literature

Introduction

This chapter aims to reveal the perspectives on cyber security in the literature. To derive these perspectives, many papers are investigated to find relevant information. Scientific search engines Scopus, Web of Science and Google Scholar are used to find papers. The following selection of keywords is used to search: awareness, human weakest link, usability, usable security software, user-centered security, information security, security governance, perspectives, cyber security, risk management strategies and combinations of the above keywords. In addition, citations of papers found are used and author names of papers are used to find more papers as well. The supervisors of this thesis have also provided recommendations for papers.

First, the technical possibilities are usually accepted in literature as fundament for cyber security. Numbers of Colwill (2009) show that over 95% of business enterprises in the UK have technical prevention tools. Examples are: spam filters, automatic backup systems and encryption. There is not really discussion about whether technical measures need to be used; it is rather which technical measures are appropriate for which situation. As stated before, there are many possibilities, described by Venter and Eloff (2003), visible in figure 10. According to Von Solms (2000) the technical risks and measures have been the first step in cyber security. It is commonly known that technical issues are the base of basic security. However, the discussion is in human factors.

The different perspectives are mainly based on differences in the topic of human factors. There are different opinions about the role and elements of the context of awareness, as well as the goals and roles relevant for awareness. The main cause of debate is the role of awareness in cyber security; is a lack of awareness cause of increased cyber risk? Or does the topic of human risks has to be approached in a different way?

The ambiguities on the definition of awareness, the context of awareness and awareness as possible cause, can consequently have impact on the perception of necessity of awareness. Before investigating different perceptions of necessity, the ambiguities of awareness are explained. Afterwards, 'lacking awareness as cause of human risk' is discussed; resulting in three different perspectives on cyber security and end user awareness.

Ambiguities about the definition of awareness

There are many definitions of cyber security awareness defined in literature, although there is no uniform meaning. According to Siponen (2001), this is due to the informal nature of cyber security awareness. In addition, Häussinger (2015) found that in many studies cyber security awareness is not (clearly) defined, even if cyber or information security awareness is the main topic in a paper.

Some definitions include every aspect indicated by Häussinger (2015): cognitive, behavioural and process aspect. For example the definition of NIST (2003): *"The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. (…awareness seeks to focus an individual's attention on an issue or set of issues.)"* The question remains if all aspects should be included.

In literature, there is discussion about what cyber security awareness includes. Tsohou et al. (2008) pointed out some dimensions that are unclear, like, awareness including training and education or not; also what the goal of cyber security awareness is differs in different papers. Some of the dimensions of Tsohou et al. (2008) are used in this thesis, others are found in different papers like Hänsch and Benenson (2014) and Häussinger (2015).

It is important to understand the differences in the definitions of awareness, because confusion about the definition can cause confusion in communication. There is no “right or wrong” about security awareness according to Hänsch and Benenson (2014), but a clear definition is required to reach mutual understanding.

Because there is no uniform definition in literature, it is not likely that all the managers ‘in the field’ will have the same perspective of cyber security awareness as well. A deviation or ambiguity in perspective about cyber security awareness can be in different fields: the definition of cyber security awareness, the context definition around awareness and the issue that awareness should not be important at all.

To understand which differences in definitions of awareness exist, an overview will be provided. First, a graphical overview is presented in figure 14, followed by a brief explanation of each topic that is not uniformly clear.

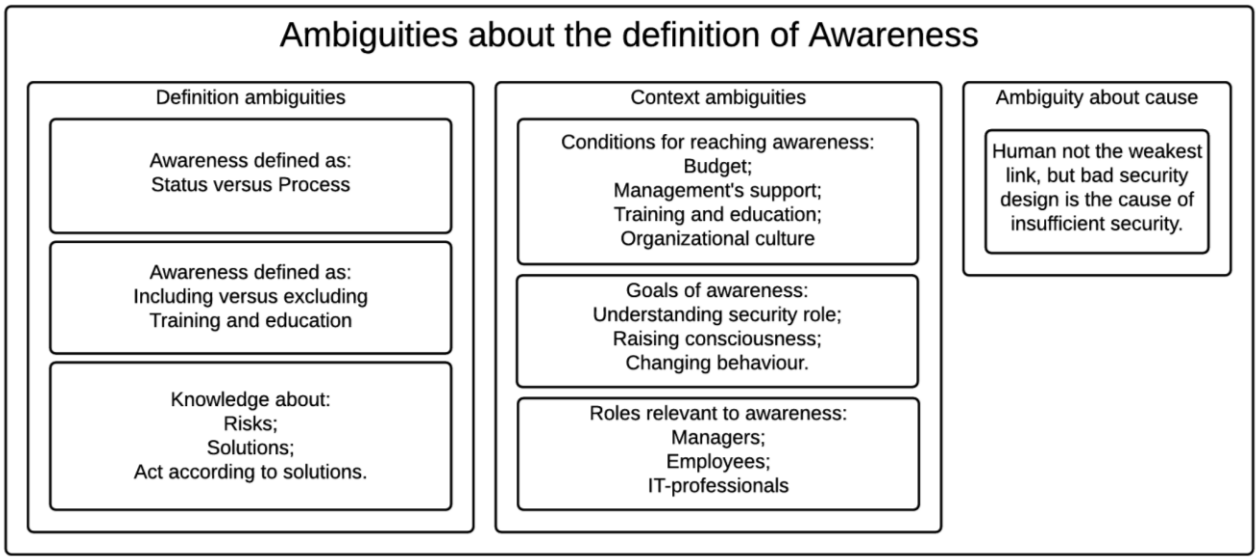


Figure 15 Overview of unclear dimensions in the definition of cyber security awareness

Issues regarding the definition

Literature does not know a single definition of awareness. There are a few different stances among which there are major differences regarding the definition. The differences are explained, so that one can understand what and why the differences are. The first difference is the idea of cyber security awareness as a status or as a process. Secondly, the definition of awareness, which should include or exclude education and training, is debated. Lastly, the knowledge part of, that what is called, awareness, remains unclear: knowledge about risks solely, about risks and means to deal with risk, or knowledge about risks, means and actions. All differences will be explained briefly.

Status versus process

Literature describes awareness in two different forms: awareness as a status versus awareness as a continuously process. Both classifications of behaviour, as a status and as a process, can result in secure behaviour; Siponen (2000) defines secure behaviour as ideal result of awareness. To illustrate the difference between status and process some examples are given:

Awareness as a status means that awareness is a static state of mind; it is a static result, which can be reached through training. Awareness as a status can have different levels: it can be high and can be low. That implies that awareness can be improved through training or education. The level of

awareness is thus a result of training and/or education. Not all definitions of awareness as a status are the same; what you are aware of can differ. For example, Bulgurcu (2011) differs in GISA and ISPA. The difference in 'what you are aware of' is explained later.

Awareness as a process has a different meaning: it means a continuous process to improve the awareness, by training and/or education. It is not a static situation, but a dynamic process that never ends. Awareness cannot be caught into levels or states. What the exact process includes can be different: only training or also reading flyers and having browser pop-ups as well.

Both classifications of awareness should result in behaviour that is positive for the security situation. Tsohou et al. (2008) makes the difference in status and process as well, but in different terms: awareness as a product and a process. The product is the result of training and process is a continuous process to raise awareness. This division is also made in literature by Häussinger (2015).

Awareness with(out) education and training

The differences between awareness and education and training are not clearly separated in every paper. This difference is explicitly indicated by Tsohou (2008) for the first time. Sometimes awareness only includes awareness as in the dictionary definition; other times it includes awareness training and education as well.

To illustrate the differences in papers, examples for the both classifications will be given: The definition by Wilson and Hash (2003) is explicitly separating the different terms: awareness, training and education. Resulting in: 'Awareness is not training, the goal is simply to focus attention on a certain topic', 'Training strives to produce relevant skills and competencies.' and 'Education integrates all of the security skills'. The meaning of the different terms differ explicitly.

Another used definition by Siponen (2000) includes training and education in the term of awareness. The definition he uses: *'a state where users in an organization are aware of – ideally committed to – their security mission.'* with the addition of *'awareness involves training and education'.* Therefore, there is no clear distinction in the terms.

For many other papers, the same conclusion holds there is no unambiguous adoption among the papers of inclusion or exclusion of training and education in awareness.

Knowledge about….

Next to the difference between status and intervention, there is also a difference in *what* a person is aware of. Cyber security awareness can include several topics like knowledge of risks, knowledge of risk management possibilities and knowledge of how to solve an incident. Hänsch and Benenson (2014) distinguish three dimensions: perception, protection and behaviour. Perception is the knowledge about the threats, protection is the knowledge about security solution and behaviour is acting to the knowledge about threats and solutions.

According to the division of Hänsch and Benenson (2014), Bulgurcu et al. (2010) is focusing on solely recognizing threats; not on solutions. Bulgurcu also differs in GISA and ISPA, which means there is a difference in knowledge about the actual threats and the security procedures of an organization.

Straub and Welke (1998) emphasize the difference between risk and solution in their definition (Already stated under the header 'cognitive aspect'). Knowing what the risk is, is different from knowing what the solution is. A solution might also differ in how it is informed with respect to remedial, detective or preventive measures.

Knowledge about the 'actions to take' are included in the definition of awareness by Shaw et al (2009). This is also important for Siponen (2000) and Kruger and Kearney (2006). Knowledge about actions can differ from 'knowledge about the rules to comply to', 'the sense to act according to your responsibilities'.

Awareness is not uniformly specifying what a user has to know. It can be knowledge about risk, solutions and actions to take. Moreover, what actions does a user have to take and which solution is the best for a certain incident. There are many possibilities, the topics pointed out in this part are presented to understand the differences.

Issues regarding the context

Contextual issues regarding the theoretical definition of cyber security awareness contain several topics: differences in goals, conditions to reach awareness and relevant roles for raising awareness. These topics are subject to discussion, for each topic the discussion will be briefly explained.

Differences in goal

There are some more goals stated in the previous part, but the point is that there is no common understanding of what the goals should be. This is also visible in the definitions used in this research. A goal according to Hellqvist et al (2013) is 'complying with rules' or 'act according to your responsibilities' according to Rotvold and Braathen (2008). Tsohou et al (2010) does not have an explicit goal: *"Awareness is an interfunctional process (check, act, plan, do) that crosses different divisional units or departments of organizations."* It only describes what it is. In a different way by Rastogi and von Solms (2012): "*to influence end-users towards compliance with information security policies and controls in the organization."* Straub and Welke (1998) have other goals: *"training should also make participants aware of the general effectiveness of deterrent, preventive, detective, and remedial countermeasures in lowering systems risk".*

The differences in desired outcome are in the field of raising awareness, influencing behaviour, improving compliant behaviour. It might also happen, these do not have an explicit goal. Fact is that the goal of awareness or an awareness program is ambiguously defined. The lack of a clear goal can be result of the diffuse definitions of cyber security awareness in general.

Differences in conditions

There is no common understanding about which of the factors are important to improve cyber security awareness. To understand the differences a few examples are given. Shaw et al. (2009) state that awareness training is one of the most important factors next to the factor of computer skills. Explicitly stated by Turle (2009): organizations can avoid people or user risk by proper training and awareness. Von Solms (2005) focusses on awareness programs to make users aware of the risk involved and their responsibilities.

Tsohou et al. (2008) find in literature many other factors. Factors like strategy, goals and vision; those have to be in line with the goals of awareness. Part of a strategy is budget, which is pointed out to be important by Casmir (2005). They find that management support is a success factor for increasing end user awareness. The reasons used in that paper is already stated earlier, before employees can be aware, management has to be aware to guide the employees. Other factors mentioned by Tsohou are risk analysis, security policies and procedures.

However, a single factor cannot improve the implementation of cyber security awareness (Casmir, 2005). Improving awareness is complex: Johnston and Hale (2009) regard awareness because of security policies that are implemented in an organization. Those implementations are complicated and

depend on many factors, such as governance and compliance. If the policies are well-designed, implemented awareness can increase.

The differences in conditions expose also another classification problem. The factors mentioned are not all in the same classification of the categorization by Cherdantseva and Hilton (2013). Strategies and policies can overlap with organizational culture in a way human and organizational means overlap.

Improving awareness is complex and there is no common understanding about the intervening success factors. Some papers state that single factors do not have the desired effect, but only contribute to a bigger whole of factors, which can influence the success of awareness. Another reasoning considers awareness as factor to reach a secure culture in an organization.

Relevant roles

This dimension is already pointed out in the previous chapter under the cognitive aspect of the definition of awareness. Different papers involve different roles in cyber security awareness. Some of the papers involve the board and end users, others only involve IT-personnel. This is also explained as one of the dimensions that make the definition of awareness unclear (Tsohou, 2008).

In this research, the papers used show some examples as well: Cyber security awareness refers to different groups according to Spears and Barki (2010); they describe end users, IT professionals and management as actors. Bray (2002) focusses only on employees and ex-employees. Choi et al. (2006) focusses only on the managers in an organization, by proving that more managerial awareness causes more managerial actions towards cyber security. Kritzinger (2006) involves every layer of an organization; he explains all the levels from user level to the board level, including the technical and security management. For all the levels the important task involved are specified.

Tsohou et al (2008) emphasize the differences in specifying the roles regarding cyber security awareness. It also shows that many papers do not specify the roles relevant to cyber security awareness. It is important to know that many opinions exist about the roles relevant for awareness, ranging from all the levels in an organization to just the IT department.

Lack of awareness as cause of cyber risk

In this research, it already became clear that literature is serious about the weak role of the user in cyber security; different examples in papers show the user is the weakest link in cyber security. There is a discussion about the role of cyber security awareness in cyber security for users. Namely, there are also papers describing the weak role of the user, but not blaming the user for that. Instead of the user, the experts and developers of security software and policies are blamed for the insecure user behaviour.

This view is proposed by Adams and Sasse (1999). The solution is user-centered security design is according to Adams and Sasse (1999) and Smetters and Grinter (2002). Usable security design is design of security measures and technologies from a perspective of the user. This is just an illustration of the debate. The discussion is about whether the user is the cause of the lack of security or not. The end user is thus not the cause of the problem, but only the place where the problem shows up (Adams and Sasse, 1999). A more detailed description of the exact debate is given in the next section about perspectives of cyber security and end user awareness.

Perspectives

During the literature research, the paper of Herley (2009, p.133) was found; this paper provides an explicit categorization of perspectives in literature: the user as weakest link, a lacking usability of security and an economic approach. In order to check the status of the division made, the author

contacted Herley. Herley answered[7] by emphasizing the lack of consensus about categorizing these perspectives among scholars. The division is a crude generalization of common perspectives in the field. Nuances are mainly ignored and only the general perspective is mentioned; the three perspectives found are umbrella perspectives.

The perspectives found in Herley (2009) are verified by investigating literature regarding the three suggested different perspectives. Literature research focused on the three perspectives identified by Herley and the findings are sorted on the perspective the paper is based on; not all papers sorted are used in the perspectives, since they are simply too numerous. The papers are stated in table 2. Perspective I is a dominant paradigm in literature, indicated by the numerous papers regarding the first perspective. For perspective I, 36 papers are found; perspective II, 12 papers; and perspective III, 7 papers are found. For the three topics, approximately the same effort is made to find papers.

Table 2 overview of the three perspectives of Herley (2009) and relevant literature for each perspective

Perspective I	Perspective II	Perspective III
Peltier (2005), Vroom and von Solms (2002), Bulgurcu et al (2011), D'Arcy et al (2009), Choi et al (2008), Tsohou et al (2010), Shaw et al (2009), Wilson and Hash (2003), Kruger and Kearney (2006), Hansch and Benenson (2014), Dinev and Hu (2007), Lim et al (2010), Stanton et al (2005), Okenyi and Owens (2008), Liginlal et al (2009), Im and Baskerville (2005), Liginlal et al (2014), Pfleeger and Caputo (2012), Turle (2009), Hellqvist et al (2008), Casmir (2005) McCoy and Fowler (2004) Rastogi and von Solms (2012), Dominguez et al (2010), Straub and Welke (2008), Spencer (2015), Vidyaraman et al (2008), Carayon et al (2003), Johnston and Hale (2009), Stoneburner et al (2002), von Solms (2003), Madigan et al (2004), Forte (2008), Tariq et al (2014), Colwill (2009), McNeese et al (2012) and West et al (2009)	Parkin et al (2010), Nurse et al (2011), Whitten and Tygar (1998), Braz and Robert (2006), Gutmann and Grigg (2005), Beautement et al (2008), Zurko and Simon (1996), Smetters and Grinter (2002), Sasse et al (2001), Faily and Flechais (2011), Görling (2006) and Adams and Sasse (1999)	Herley (2009), Herley (2014), Moore (2010), Anderson and Moore (2007), Florencio et al (2007), Florencio et al (2011) and Florencio et al (2014)

[7] By means of a mail conversation

First, the three different perspectives will be explained. Afterwards, the common ground of the perspectives mentioned in literature is discussed. Then the differences that exist among the perspectives will be treated. Lastly, the shortcomings of the perspectives from literature are denoted.

Perspective I – End user as weakest link

This perspective is also sketched in the introduction of this thesis. Risk of user actions is perceived as a crucial risk (Liginlal et al, 2009). Im & Baskerville (2005) researched the human errors in security accidents and concluded almost two third of the 119 human errors was accidental. In addition, Liginlal et al (2014) also investigated the difference between accidental and deliberate actions. Liginlal indicates more than two third of the 915 investigated human errors was accidental. For both researches, the remainder is considered as deliberate actions. Important is to note that not only malicious insider actions are included in the category deliberate actions, but also hacking from the outside are part of this 'remainder'.

The majority of the incidents in the category of 'risk of people' is a result from the risk of an accidental error. End user cyber security awareness can help to reduce accidental human errors (Liginlal et al, 2009; Stanton et al, 2005). These accidental errors are happening due to low expertise and 'laziness' (Stanton et al, 2005) of the user. These low expertise errors can be prevented by end user cyber security awareness, according to Liginlal et al (2014) and Stanton et al (2005). In addition, Shaw et al (2009) state that awareness causes the employees to understand their security responsibilities and reflect on how to use IT resources.

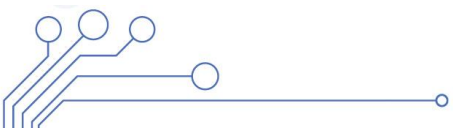
Besides, Turle (2009) explicitly states that organizations can avoid people- or user risk by training and cyber security awareness. Carayon et al (2003) indicate another reason why cyber security awareness is important. They state that cyber security awareness may reveal security needs and mechanisms for an organization, since understanding of critical errors increases awareness. In addition, awareness also helps avoiding user risk. Pfleeger and Caputo (2012) state that cyber security awareness will change behaviour; bad security behaviour has to be changed to proper security behaviour.

Not only education and training can be used to improve the awareness of end users; policies and procedures can also help to change the behaviour of the end user in an organization (Peltier, 2005). Besides, Lim et al (2010) mention the so-called security culture as a possibility to increase the awareness; a security culture is the totality of shared values, beliefs and behaviour to influence behaviour in order to increase the cyber security. The security culture should be more focussed on cyber security.

In other words, the user may make mistakes, because he or she is not aware or does not have the required knowledge to deal with IT. The user is the weakest link in the security chain. This issue can be solved by training and educating the user, so that his knowledge is up to date. In addition, security culture, policies and procedures can be used to increase the awareness of end users. Awareness is reached when the end user is aware of the risks, and knows how to act when encountering a risk. However, it is imperative the user is motivated to act cyber security aware (Stanton et al, 2005).

Perspective II – Usability of security

The second perspective from literature seeks the cause in security technologies, rather than in the end users. *The users are not the enemy*, as stated by Adams and Sasse (1999). However, the users have a role; users behave in an insecure way, because the security technologies are too complex to use. Therefore, many mistakes are made and consequently the user is blamed. The solution is found in so-called usable security.



Many security systems are too complex for a user (Adams and Sasse, 1999). For example, many websites have different requirements for passwords, whereas end users simply cannot remember all the different passwords. This will, again, negatively influence security (Beautement et al, 2008).The same holds for policies that require setting a new passwords once a month; it causes a lot of overhead for the end user; it even tempts end users to choose easy- to-guess passwords (Adams and Sasse, 1999).

Therefore, it is not the user who is the weakest link; it is the security system, which is problematic. In other words, stated by Vidyaraman et al (2008), the security designs are not adapted to the users; the security measures have to be aligned with the expected end user behaviour. A logical consequence of ignoring the user in the security design is bad usability (Zurko and Simon, 1996). Zurko and Simon (1996) introduced a term for this lack of usability: they say security is too often 'not user-centered'.

Parkin et al (2010) connect the lack of usability to a limited view on security. Security is often considered in terms of risk reduction, business impact and security control, but not in terms of impact on end users. However, a visible consequence related to end users and business are the costs to reset passwords that users forget; this costs time and thus money for the relevant department (Adams and Sasse, 1999).

Security and usability are often perceived to be mutually exclusive; but this compromise is too easily accepted according to Gutmann and Grigg (2005). They state that one of the most important characteristics of security systems has to be easy usage, without any knowledge rules or guides.

To come to usable security systems Zurko and Simon (1996) propose user needs need to be the primary design goal for the development of security systems. In addition, Adams and Sasse (1999) explain that users need to be involved in the development process. Whitten & Tygar (1998) set demands for usable security; usable security should be easy to use and hard to misuse. Over time, the skills of the user have to be increased by learning.

Summarized, it is clear that one should not only blame users; the security software may also be too complex to use. Therefore, there is no need to focus on awareness of end users, to increase security. Instead, the usability of the end user needs to be the central topic in security software development. This is called user-centered security software.

Perspective III – Economic considerations

The third perspective takes into account the economic consequences of increased security. Cormac Herley proposed this third alternative perspective (Herley, 2009). There are a few interesting things about the economic consequences of cyber risk and cyber security according to Herley. The known consequences of cyber security and risk are based on fear, uncertainty and doubt (FUD). However, the data used are not verified to create this perspective. In addition, the cyber security measure may do more harm than good, because they cost money and deliver nothing in return. Finally, Herley concludes that end users are not willing to put more effort in security and not getting anything in return as well. To prove this perspective, Herley used passwords to illustrate the economic advantages. Because the consequences in the example of passwords are easier to quantify.

Starting with the perceived consequences of cyber risk and cyber security, most of the information that end users know is based on FUD (Herley, 2014). FUD is about to persuade the end user 'that things are bad and constantly get worse' (Herley, 2014). Most of the information is false or creates confusion. In addition, Florencio and Herley's (2011) notion that the major part of the information that is used is unverified comes into play.

To illustrate that knowledge about the consequences of unprecise behaviour is doubtful Florencio et al (2014) investigated the use of passwords. They compared the use of simple and the forced use of more complex passwords. Passwords that are more complex cannot protect the end users against key-logging or phishing attacks; the complex passwords only protect against 'bulk guessing' and brute force attacks. Florencio and Herley conclude forcing end users to have passwords that are more complex does not result in significant more security.

Using more complex passwords even is harmful (Herley, 2009). Herley shows that end users are increasingly confronted with a more and more complex set of security advice and measures; as a result, there is an increase in end user effort and thus a loss of productivity. Nonetheless, there will still never occur a completely secure situation. Risks will be reduced, not eliminated. Therefore, when the end users ignore all the advice and measures to generate complex passwords, the end users save time and can use it to be productive. The time users spend to type the complex passwords does not outweigh the effort of the worst-case impact of a possible incident. Therefore, the effort to implement and use the security measures is higher than the damage of a possible worst-case impact.

In a more recent paper, Herley (2014) describes that even usable security is not a proper alternative. It is impossible to force every end user to adapt technology that is used for high-assurance environments; however, an unprotected environment is undesirable as well. Herley (2014) emphasizes that it is almost impossible to let the end user spend more time on security; this relates to the general misperception of a lazy and foolish end user, generated by FUD information. The end user makes a rational decision how to spend his time; security advice proposes a negative cost-benefit trade off. When there is more attention for security, attention elsewhere decreases. The security advice should be 'effort-neutral', only then there will be an increased attention for security without decreasing attention anywhere else.

Summarized, the third perspective focusses on economic consequences for the end users in an organization. First of all, the impact of cyber incidents is exaggerated and even worse, the advantages of increased security measures are exaggerated as well. An abundance of security measures can do harm; when increased security measures provide marginal increased security, the costs to implement and maintain the measures are higher than the possible costs of an incident. In addition, some end users do not like to make a greater (security) effort and get nothing in return; which is perceived as bad cost-benefit trade off. End users are not willing to take measures when the have to spend more effort. Security measures are interesting when they are effort-neutral.

Common ground

Three perspectives have been explained regarding cyber security and the role of end user awareness, however there is a common ground for the different perspectives. The common ground aims at mitigation as best option for risk management; in addition, the mitigation measures are particularly focussing on technological oriented measures and human oriented measures. The detailed common ground of the three perspectives will be explained next.

The main concerns for the preceding authors are cyber risks of technological nature and cyber risk engrained in human nature. Both topics are the main occasion for research in the field of cyber security. Papers aim at the mitigation of risks of human or technical nature. Which makes a connection with the other main topic in literature, mitigation as strategy. However, the topic of human risks cause division among researcher. The technological risks are admitted by almost all scholarly papers; equally, the risks have to be mitigated by technological means. As well as some of the technological means protect against more than only technological risks. Technical issues are also pointed out in the introduction of this chapter.

Most of the knowledge in scientific literature is aimed at the mitigation of cyber risk. Becker and Ehrlich (1972), Stoneburner et al (2002), Jones (2005), Venter and Eloff (2003), Cherdantseva and Hilton (2013) and many more describe how risk can be reduced. Mitigation is also grounded in the definition of cyber security as stated by the ITU. The other risk management strategies are investigated less. For example, proactive avoidance of cyber risk is perceived to be impossible by Bolot and Lelarge (2008); this is because of the nature of Internet. Elaboration on that is provided in Chapter 2 under Level 2. Transference in cyber is an upcoming subject in literature, but there are still many important knowledge gaps (Tondel et al, 2015). Retaining risk is performed by almost every cyber entity, because complete security is not possible. The discussion is about 'how much security is enough' by Soo Hoo (2000). This will be elaborated in the differences section.

The common perspective on technical cyber risks is to mitigate these risks by technical means (Colwill, 2009). An indication of the technical possibilities is given by Venter and Eloff (2003); this paper is based on investigations of many different technical means. Next to the technical means, there is a focus on the risk of human actions (Liginlal et al, 2009). Human related risk should be mitigated by human oriented measures. However, Kraemer and Carayon (2007) indicate that individual human elements and organizational elements in mitigation are very closely related and sometimes not separable. In addition, Colwill (2009) states that organizational oriented measures and human oriented measures are usually sensible to take.

The real difference is in the focus on human and organizational oriented means. Some of the papers indicate that man is the weakest link (Spencer, 2015; Im & Baskerville, 2005). Others find the usability of the security technology more interesting (Adams and Sasse, 2009), or an economical approach (Herley, 2009). This will be discussed in the next section about differences.

Summarized, the common ground is a mainstream acknowledgement mitigation is an inevitable strategy and technical measures are the first step in cyber risk mitigation. Spam filters, anomaly detection, passwords etc. are all technical measures that are the basis for cyber security. Technical risks are mitigated by technical measures. The differences among the perspectives aim on the risk of the human actions and the solution for that risk.

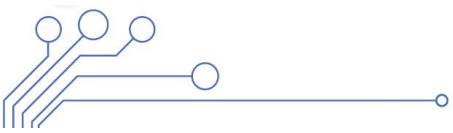
Differences among the perspectives

The perspective regarding the users as weakest link is the perspective with most scientific research. Many papers investigate the role of the user in security; also, on how awareness can be improved. Herley (2009) states as well that the weakest link perspective is overruling. He indicates this as very worrying. The usability perspective is smaller. Herley and Florencio are two of the few that investigate a different perspective. These three perspectives have their clear differences, explained next.

The risk of human actions is universally accepted; however, it is the approach to mitigate this risk, which is a cause for a division of perspectives in scientific literature. The differences are in the perception of the problem and therefore also in the perception of the solution of the problem.

The problem is in the first perspective clearly the end user. The end user is lacking and therefore he makes accidental errors. These accidental errors are the cause of many cyber security issues. The solution is to raise awareness of the end user and prevent him from making mistakes. Raising awareness can be done in different ways: through education, security culture or policies and procedures.

The second perspective does not agree on the cause of the problem. The end user is not 'stupid' and 'lazy' at all, but the security software and solution are simply not usable. The failure appears with the human interaction, so the human can be easily blamed. However, the problems only manifest when



users interact with the software, because the security software is not usable. That is why the focus is not on humans when improving security, but on the software. Technical issues are to blame.

The possible consequences of risks in the first two perspectives are too exaggerated according to the third perspective. The two preceding perspectives are nonsensical and only scare the end users. Both perspectives are said to be false, for the first two perspectives are based on falsehoods. Literally almost any research exaggerates the cybercrime impact, cyber security leaks impact and frequency. People have to be scared, in order to let them comply with extra security measures. However, the third perspective indicates end user are tired of endless compliance to security measures. A down-to-earth real cost-benefit approach proves that too much money is invested and too much productivity is lost in cyber security. The solution is to only take necessary measures and make the measures effort-neutral for the end user.

The differences lay especially in the way the cause of the problem is perceived; the perception of the problem implies a difference in the perceived best solution, which is the second great difference. The user is the problem according to the first perspective and has to be solved by improving their awareness; the second acknowledges the role of the user, but states the cause of the problem lies in the failing technology; therefore, technology has to be improved. The third perspectives accuses the first two perspectives of basing their reasoning on falsehoods. Solution is a fair cost-benefit comparison to weigh the measures.

Shortcomings

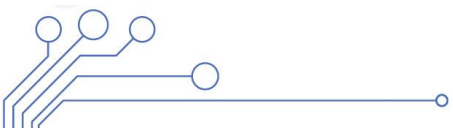
The similarities and differences are clear, but there are some other points that need explanation. The perspectives in literature are lacking in some points regarding the typology of Chapter 2.

Perspective I lacks an in-depth analysis of the problem; the problem is stated very linearly and idem for the solution of the problem. Only the human actions are a problem and only awareness is a solution for the problem. There are many more elements in the security situation of an organization like, organizational policies and external risks. Other risks and measures are not taken into account. The view that is explained only aims at the problems regarding end users; it also poses only the solution of awareness.

Perspective II is naïve to think that the problems are solved with only improved security software. People will make mistakes and elsewise social engineering will be an important threat. Besides, the security software is designed and implemented by humans; they can make mistakes as well. There is no notion of the feasibility of security usability. Nurse et al (2011) pose 19 additional requirements for a software developing process; this process is already complex and usable security is only adding another factor of complexity. Besides, when usable security is feasible, it probably makes the development more expensive. In the end, there needs to be somebody to pay for the extra effort.

The third perspective has its drawbacks as well. An important issue is the limited range of the research by Herley; based on research in the field of passwords Herley and Florencio explain their perspective. This is however, a small base for research in the field of security costs. Florencio et al (2014) indicate that information is based on falsehoods, but they do not provide a concrete alternative to estimate costs either. Herley and Florencio have no clue either. The impact of cyber security and breaches is hard to estimate. Therefore, it is hard to estimate where the concept of the third perspective can be applied.

All the perspectives ignore many aspects of the framework developed in Chapter 2. They mainly focus on a mitigation strategy and the risks in the field of technology and actions of people; however, failing internal processes and risk of external events are ignored. Moreover, as stated before, cyber insurance



is lacking in the risk management strategies. In addition, legal means are almost completely out of scope in literature. The possibilities are noticed by Cherdantseva and Hilton (2013), but nowhere elaborated.

An overview of all the topics discussed in the chapter is displayed in the table 3. Per level and aspect of the typology, the focus of the perspectives is presented. Per topic in the typology, the perspectives are divided based on their focus on the topic. If the perspective has a focus on a topic, the name of the perspective is presented under the relevant topic. The topics mentioned in the table embody the relevant perspective.

A concrete example for table 3: perspective I is mainly focussed on the risk caused by humans and a solution through raising awareness. All perspectives, including perspective I are focussed on technical risks and mitigation means. Perspective I is therefore noted in elements of the typology that are emphasized in the perspective. Table 3 is a quick overview to check which of the elements are included in which perspective.

Table 3 overview of the focus of perspectives in literature regarding topics in the cyber security typology

Level 1	Actions of people	Systems and technology failure	Failed internal processes	External events
	Perspective I	All perspectives	Perceived out of the field	Perceived out of the field
Level 2	Avoidance	Retention	Mitigation	Transference
	Perceived as impossible	Perspective III	All perspectives	Perceived out of the field
Level 3	Technical oriented means	Human oriented means	Organizational oriented means	Legal oriented means
	All perspectives	More or less all perspectives	Perspective III	Perceived out of the field
Level 4	Conditions of awareness	Roles of awareness	Importance of awareness	
	Perspective I	Perspective I	Perspective I	

The three perspectives have their strengths and shortcomings, but how do these perspectives compare to the perspectives from practice? The next chapter will investigate the perspectives of managers in the field regarding cyber security and end user awareness.

Chapter 4: Q-method and results

Introduction

In this chapter, the execution of the Q-method is described. In every step of the Q-method procedure, the step is explained and at the same time applied in this thesis. A brief overview of the content of this chapter contains; first of all, the preparations of the Q-method are discussed in step 1 – 3. Step1, defines the concourse; step 2, selects the Q-sample and step 3, selects the P-sample. Secondly, the execution of the Q-method is explained in step 4, performing the Q-sort. The results are analysed in step 5, called the correlation- and factor analysis. Finally, the interpretation of the result is made in step 6. All the preceding terms of Q-sample, P-sample, correlation analysis and so forth, will be explained in the procedure when needed.

The theoretical context of cyber security and end user awareness is given in Chapter 2. This theoretical framework will be used to categorise and select the statements regarding the perspectives of managers on cyber security and end user awareness in step 2 of the Q-method. This chapter provides the answer on research question two, regarding the perspectives from the field. Starting with step 1.

Step 1: Concourse

The concourse is a set of approximately 200 statements stating anything that is said or written about cyber security and end user awareness. This is derived from interviews, (white) papers, news and fora. Those statements cover all different perspectives regarding cyber security. Important is that the information is derived from the target group, that is the managers, themselves. Managers could express themselves in interviews. These interviews are an important part of the collection of data, because the information is from the specified target group itself. In addition, a completely personal perspective can be derived; all aspects of cyber security are connected by the same person.

The framework stated in chapter 2 in figure 13 is used to structure the topic of cyber security in clear aspects. Each of the aspects has to be covered in order to maximize the variety in the topic of cyber security. Aspects like different categories of cyber risks, different risk management strategies and ways of mitigation are all included.

In order to represent the complete topic, the statements of the concourse has to cover all the topics presented in the framework. The approximately 200 statements describe all the categories and the different perspectives per categories. For example in the category of external risks, there are two important risks: risk of third parties software leakages and risk of external nature events disturbing business. All the important subtopics inside a category have to be represented in the statements; in this case, both topics of external events need a statement. For every aspect, subtopics are identified. The concourse is 'full' when all the aspects are covered by at least a few statements.

Collection of data

Only information from the field of managers is relevant for the research. The Q-method is using the 'own terms' in the field to investigate a topic. That is why only managers are interviewed and information is gathered from journals and magazines relating to management and managerial tasks. The same holds for the Internet sources used. The process of gathering data will be explained.

Four managers were available for an interview[8]; these managers have different levels of (expected) knowledge about IT. However, it is hard to determine the exact level of expertise of a respondent in advance of an interview. Two factors can have influence on the expected knowledge, namely the position of the respondent and the business sector of the organization. When the position demands a

[8] Summaries in Appendix A

lot of IT knowledge or the sector is IT, the knowledge of IT will be higher than in other fields of positions. The selection of respondents takes place beforehand, based on the position they have in their organization as well as the business sector of the organization. To differentiate in the content of the statements different positions and sectors have been selected.

The positions of the respondents are all in middle- and top management. The requirements are according the description in the target group section in chapter one. The actual positions of the respondents are:

- Service manager in a hospital
- Service manager in an insurance company
- Delivery manager in a governmental organization
- Vice president of product development in an IT company

Not all the positions have a direct relation to IT. The reason for this is that the statements need diverse content to identify differences among aspects of cyber security. Knowledge about cyber security from different perspectives is needed.

The interviews are based on the framework presented in chapter two. For every umbrella category, cyber risk, risk management, mitigation strategies and end user awareness, managers are extensively questioned. This resulted in many statements covering many categories. Not every category was covered well or the content was not diverse.

Sources like journals, magazines and Internet are used to complete the information in every category. These sources are in the topic of cyber security directly aimed at managers, or about managerial tasks in cyber security. Examples of sources[9]: ITgovernance.com, which is about information security management; Security magazine, which is about security in general and sometimes about managerial tasks; A Manager, Dario Forte, shares his opinion about cyber security in a management paper including relevant issues in security.

Results

Analysis of the sources resulted in many statements about the topics in the framework. Especially the interviews are a valuable source. Approximately 70% of the statements in the concourse are based on the interviews. The other statements are from the other sources mentioned. Magazines and journals usually are about a single topic in the framework; incidentally, more topics of the framework are covered. Every topic can be easily referred to in an interview, which is more difficult in an article; that is a reason why many statements are from interviews.

The statements are derived from the interviews and articles. The extraction cannot be always one to one; some statements are only factual and thus contain no normative information, which is necessary for the Q-sort in the Q-method.

Some of the statements are slightly adapted to meet a normative character and can thus differ a little from the original source. Important is that the message of the source stays as much as possible the same. The headlines of the interviews can be found in appendix A. The final statements that are used in the Q-sort are stated in the next section. In addition, the process of selection will be explained.

[9] Infosecuritymangazine.nl / beveiligingswereld.nl / marsh.com / computable.nl / cybersecurityraad.nl / itgovernance.co.uk / msisac.cisecurity.org / nu.nl / white paper cyber security NCSC / Cyber security report UK

Step 2: Q-sample

The complete set of statements gathered in step 1 is not suitable to present to managers. The Q-method requires a reduction of the total concours to a selection of 40 – 60 statements, which is called the Q-sample. The Q-sample has to cover all the important topics stated by managers about cyber security and end user awareness.

The selection of the statements is based on a slightly adjusted framework from chapter two. It is adjusted, because some of the issues are not relevant. The goals of awareness appeared to be univocal and the theoretical definition appeared not relevant.

All sources regarding perspectives in the field agreed on the goal of awareness, namely increasing the security situation. There is no deviation in perspective on the goals of awareness; therefore, there is no need to include the aspect of goals in the Q-set.

In addition, all four interviewees indicated the irrelevant position of the theoretical definition of cyber security awareness in the research. The managers only cared about the organizational implications of awareness, because it is important for the security of their organization. This is to say, the importance in cyber security, the conditions to achieve awareness and the relevant roles for awareness. No matter what the theoretical definition is for an organization, these aspects matter. Besides, there is also barely a normative character in the theoretical definition, which is required for the Q-method.

Therefore, the framework is slightly adjusted on Level 4. In Level 3 of the framework all the specific measures are removed for the sake of a clear overview, nothing has changed in Level 3! Level 4 is adjusted in the following way; as stated, the theoretical definition and goals are not relevant and thus removed. The residual aspects are adopted in the selection criteria: conditions to achieve awareness, relevant roles for awareness and importance of awareness. These aspects are now forming Level 4 of the framework.

This results in the following framework in figure 16, which will be used for the aspects relevant for the perspectives of managers regarding cyber security and end user awareness.

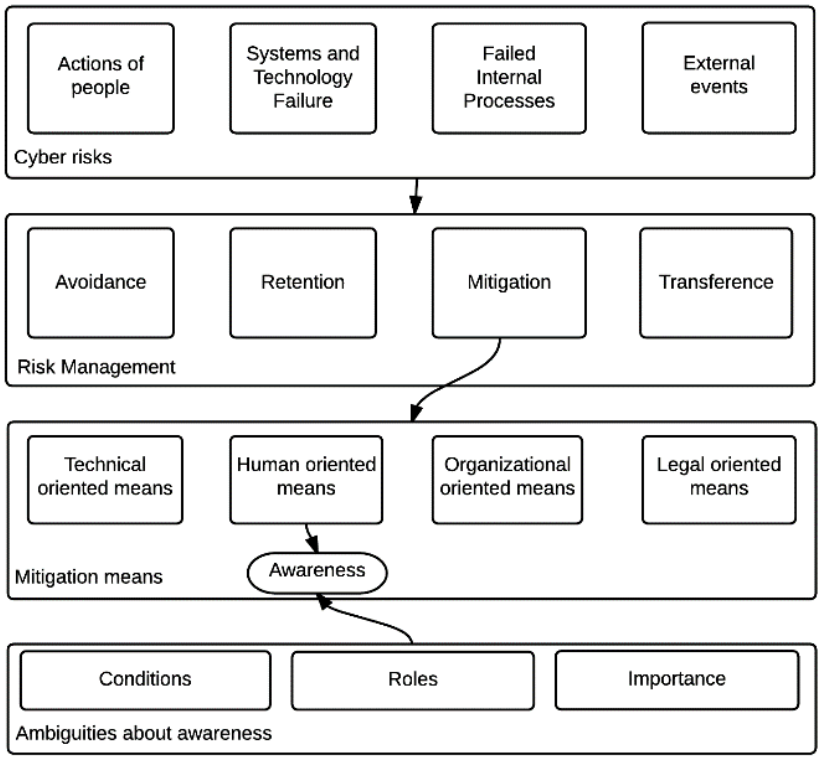


Figure 16 Framework with relevant aspects of cyber security and end user awareness

Explanation of the selection of statements

The selection of the statements has the objective to reduce the amount of statements to approximately 40 – 50 statements. Therefore, it is important to find the important relevant views per topic stated in the scheme in figure 16. In the final

set of statements, all the important views per topic have to be present. The selection is based on the (Dutch) concourse, which can be found in Appendix H.

To foster diversity in the views per topic, the statements are as much as possible selected from different sources. This seems logical, because other sources usually have other ideas and opinions. A single source will rarely have opposite or different views on a single topic.

For some topics, it is difficult make a clear distinction from other topics. For example, mitigation has a complete overlap with all the means to mitigate. Organizational means and human oriented means in the mitigation section also overlap a little. The choices made in these cases will be explained. The explanation of selection of statements per topic is as follows:

The only criteria for every set of statements is that it has to represent the different views that are present in the statements of the concourse. In other words, in the concourse, there are many things stated about one of the aspects of cyber security; the Q-set has to represent the same differences and similarities, but in fewer statements.

1.1 Risk: Actions of People

In the topic of risks through actions of people, there are three main opinions regarding the statements in the concourse: deliberate actions that cause damage; a small accidental incident that cause damage; and an error due to a lack of knowledge causing damage. With an addition to the topic of deliberate actions: managers often underestimate malicious behaviour by employees.

Many of the statements collected in the concourse are focused on only a detailed part of the risks and are thus too specific. For example, USB-sticks found and used by employees are dangerous; this statement is too specific to use. The following statements cover the topics described above:

- “The end user does hardly know anything about cyber risks and he does not know anything about dealing with the risks.”
- “Many employees working in a big organization implies a high chance on a cyber incident, because not everybody is compliant to the rules.”
- “A risk that has insufficient attention is the risk of unsatisfied employees that have access to sensitive data and systems.”

1.2 Risk: Systems and Technical Failure

Several major technical risks are identified by the interviewees. The first is the risk of outdated software; secondly, new technologies bring new risks; and last, technical failure or cyber attacks cause important risk. Many collected statements dive into the last category. Mainly because many different kinds of external attacks can be covered by this topic. The statements that are chosen are:

- “An underestimated risk is the risk of new technologies that cause new cyber risks.”
- “Outdated software is a big risk for cyber security.”
- “Unavailability of our services due to technical failure or cyber attacks has huge consequences.”

1.3 Risk: Failed internal processes

Failed internal processes is about the business processes and organizational issues in an organization. Several risks are important according to the statements in the concourse: there are issues focussing on the role of management; the procedures and measures are insufficient; and lastly, responsibilities are not well divided among departments. Those three topics have a variety in focus in the statements

in the concourse; the statements selected represent the views in the statements in the concourse. The statements are:

- "Top management underestimates the cyber risks."
- "Cyber security policies and procedures in our organization are not sufficiently developed."
- "Cyber security is seen as IT problem only too often. It is also about governance, leadership, culture, awareness and behaviours. These are often forgotten."

1.4 Risk: External events

In this section, there are only a few risks mentioned in the concourse. The most risks in this category are focussing on external events like, fire, flooding and power supplier failure. These are covered in a statement that is generally covering the complete topic of physical external events. Another issue that is often mentioned is software or services from third parties, which can contain leakages. This is the other issue covered in the final set of statements, which is:

- "Unavailability of our services due to external events like flooding, fire or Internet disruption is serious. We need to have a high level of up-time."
- "Suppliers and other third parties can be a serious risk for our organisation, due to their own bad/insufficient cyber security."

2.1 Risk avoidance

In the statements about risk management strategies, complete risk avoidance is perceived as impossible. However, risk is partly avoidable; risk avoidance is also perceived as better than recovering from incidents. Many statements gave uncoupling IT systems of the Internet as example of partly avoidable cyber risks. Therefore, the statements need to cover the impossibility of complete avoidance, but also have to stress the importance of partly avoidance. Another view emphasizes not to take unnecessary risks. Resulting in the statements:

- "It is better to prevent suffering from cyber attacks than to recover from cyber attacks."
- "An organization has to avoid risk as much as possible, for example do not save personal data that is not necessary to save."
- "Uncoupling several IT systems is a good way to avoid a part of the cyber risks."

2.2 Risk retention

The statements in the category of risk retention distinguishes several views. First of all, it is often said that 100% protection against cyber risk is fiction. Some of the statements give options how to treat the residual risk. For example, leaving the residual risk for what it is, because the organization will not be attacked anyway. Another view says, one does not have to protect against a risk when a risk is not relevant. Other sources indicate security is always an economical consideration. The statements covering the statements in the concourse:

- "An organization's cyber security cannot be 100% safe. There is always residual risk, which is acceptable."
- "Organizations do not have to protect against risks which never will be encountered."
- "There is a possibility that cyber risks can be accepted, when the costs of securing are higher than the possible impact."

2.3 Risk mitigation

Statements in risk mitigation methods also represent risk mitigation as a general topic. A general statement for mitigation has to cover an attitude towards mitigation. Cyber security is by definition

the attempt to reduce cyber risk, which is risk mitigation. That is why is chosen for a statement that is stresses the general attitude of organizations towards cyber security.

- "Nowadays almost every organization is an IT company, which implies every organization has to reduce risk by taking cyber security measures equal to an IT company."

2.4 Risk transference

Transference is by the interviewees directly linked to insurance. All respondents and sources associate transference with insurance. The content of insurance in cyber security is however not always clear. Others find insurance useless and some find insurance only interesting when it is economically profitable. Insurers could also function as an information hub. All statements that are found in any source are summarized by those four different views. Because there are four important views on insurance in cyber security, four statements are selected as well. The selected statements are expressions of those views:

- "Cyber insurance is useless; the (cyber) damage already had its impact."
- "Cyber insurance is not needed. The premiums are high and the chance on breach in our cyber security low. It is economical not interesting."
- "The role of insurances in cyber security and risk management is unclear to me."
- "Insurers can help organizations with cyber risk management; insurers have a lot of knowledge in the fields they insure."

3.1 Technology oriented means

To dive in all the separate technological means to mitigate cyber risk is too detailed for the statements. There are more general views on 'the use of technological means to mitigate risk'. Most of the statements are focussing on the specific measures that can be taken to improve security. The deviant views are on the general use of technological means, like: cyber security is the best solution to protect against risk, cyber security is important but not faultlessly and when certified technological means are safe. The following statements cover these views:

- "Cyber security IT systems should be tested regularly to improve the safety even further."
- "Total cyber security can best be reached through technological means."
- "When technical means are certified, they can be perceived as totally safe."

3.2 Human oriented means

Human oriented means are about means focussed on humans to increase the cyber security; or in other words, to mitigate the cyber risk. The statements are mainly focussing on the ways in which employees can be informed about cyber risks and risk management. There are different ways how to update the knowledge of dangers and solution: Only inform people by newsletter, set procedures to be complied to and a different approach is training. Those options can be used to raise awareness or educate people in the field of cyber security. The statements in this topic are covering the three options stated above:

- "It is sufficient to raise cyber security awareness of employees by informing the employees by newsletter or mail on the topic of cyber risks and how to deal with the risk. "
- "When employees comply with the policies and procedures regarding cyber security, sufficient mitigation of human errors is reached."
- "Cyber security awareness training has to be mandatory for every employee in an organization."

3.3 Organizational oriented means

Organizational means describe measures that affect the organization, not only a person or only technical issues. Examples of such means are policies, business processes, staff and responsibilities. Many statements indicate that only technological means are not enough. The same holds for only human means. Other statements are about the use of policies and certifying the organization. In addition, the issues of different responsibilities of the organization is mentioned. The main views regarding the topic of organizational means are: an integral cyber security approach is necessary; procedures are very important for cyber security and last: the knowledge to manage cyber security in an organization should be in the organization as well. The statements covering those topics:

- "The knowledge to manage all aspects of cyber security should be present in the company itself."
- "For every cyber scenario that is possible, even the unlikely ones, there have to be extensive procedures."
- "Organizations cannot without integral cyber security approach; cyber security has to be throughout the whole organization."

3.4 Legal means

There are three quite simple main views for legal means of cyber security: Legal means are useful, legal means are not useful and legal means bring obligations, which are perceived negative. The last option is in that situation also the only reason for having cyber security for many companies. Covered by:

- "Legislation is not necessary to achieve an acceptable level of cyber security."
- "It is necessary to contractually define cyber security with employees and third parties. Contracts that define cyber security measures that have to be taken by the relevant parties."
- "Some cyber security measures are mandatory by law. That they are mandatory is also the only reason they are taken."

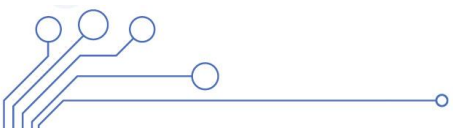
4.1 Conditions to achieve awareness

In the statements in the concourse there are several conditions mentioned to achieve awareness. Money was one of the factors that almost every interviewee brought in. Money can be used in different ways: more training or more personal coaching. Another field is management: Management support and noticing the importance of awareness by managers are also a major part of the concourse. Also integrating awareness through the whole organization is important in the statements of the concourse. That can be used in different ways: integrating awareness in the processes and procedures, other way is to let employees be aware. The statements cover the important views in this topic; the first statement is an example of employees being aware through the organization:

- "Employees have to be stimulated to report each other's' cyber incidents."
- "Management support is important to increase the cyber security awareness in an organization."
- "Much budget has to be available to improve the cyber security awareness in an organization."
- "Cyber security awareness has to be formally integrated in business processes. In this way no one can ignore security awareness."

4.2 Roles regarding awareness

The roles regarding awareness are about the question 'who has to be aware in an organization?' In the statements in the concourse, different roles are mentioned. Especially management is often emphasized in different ways: The whole management has to be aware, or only a representative



manager in the board has to be aware and some mention that awareness at top-level management is not high enough.

Another role is a dedicated department on cyber security. That can be one person, a cyber security officer or manager, or it can be a complete cyber security department. Which is explicitly not only an extension of the IT department. Cyber security awareness is also mentioned to be important for everybody in the organization. To cover the different roles in the concourse the following statements are selected:

- "All users in an organization have to be cyber security aware for the purpose of cyber security."
- "Cyber security is pushed off to the IT department. This department has to be cyber security aware, the rest of the employees do not matter."
- "For good cyber security in an organization a separate department or function needs to be cyber security aware. For example: a cyber security officer or a cyber security department."
- "In every board of directors or management team there has to be a security officer which is cyber security aware. Only then cyber security is guaranteed."

4.3 Importance of awareness

The role of awareness in cyber security is ambiguous. Some say that awareness is the solution to all problems regarding cyber security. Thus, technological issues are no problems; the human actions are the problem and are solved by higher awareness. Another view is more moderate: awareness is a part of the solution and has to be combined with other measures; measures like procedures and technical solutions. Another point of view does not know what the role of awareness is in cyber security. The statements collected are all under these viewpoints; the statements chosen are covering the most general message of the viewpoints:

- "For me it is not clear what the use of cyber security awareness is."
- "The human is the weakest link in cyber security; cyber security awareness can be a partial solution for that."
- "People in an organization are the biggest risk, which is why everything has to be focussed on increasing cyber security awareness of users."

Extra personal statements

There are some extra statements relating to the manager himself. The statements are about the context of the manager and his organization. This kind of information is normative and not appropriate for the side questions in the Q-sort. The context of the organization of the interviewed is important for the context of the answers of the Q-sort. The normative judgement of the manager is needed about the importance of IT in his organization, about the security of the organisation and the awareness of the manager himself. The importance of IT can be relating to the security measures taken and to the perceived own cyber security awareness as well. Therefore, the following statements are added to the Q-sample:

- "Our organization is well protected against cyber risks."
- "IT is very important in our organization."
- "My cyber security awareness is high enough."

Step 3: P-sample

The P-sample is the process of selection of managers who will perform the Q-sort (step 4). The P-sample is selected according to the requirements set in the sections domain and target group, in the

first chapter. The main issue is to find the all perspectives in the field, which are embodied by the managers.

In this thesis, it is assumed two main dimensions have influence on the perspectives of managers. The importance of IT for the organization's business and the size of the organization. For the illustration of the dimension, examples are given.

The first dimension is the importance of IT in the organization's business. IT can be a primary resource or a secondary- or facilitating resource. When IT is a primary resource, IT influences the revenues and profits. Failure in IT will immediately have impact on the business of the organization. For example, a crashed web shop will cause lost revenues. Therefore, the managers are assumed to estimate the worth of IT higher in comparison to managers who use IT as secondary resource. Since the risk equation is based on how much loss is likely to result, the risk will thus be estimated higher in organizations depending on IT.

IT as secondary resources has less impact on the business. For example, a small butchery doing his administration on the computer is not depending on IT in his primary business. When the computer fails, only his administration cannot be updated. The administrative proceedings are only postponed and business is not interrupted. The risk will not be estimated as high as in an organization with IT as primary resource.

A small business owner does not prefer to write every policy and procedure for cyber security down. Since it is a small organization, the overhead is huge and profit is minimum. In addition, a small business owner does probably not think all knowledge for cyber security should be incorporated.

Large organizations have different possibilities and thus a different focus. Incorporating all knowledge for cyber security can be cheaper for a large organization, because the costs can be spread over more revenues and services can be used by more employees. The size of the organization can thus influence the perspective of the managers.

The selection of respondents started in personal networks; respondents are obtained in all kinds of domains. Each respondent in the research is asked for another respondent; the 'snowballing' effect is used to acquire more respondents. The question to respondents focussed on new respondents with a likely different perspective than their own. In this way, many respondents with probable diverse perspectives are obtained.

In addition, on cyber security meetings and workshops for 'MKB Nederland'[10], respondents are asked to participate. On such meetings, many managers from organizations in SMB are present and related parties as well. The meeting functions as a hub for managers, who have an interest in cyber security. Therefore, they are likely to be interested in participating in a research about this topic. In addition, a SMB meeting is usually a collection of many different fields and thus very diverse. Managers acquired on such meetings also are used in the snowball method.

The procedures used to acquire managers resulted in 40 managers who participated in the study. Many different domains and functions passed by; domains like, transport, IT, healthcare, marketing, distribution, industry, textile, retail, bank, insurances, offshore and advocacy. Functions vary wide in the middle- and higher management; several CEO's, CFO's, owners, departmental managers, IT-managers, security managers and risk managers. All 40 managers are from top management or middle management.

[10] MKB stands for "Midden- Klein Bedrijf", as in Small and Medium Businesses/Enterprises

The dimensions of the different selection criteria are as follows. The dimension of organization size is divided in several categories. Organizations from 0-10 FTE; 11-100 FTE; 101-500 FTE and 501 and larger FTE. This division is usually made by Centraal Bureau voor de Statistiek (CBS) in the Netherlands. Ideally, of every group in the division an equal number of persons is selected. The actual number of managers in the research are per category respectively, 7, 10, 13 and 10 respondents. The distribution of managers is thus quite evenly divided per category

The other dimension is the role of IT as primary- or secondary resource. The amount of managers from an organization with IT as primary resource is 17. The residual 23 respondents is from an organization using IT as secondary resource. Both categories are and their mutual ratio are presented in table 4. With the broad set of functions, organization sizes and domains, a sufficiently diverse P-sample is composited.

Table 4 number of respondents per category in the P-selection

	Small size organization (<=100)	Large size organization (>100)
IT as secondary resource	7 respondents	16 respondents
IT as primary resource	10 respondents	7 respondents

Several managers asked explicitly for anonymity, because cyber security is an important and sensitive subject in their organization. Therefore, the results of the thesis will be anonymous.

Step 4: Q-sort

Q-sorting is one of the most important parts of the Q-method. This is the step where managers give their perspective on cyber security. Q-sorting is prioritizing the statements in a certain order so that it meets the individual perspective of the manager from the P-sample. The statements are sorted in a forced distribution; in this way, the respondents have to think more carefully about their choices. This can help to point out the real meanings of the individuals (Prasad, 2001). The forced distribution used in this thesis is presented in figure 17. The complete questionnaire can be found in Appendix B. The shape of the forced distribution is with quite sharp tails. Thereby, the differences in the analysis are expected to be clearer. There are 11 columns, with the values of '-5' to '+5'. The distribution used in this thesis is based on the distribution in figure 1 in Watts Stenner (2005). In total 48 places in the distribution are available, for every statements in the Q-sample.

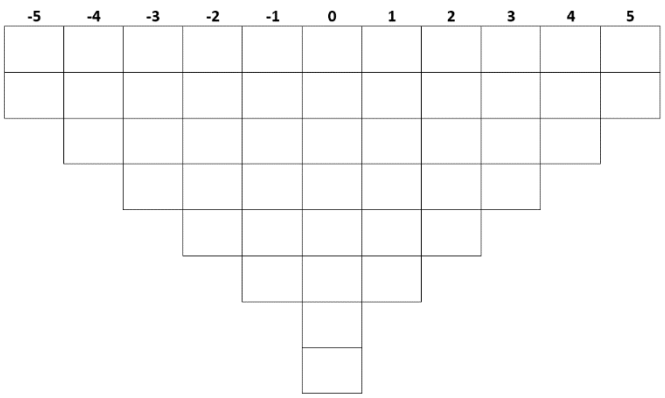


Figure 17 Forced distribution used to sort the statements

The Q-sort is usually performed face-to-face; in this way, the respondent can easily explain his choices. The Q-sort procedure starts with the sorting of the statements in 'agree', 'neutral' and 'disagree'. This makes it easier for the respondent to sort the 'pyramid', but also defines a reference point. This reference point can be used to define the 'real zero'. The means of the three piles are approximately:

agree, 26; neutral, 8; and disagree, 14; this implies that the real zero is approximately around the '-1' in figure 16.

The respondent sorted the statements in three piles and then fitted the statements in the forced distribution. After the ranking, his perspective will be discussed and his general view on the topic is asked. It is a way to check the sorting of the respondent. Questions like, is the current sorting corresponding with your view on cyber security? How would you describe your view on cyber security? Are you satisfied with the sorting? In the last case, some respondents confirmed their ideal ranking. Others admitted they would probably never get their ideal sorting, because every statement has its pro and con.

Seven managers were not able to do a face-to-face questionnaire; therefore, the Q-sort was performed by an online tool. Via HTMLQ[11], which is an extension of FlashQ[12], the Q-sorts are executed via a web portal. The results are automatically saved on a web server. The questions usually asked in a face-to-face sort, are verified by telephone call when possible.

Last step of the Q-sort is an additional form with question about the context. Additional information about the managers' own IT tasks, security-training, size of the organization, certification of the organization and knowledge about the legislation that holds for the organization.

The complete session took around 45 minutes to one hour. In this time, the Q-sort is performed and additional questions are answered. The scores of the Q-sorts are all entered in the software package by Peter Schmolk, the PQMethod software package[13]. This software package checks and validates the input of the Q-sorts. This particular software package is also capable of analysing the data, which will be explained in the next step, step 5.

Step 5: Correlation- and factor analysis

The information gathered in the Q-sort is put together and analysed in this section. The goal of the analysis is to reduce all the different views of the individual managers to shared major perspectives of managers. By factorizing the correlations of the individual respondents, clusters can be formed. The groups are based on a shared perspective regarding a cyber security. In other words, the managers choose the same statements in approximately the same configuration.

The theory and methods behind correlation and factor analysis are well described by Brown (1993). "Factor analysis examines a correlation matrix (Appendix E) and determines how many basically different Q sorts exist" (Brown, 1993). In other words, some of the Q sorts correlate very strong to each other and barely correlate to the rest; these Q sorts relate to a single factor (a cluster), which is called 'loading high on a factor'. Factor analysis determines how many factors exist in the total set of Q sorts. 'Loading high' means in terms of factor analysis that the respondent significantly correlates with the factor; the statement configuration of the respondent is closely similar to the statement configuration of the factor.

In this thesis, the PQMethod software is used to perform the analysis of the data. This software package is capable of doing the correlation analysis and factor analysis in a quick and easy way. PQMethod has implemented the Varimax method, which is a factor rotation method; The Varimax method combines two important characteristics; it maximizes the variance of the least possible number of factors. Before looking at the factor analysis, first the correlation analysis is explained.

[11] https://github.com/aproxima/htmlq
[12] http://www.hackert.biz/flashq/home/
[13] http://schmolck.userweb.mwn.de/qmethod/downpqwin.htm

The correlation matrix of the 40 respondents is characterised by mostly positive correlations[14] among the individuals. This means there is common understanding about what the statements mean to the respondents. The minimum of the correlations is -0.09 and the maximum is 0.80. The correlations are not of the same significance everywhere; many correlations are between 0.10 and 0.40, which implies there is enough room for differences in perspectives. A high correlation does not inevitably mean that the relevant respondents are correlated to the same factor.

In addition, every respondent respected the forced distribution of the ranking. This is presented in Appendix D; when a respondent deviates from the forced distribution, the mean would deviate from zero. However, all the respondents have a mean of zero and the same standard deviation.

The factor extraction method is called the centroid method. Which is preferred for usage in the Q-method (Watts and Stenner, 2005). The main difference with Principal Component Analysis is the focus on objects or individuals instead of variables. In centroid analysis it is about the individuals and the homogeneity with respect to their similarity on variables; PCA is about the homogeneity with respect to similarity of values assigned to variables by respondents (Krebs et al, 2000). The Q-method is also about the perspective of individuals; the perspective is recorded in a set of variables as a whole. The similarity of the individuals is needed. Therefore, the centroid analysis is the most appropriate reduction method to use. The factor extraction results in a set of factors.

Next, through the Varimax method, the data is rotated; Varimax maximizes the variance of factors across variables on a minimum number of factors possible. Important to note is that the rotation does not change any of the results. The rotation provides a different point of view for the researcher on the data (Exel and de Graaf, 2005). A different point of view can make it easier for the researcher to interpret the data.

Manual rotation can only be used when there are clear theoretical reasons. However, beforehand a theoretical basis is not known in this thesis, since unknown perspectives have to be mapped. Therefore, Varimax is an appropriate factor rotation method (Watts and Stenner, 2005). In addition, Varimax provides a single optimal solution; this increases the replicability of the analysis and thus the reliability.

Brown (1980) recommends seven factors to rotate, because that is the maximum number of plausibly significant factors in a data set states Brown. The Varimax is therefore executed with seven factors by the software of PQMethod. This resulted in correlations of respondents that loaded on only four of the seven factors. Therefore, only four factors are needed to explain the data of the respondents.

Loading high is a significant or distinguishing correlation, but 'significant' is not yet defined. The significance is usually set on a correlation of >.50. However, according to Brown, the significance is defined by $1/\sqrt{N} \times 2.5$ where N is the number of respondents. This would result in $1/\sqrt{40} \times 2.5 \approx 0.39$. This .39 is a guideline for the maximization of the amount of 'single loadings' in the total amount of respondents. A single loading, means each respondent only loads high on a single factor. Not loading at all is to say the respondent has no correlation to any of the factors; loading double means the respondent is significantly correlating with two factors. When loading double there is no significant proof for correlation to a single factor, therefore the respondent cannot be assigned to any of the factors.

[14] The correlation matrix of the respondents is presented in Appendix E

Maximization of the amount of single loadings of respondents results in a maximal amount of respondents loading on one of the factors. The more respondents loading on a factor, the more individual perspectives of respondents are included in the analysis. Multiple significant loadings are called confounded and these respondents are usually left out any further analysis (Akhtar-Danesh et al, 2008); the same holds for respondents without significant loading. The maximization of respondents on a factor is graphically represented in figure 16. When the significance threshold is set at .41 the amount of respondents is maximized.

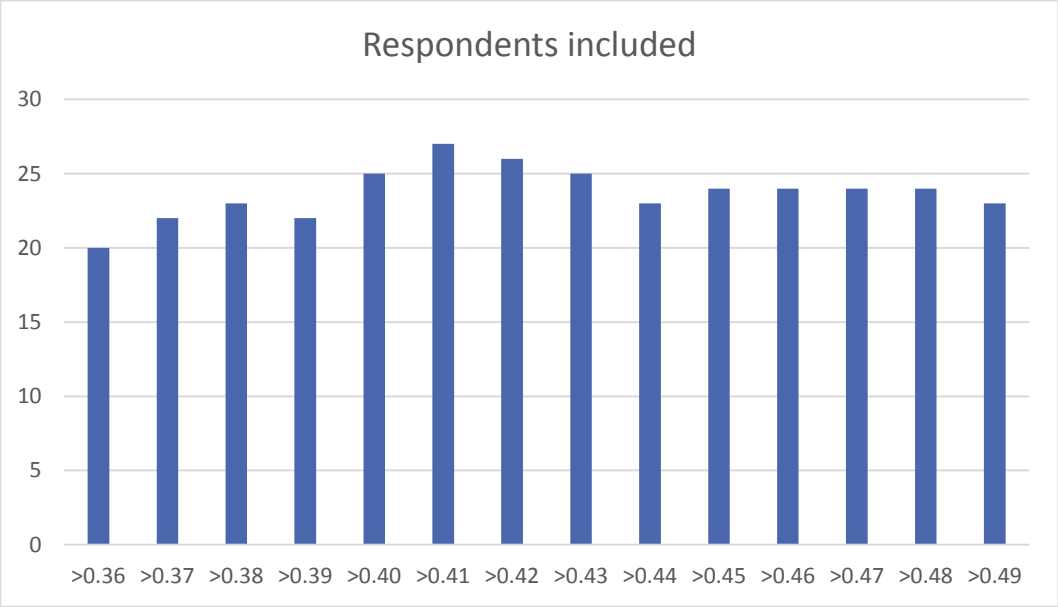


Figure 18 amount of single loading respondents in respect to the threshold of the loading

The results of the Varimax rotation are presented in Table 5 on the next page. Only on four factors, the respondents load high; therefore, only four factors are presented. The respondents that load on a factor with a value above the significance threshold (.41) are correlating with the relevant factor; these are marked bold. This means that the respondent significantly agrees with the ordering of statements in the relevant factor.

Some of the respondents do not load on one of the four factors at all; these respondents have such a deviate ranking of the statements that they do not fit in a factor (respondent 7, 9, 14, 21, 35, and 39). Other respondents load on several factors; in this case, the respondents have a perspective that overlaps with two (confounded) factors (Respondent 2, 3, 8, 13, 25, 27, and 29).

All the results of the Q-method are now statistically analysed. The next step is to interpret the results from the analysis and identify the perspective of the factor.

Table 5 Rotated correlation matrix. Per respondent, the loadings on each of the factors is shown. Significant single loadings are bold.

	Factor I	*Factor II*	*Factor III*	*Factor IV*		*Factor I*	*Factor II*	*Factor III*	*Factor IV*
1	0,3493	0,08892	**0,43682**	0,29815	21	0,24283	0,31423	0,23329	0,09041
2	0,32226	0,46252	0,38074	0,53243	22	**0,65246**	0,24019	0,24978	0,29437
3	0,2141	0,52098	0,20868	0,4781	23	0,34658	0,29486	0,40473	**0,59394**
4	**0,43694**	0,20358	0,08985	0,02837	24	0,01504	**0,41172**	0,36528	0,09011
5	**0,47891**	0,11295	0,36532	-0,04728	25	0,54266	0,48979	0,10324	0,09662
6	**0,70717**	0,02617	0,15532	0,38217	26	0,16294	0,24339	0,32479	**0,58548**
7	0,05806	0,31744	0,19703	0,15112	27	0,05802	0,38746	0,48927	0,44697
8	0,17355	0,50116	0,59297	0,11636	28	0,18451	-0,01292	**0,56601**	0,16835
9	-0,0035	0,15849	0,18266	0,38675	29	0,04829	0,00032	0,50578	0,54591
10	0,4025	0,05871	0,2996	**0,66078**	30	0,06178	**0,63824**	0,01655	0,07346
11	0,05578	**0,80535**	0,15346	0,26741	31	**0,72311**	0,14823	0,34849	0,33463
12	0,37253	0,09682	0,09106	**0,58518**	32	0,01028	**0,46854**	0,17647	0,39551
13	0,49512	-0,04254	0,20128	0,42247	33	0,27084	-0,01452	**0,65289**	0,33133
14	0,3835	0,30009	0,20982	0,12099	34	0,2716	0,26347	**0,56303**	0,18359
15	**0,49122**	0,09227	0,06988	0,0459	35	0,25175	0,05484	0,3441	0,19196
16	0,39769	0,12511	-0,01903	**0,59547**	36	0,30205	0,3978	**0,52741**	0,3896
17	**0,52282**	0,04727	0,13038	0,16218	37	0,08692	0,33704	0,16789	**0,48247**
18	0,20098	0,22136	**0,54572**	0,06413	38	0,24469	**0,42571**	-0,08328	0,15736
19	0,35811	**0,54073**	0,14042	0,3501	39	0,13406	0,39676	0,11875	-0,0545
20	0,06967	0,34193	**0,70901**	0,22467	40	0,39216	0,28154	0,16722	**0,42623**

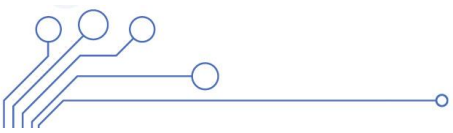
Step 6: Interpretation of results

The loadings from table 5 can be normalized per factor to a so-called Z-score or factor score; these are presented in Appendix J. The Z-scores are translated to the statement scores as ranked by the respondents. The two statements per factor with the highest Z-scores in Appendix J are valued '+5' analogue to forced distribution in figure 17; the lowest Z-scores are then ranked '-5' and so on. The result is presented in table 6. The statements ranked with '+5' or '-5' mean that the group of people does significantly agree or disagree with the relevant statement. By checking all the statements that are significant to a group, the perspective of that group can be interpreted. In this way, it is possible to derive a perspective of a group of managers on cyber security and end user awareness.

Table 6 Scores per statement for each factor

		Factor			
	Statements	I	II	III	IV
1	Our organization is well protected against cyber risks.	-4	0	1	-1
2	IT is very important in our organization.	5	1	4	4
3	My cyber security awareness is high enough.	-3	0	0	-2
4	The end user does hardly know anything about cyber risks and he does not know anything about dealing with the risks.	3	-1	-2	-1
5	Many employees in a big organization implies a high chance on a cyber incident, because not everybody is compliant to the rules.	1	-1	1	-1

6	A risk that has insufficient attention is the risk of unsatisfied employees that have access to sensitive data and systems.	0	-1	2	0
7	An underestimated risk is the risk of new technologies that cause new cyber risks.	1	1	0	2
8	Outdated software is a big risk for cyber security.	0	3	2	5
9	Unavailability of our services due to technical failure or cyber attack has huge consequences.	5	0	4	5
10	Top management underestimates the cyber risks.	2	-1	-3	0
11	Cyber security policies and procedures in our organization are not sufficiently developed.	4	-2	-1	1
12	Cyber security is seen as IT only problem too often. It is also about governance, leadership, culture, awareness and behaviours. Which are often forgotten.	1	5	3	2
13	Unavailability of our services due to external events like flooding, fire or Internet disruption is serious. We need to have a high level of up time.	3	-2	3	4
14	Suppliers and other third parties can be a serious risk for our organisation, due to their own bad/insufficient cyber security.	0	3	2	2
15	Uncoupling several IT systems is a good way to avoid a part of the cyber risks.	0	-2	-2	2
16	It is better to prevent suffering from cyber attacks than to recover from cyber attacks.	2	3	3	4
17	An organization has to avoid risk as much as possible, for example do not save personal data that is not necessary to save.	-1	2	-3	1
18	An organization's cyber security cannot be 100% safe. There is always residual risk, which is acceptable.	4	0	5	1
19	Organizations do not have to protect against risks, which never will be encountered.	-1	-2	-1	-3
20	There is a possibility that cyber risks can be accepted, when the costs of securing are higher than the possible impact.	0	-3	3	-1
21	Nowadays almost every organization is an IT company, which implies every organization has to reduce risk by taking cyber security measures equal to an IT company.	-1	2	-2	3
22	Cyber insurance is useless; the (cyber) damage already had its impact.	-1	-4	-1	-1
23	Cyber insurance is not needed. The premiums are high and the chance on breach in our cyber security low. It is economical not interesting.	-2	-5	-1	-2
24	The role of insurances in cyber security and risk management is unclear to me.	1	-1	0	0
25	Insurers can help organizations with cyber risk management; insurers have a lot of knowledge in the fields they insure.	-1	1	-1	-4
26	IT systems in cyber security should be tested regularly to foster the safety.	3	2	1	3
27	Total cyber security can best be reached through technological means.	-2	-3	-5	-4
28	When technical means are certified, they can be perceived as totally safe.	-4	-4	-5	-5
29	It is sufficient to raise cyber security awareness of employees by informing the employees by newsletter or mail on the topic of cyber risks and how to deal with the risk.	-4	-3	-4	-3
30	Cyber security awareness training has to be mandatory for every employee in an organization.	-2	2	0	-2
31	When employees comply with the policies and procedures regarding cyber security, sufficient mitigation of human errors is reached.	0	-2	-2	0
32	The knowledge to manage all aspects of cyber security should be present in the company itself.	-3	0	0	-3



33	Organizations cannot without integral cyber security approach; cyber security has to be throughout the whole organization.	0	5	4	2
34	For every cyber scenario that is possible, even the unlikely ones, there have to be extensive procedures.	-5	1	-3	-5
35	Some cyber security measures are mandatory by law. That they are mandatory is also the only reason they are taken.	-2	-4	-4	-4
36	Legislation is not necessary to achieve an acceptable level of cyber security.	-2	-3	1	-2
37	It is necessary to define cyber security in contracts with employees and third parties. Contracts that define cyber security measures that have to be taken by the relevant parties.	0	3	0	1
38	Employees have to be stimulated to report each other's' cyber incidents.	2	1	1	1
39	Management support is important to increase the cyber security awareness in an organization.	2	2	5	1
40	Much budget has to be available to improve the cyber security awareness in an organization.	-3	-1	-2	0
41	Cyber security awareness has to be formally integrated in business processes. In this way, no one can ignore security awareness.	1	4	2	0
42	All users of IT systems in an organization have to be cyber security aware for the purpose of cyber security.	2	4	0	3
43	Cyber security is pushed off to the IT department; which is undesirable.	1	0	1	0
44	For good cyber security in an organization a separate department or function needs to be cyber security aware. For example, a cyber security officer or a cyber security department.	-3	0	0	-1
45	In every board of directors or management, team there has to be a security officer, which is cyber security aware. Only then, cyber security is guaranteed.	-5	0	-4	-2
46	For me it is not clear what the use of cyber security awareness is.	-1	-5	-3	-3
47	The human is the weakest link in cyber security; cyber security awareness can be a partial solution for that.	4	1	2	3
48	People in an organization are the biggest risk, which is why everything has to be focussed on increasing cyber security awareness of users.	3	4	-1	0

From the loadings in table 5 can be derived, which of the respondents are divided in which factor. This division is the basis of the percentages of the contextual questions (Appendix B). In Factor I, 7 respondents loaded highest; Factor II, 6 respondents; Factor III, 7 respondents; Factor IV, 7 respondents; and 13 respondents have no or a double loading. For every answer on the questions from Appendix B, a division is presented in Appendix C. In the table, the percentage of respondents is presented. Notable are the percentages in the topic of certification; some organizations have a combination of NEN7510 and ISO 27001, since NEN7510 is a healthcare specific certification. That means that the percentages add up to more than 100%. The tables presented are a guide to interpret the perspectives from the managers.

The scores in table 6 identify significant statements, statements that are important for the relevant factor. In addition, differences among the factors can also identify characteristics. If two factors strongly differ on a statement, it will probably lay bare a different viewpoint. Statement 20 is an example of strong disagreement among the factors. The statements will tell the story through their own content and the opinion of managers about the statement.

In addition, the absolute scores of the factors are summed up per category of the topology in appendix I. The higher the sum, the higher the rankings were in that particular topic. High values indicate a focus

of the managers in the factor on a certain topic. The summations are made according to the typology in Chapter 2 and the categories made in Chapter 4 step 2. For example, factor IV scored 12 points in technical oriented mitigation means (category 3.1); this means the scores of the rankings of statements 26, 27 and 28 add up to 12. The tables in appendix I can help to interpret the perspectives. In the next section, the perspectives of the factors will be explained.

First, four different factors are distinguished by factor extraction and rotation. The next step is to identify the 'perspective of the factor'. In other words, what is the common message of the respondents loading on the same factor?

When there is a reference to a statement, it will be indicated by parenthesis with the statement number; followed by the statements scores of every factor. The factor described is indicated by a bold number. For example, a reference to statement 1 in factor I will be: (1; **-4,** 0, 1, -1).

Factor I – Clear in recognizing risks, inconclusive about measures

The respondents loading high on this factor know their organizational cyber security can be improved. In addition, IT is important for their operations. However, the managers are inconclusive about if and which measures have to be taken.

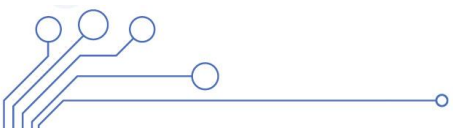
The managers in this factor think of statement 1 to be not true: "organization is well protected against cyber risks" (1; **-4,** 0, 1, -1). In addition, their own cyber security awareness is not perceived as sufficient (3; **-3**, 0, 0, -2). Compared to the other factors, they believe the strongest that "the top of the company underestimates the cyber risks that the organization is facing" (10; **2,** -1, -3, 0). The managers of factor I are the most outspoken about their own situation and do not have a positive view on their cyber security situation.

This negative nature of the situation is reflected in contextual information about the organizations. In appendix C, clearly is visible that organizations of managers in factor I have almost no certifications. Other notable fact about the bad security situation, the absence of dedicated security officers and specialized departments in the current situation of the organizations. As well as the complete absence of cyber security training among the managers in factor I. It is clear that the current cyber security situation is not good, which is equally perceived by the managers.

Moreover, "IT is perceived as very important for the business" (2; **5**, 1, 4, 4) and the "interruption of the IT systems has large consequences" (9; **5**, 0, 4, 5) and (13; **3**, -2, 3, 4). Regarding the cause, the respondents recognize the risk of the human actions (4); they even think that "the human actions are the key factor to all the problems regarding cyber security and awareness is a key factor (47; **4**, 1, 2, 3) to solve this problem", if not the only factor (48; **3**, 4, -1, 0).

However, the importance of IT and the bad security situation are apparently no reason to take measures. It seems the managers are not willing to improve the situation. "A dedicated department is needed" is not preferred by the managers (44; **-3**, 0, 0, -1), neither is "a dedicated person has to participate in the management team" (45; **-5**, 0, -4, -2). This is also reflected in the current situation; the absence of specialized departments and officers (Appendix C) is on purpose.

Besides, the managers do not want to introduce a cyber security training for every employee in the organization (30; **-2**, 2, 0, -2). This is also reflected in the current situation, not a single manager has had a cyber security training. Moreover, to them there is also no preference for "extensive procedures and policies are needed to regulate the cyber security in the organization" (34; **-5**, 1, -3, -5). Extensive procedures and policies will negatively influence the bureaucracy and speed of the business in the



organization; therefore, the measures are not desirable. In general, the interest in risk management and mitigation measures is lowest of all factors (Appendix I).

On the other hand, "employees can foster cyber security awareness by reporting each other's incidents" (38; **2**, 1, 1, 1). This measure does not create any additional costs for the organization; this is important, because manager in this factor do think opposite of "much budget is need for increasing awareness" (40; -**3**, -1, -2, 0); thus, as long as it is cheap.

Summarized, the managers correlating to this factor know the cyber security situation in their organization can be improved. They are even most self-critical of all factors. However, they do not explicitly want to take any measures to improve the cyber security. The managers are inconclusive about measures to increase cyber security, but seem to prefer cheap solutions.

Factor II – Awareness as primary means in a strong avoidance strategy

The managers characterized by factor II are very risk avoidant. Every possible means have to be used to increase the cyber security in the organization. The managers prefer a 100% secure organization. Another aspect characterizing the managers in factor II is the focus on the risk of human actions and awareness as only means to mitigate this particular risk.

The reason for the avoidant nature of the managers is the importance of the data in the organization. "IT is not that important in the organization" (2; 5, **1**, 4, 4), but the safety of the data is. Therefore, the managers perceive "interruption of the services not as enormous problem" (9; 5, **0**, 4, 5). This can be caused by the legislation that can be applied on almost all organizations in this factor (Appendix C). Thus, availability of the data is of less importance than the integrity and confidentiality of the data.

The risk avoidant nature of the managers is also in other ways expressed in the statements. Accepting risk is as good as impossible for the managers (20; 0, **-3**, 3, -1). Everything possibility has to be used in order to mitigate the risk as much as possible. This avoidant character is reflected in many statements.

For example, the managers in factor II are in comparison to other factor the most positive towards many measures. A dedicated person in the management team is not dismissed by the managers in this factor (45; -5, **0**, -4, -2). They have a positive attitude towards extensive scenario description of all cyber security situations (34; -5, **1**, -3, -5). The same holds for the obligation for every employee to attend to cyber security training.

The managers in this factor see the most possibilities for insurance in the organization. Insurance as a means to cover the residual risk and have a 100% secure cyber situation: "insurance is not useful…" (22; -1, **-4,** -1, -1) and "insurances are not needed because our security is good enough" (23; -2, **-5,** -1, -2).

However, all these risks and measures are inferior to the main risk, actions of employees. "The human in the organization causes the biggest risk and everything has to be focussed on the mitigation of this risk by means of awareness" (48; 3, **4**, -1, 0). The concept and necessity of awareness are consequently completely the opposite of 'unclear' for the respondents (46; -1, **-5**, -3, -3). They propose to "let every employee in the organization attend to a cyber security awareness training" (30; -2, **2,** 0, -2). Even legal possibilities are in the range of reasonable measures to decrease the risk of human actions (37; 0, **3**, 0, 1).

Still, awareness is the most important means to reach improved security. The most important prerequisite to raise awareness is by integrating awareness in business processes (41; 1, **4**, 2, 0). Consequently, not "much money has to be invested" (40; -3, **-1**, -2, 0). An important side note for the integration in the organizational processes relates to the awareness; only complying to the security

procedures is not enough, one has to really understand why the measures are taken (31; 0, **-2**, -2, 0). In other words, the employees need to be aware.

Summarized, the respondents in factor II are very much risk avoidant. Interruption of services is not a big problem but integrity and confidentiality are very important aspects to retain. Every possible measure can be taken to reduce the risk as much as possible. However, the focus is on the mitigation of the risk of human actions. This is done by raising awareness through the organization; awareness is perceived as the only option to reduce the risk relating to humans in the organization.

Factor III – Economic considerations as base for cyber security decisions

This group of respondents is characterised by its focus on economics; the influence in their perspective is coming from their corporate working environment. From Appendix C it becomes clear that the major part of the respondents in factor III is from a corporate environment; almost all respondents are from a company with more than 100 employees.

The corporate way of thinking is mainly expressed in the economical way in which risk is approached. Cyber risks can be accepted when it is economical more profitable to do (20; 0, -3, **3**, -1). Risk does not have to be mitigated if it is cheaper to deal with an incident now and then, than to take security measures. Decisions to take cyber security are based on a cost-benefit analysis.

Besides, the "cyber security will never be 100% safe" (18; 4, 0, **5**, 1); however, it is difficult to decide what the border is. An organization can save effort and money when they decide not to implement certain measures, because managers disagree on "organizations should avoid risk as much as possible" (17; -1, 2, **-3**, 1). Without even considering the impact on the processes, because new policies can slow down business processes resulting in indirect loss. This is reflected in a relative aversion against an extensive bureaucracy (34; -5, 1, **-3**, -5).

However, there is a fine balance between taking risk and spending money on security. "It is better to avoid a cyber attack, than to recover" (16; 2, 3, **3**, 4); because recovering from a cyber attack is perceived to be expensive. Related to that, "legislation is not needed to ensure cyber security", but protecting the organization's revenue is the main reason why cyber security measures are taken (36; -2, -3, **1**, -2). Taking irresponsible risk results likely in damage and thus losses. Protecting customer data is also important for the organization, because reputation damage is critical. No legal consumer protection is needed.

Revenue and profit are also the reasons why unavailability of the system has consequences (9; 5, 0, **4**, 5). "IT is very important for the organization" (2; 5, 1, **4**, 4) to maintain the core business. The core business is the way in which money is earned; when the core business cannot be maintained, revenue and profit is lost. Long-term unavailable systems can even cause reputation damage, which can be even more costly.

The economic perspective is also reflected in personnel; in the first place, employees in the organizations are the opposites of risk (48; 3, 4, -1, 0), namely a corporate resource. However, it does not exclude the existence of "human as weakest link in the cyber security chain" (47; 4, 1, **2**, 3). In addition, the managers show they are aware, but not convinced, of other measures, like technical aspects (27; -2, -3, **-5,** -4). However, "the approach should always be an integral approach of multiple aspects" (33; 0, 5, **4**, 2), which characterizes the corporate environment. Just like "managerial influence is important to raise awareness" (39; 2, 2, **5**, 1).

Summarized, the managers in factor III are aware of the cyber risks. Risks exist and the managers simply have to deal with the risks, it is thought. The considerations for managing risks are mainly based on

economic considerations. The consequences for the company are thereby taken into account. The managers push the boundaries of taking risks as long as the cost-benefit analysis is positive. IT availability is important, because the paying customer have to have its service. Money is the key factor in the considerations.

Factor IV – Cyber security is a matter for experts

The respondents in factor IV know IT is important for the organization and thus cyber security as well. However, the managers consider cyber security as a matter for experts, since experts have the knowledge to take measures in such a complex field. Because IT is important for business operations, there is willingness to invest money and effort in the security of IT.

Their opinion about information technology in the organization is very clear; "IT is very important" (2; 5, 1, 4, **4**) and "unavailable system will have disastrous consequences" on the core business (9; 5, 0, 4, **5**). What kind of cause, technical or "external failure", does not really matter (13; 3, -2, 3, **4**). Interrupting the business has crucial consequences, because the core business cannot be continued. According to the respondents, IT is an essential enabler for their organization.

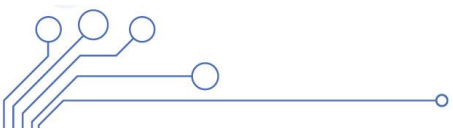
However, the managers perceive as: "my awareness is high enough" (3; -3, 0, 0, **-2**) and prefer experts take care of cyber security. Thus, other relevant people in the organisation have to take care of the problems regarding cyber security. The respondent's focus for cyber security awareness is on the relevant users. Only users of IT systems in the organization have to be aware (42; 2, 4, 0, **3**); integration in processes is not needed, because it also affects irrelevant users (41; 1, 4, 2, **0**). This is emphasized in the statement about training; not everybody in the organization is obligated to attend a cyber security training (30; -2, 2, 0, **-2**).

In addition, there the managers disagree on "all the expertise for cyber security and awareness has to be incorporated" (32; -3, 0, 0, **-3**). The respondents find core business the most important for an organization; cyber security is often not part of the core business. For example, testing the security is a job for external organizations (26; 3, 2, 1, **3**). However, contradicting with (26 and 32), "Insurance companies can provide cyber security advice" is not appreciated (25; -1, 1, -1, **-4**).

One could state that the knowledge of the managers in factor IV is 'common sense'. IT is about technology, thus the respondents focus on technology risks and means; humans control the technology, so they are also a risk factor. This is all reflected in the following: The absolute scores in Appendix C indicate a focus on technology related risks (7; 1, 1, 0, **2**), (8; 0, 3, 2, **5**), and (9; 5, 0, 4, **5**) and technology focussed mitigation means (26; 3, 2, 1, **3**). Although, cyber security is not solved with only technological means (27; -2, -3, -5, **-4**), because human related risks are also a problem (47; 4, 1, 2, **3**).

The managers agree on "because our organization uses IT, our organization needs to take measures similar to an IT organization" (21; -1, 2, -2, **3**). This is also reflected in the statement that prevention is better that recovering from an accident (16; 2, 3, 3, **4**). In the end, cyber security should not be exaggerated, too extensive is not good as well (34; -5, 1, -3, **-5**). Nevertheless, the managers do not consider themselves as right actor to deal with security.

Summarized, the managers in this factor think IT is a pillar for their core business. However, the managers do not consider themselves as designated persons to solve these problems. Experts have to decide about the approach. The managers themselves have a rather 'common sense' approach, they have a focus on technological risks and measures. In addition, human risks exist and measures have to be taken.



Respondents with a different loading

Several reasons exist for a respondent not to load high on a single factor. Either, a respondent can load high on multiple factors, or a respondent does not load high on a single factor at all. The significance threshold is set at .41. If the correlation of the respondent with the factor is not high enough, the respondent will not load high. There are six respondents not loading on a factor at all. The respondents have such a deviating perspective that it cannot be fitted in one of the factors. Possible reasons are an unclear focus in ranking the statements; thus, respondents mixing up personal and organizational perspectives. Another possible reason is the strong deviating organization respondents can act in; for example, a cyber security organization.

However, most of the respondents that have no loading, are *almost* significantly loading on a factor. For example, respondent 39 has a correlation of .396 with factor II, while the significance threshold is .41. The individual perspective does not differ that much from other respondents loading on factor two; however, the respondent is not included. This is because of the earlier explained significance threshold; when the threshold is lower, more multiple loadings emerge.

Six respondents that have a multiple loading, have a significant correlation with two (or more) factors. Which means they have a significant overlap with two perspectives; their view is represented by two factors. There is however, no consistency in combination of factors. The factors having many double loadings differ too much to draw conclusions. The combinations of double loadings can be between factors I and II; factors II and III; factors III and IV and so forth.

Now that the perspectives are derived, the differences and similarities among the perspectives in the field can be distinguished. First similarities among the perspectives will be outlined, followed by the differences. Lastly, the omissions of the perspectives will be explained.

Similarities in perspectives

First, the factors are very similar according to the correlation of perspectives in table 7. This correlation is derived during the factor extraction and analysis. The correlations of the factors are high, which means the factors have a much similarities. The perspectives described previously are focussed on the distinguishing elements of the factors. As stated in table 6, factors I and IV have a high correlation and thus are very similar. The factor that deviates the most from other factors is factor II; the correlation of factor II with the others is the lowest correlation for each of the factors.

Table 7 Correlation among the factors

	Factor I	*Factor II*	*Factor III*	*Factor IV*
Factor I	1,000	0,386	0,627	0,725
Factor II	0,386	1,000	0,483	0,568
Factor III	0,627	0,483	1,000	0,658
Factor IV	0,725	0,568	0,658	1,000

In this section, the similarities are explained. Which contains the perception of cyber security, perception of awareness, the preference for an integral approach and technical matters. The factors have large overlapping aspects; however, the similarities among the factors are not exactly the same. The factors have similarities in a way that they think more or less the same about a topic. Some factors are slightly more positive than other factors are, but in the end they all (dis)agree more or less on the same topic.

The overall attitude towards cyber security and risk is negative. All factors perceive cyber security as an inevitable necessity, which costs money and effort to establish. Cyber risk is cumbersome and organizations need to deal with it as effective as possible. All the managers have a feeling that risk has

to be mitigated. The differences lie in the way to deal with cyber risk, which will be explained in the differences section.

One aspect of the risk approach is more or less for every factor the same. Every manager prefers an integral approach throughout the organization; which also means, the organizational risks are taken into account. This is mainly based on the common perception that cyber security is more than only an IT problem. It also has to do with the integration of awareness into the organizational processes. In addition, the management support is important to raise awareness. Which also holds for the employees, they have to keep an eye on the incidents of each other; which is also denounced as a security culture in the organization.

All the managers have a quite indifferent or slightly positive attitude towards cyber insurance possibilities. Cyber insurance is out of the scope of measures to foster cyber security. Because the concept is not widely known, they may see possibilities, when the concept would gain more popularity. However, insurance companies are preferred not to provide advice for measures. This is only the case for insuring cyber risk.

Another shared value is the importance of IT systems. For every factor holds IT is important (2; 5, 1, 4, 4); the only deviating factor is number II; this factor does rank the statement lower, but the ranking is also non-negative; the shared value of the importance of IT is more or less the same. Which equally holds for the interruption of the availability for IT systems through technical errors (9; 5, 0, 4, 5). Factor II does not perceive external causes as risk for interruption of the systems (13). The importance of IT however, is clear for every factor. In line with the technical issues, all the factors think the same about the so-called 'ISO trap'. The illusion that a certified technical security system is safe (28; 3, -2, 3, 4).

As introduced earlier in literature, technical measures are commonly accepted in cyber security approaches. This also holds for the perspectives from the field. The factors rate the statements about technical measures more or less the same: IT systems need regularly testing (26; 3, 2, 1, 3); cyber security is best reached with only technical measures (27; -2, -3, -5, -4); and a certification is a guarantee for safety in the IT systems (28; -4, -4, -5, -5).

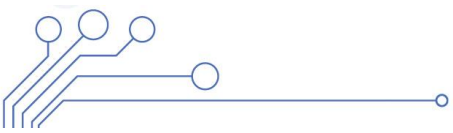
Awareness

A very important topic of similarity among the factors is end user awareness. All factors agree more or less on the importance of awareness. It is in the first place it is more or less clear to all factors what the role of awareness is in an organization (46; -1, -5, -3, -3). The same holds for awareness as partial solution for the human factor in cyber risk (47; 4, 1, 2, 3). Additionally, the differences in the role of awareness as crucial and only solution for human are small (48; 3, 4, -1, 0)

Factor III tends to think that awareness is not the only solution for the human related risks. In addition, the managers in factor III hold the opinion that not everything has to be focussed on increasing awareness (48). It should be a more nuanced decision. However, the overall perception of the role of awareness is the same for each of the factors in the field.

In addition, the factors tend to think the same about the conditions that are needed to increase cyber security awareness. Management support is important for increasing awareness throughout an organization. In contrast, not much budget is needed to reach improved end user awareness. Because, when employees report each other's incidents, awareness is raised at minimal costs. On which all the factors agree.

So, the role of awareness and the means to raise awareness are the same among the factors from the field. There is also consensus about some of the roles that are important for awareness. The factors



are indifferent about the statement of pushing off cyber security tasks to the IT department. Factor I slightly agrees that it is undesirable, factor II slightly disagrees; the differences are small. All factors more or less agree that every IT user in an organization should be aware.

In the end, the factors from the field have many similarities as shown by table 5. Especially factor I and factor IV have a strong correlation. The main topics of similarity are discussed in this section, containing cyber security perception, awareness perception, insurances and the importance of IT in an organization. Although there exist many similarities, differences also exits; which will be explained next.

Differences in perspectives

The perspectives of the factors are of different nature; especially the perception of necessity of cyber security awareness and the arguments for that are different among the factors. The factors are mainly based on their distinguishing characteristics; therefore, the differences in the perspectives in the described factors are pretty clear. Next, an overview of the differences among the perspectives field is given

Although factor I and IV are very similar, they differ on an important point. Factor I is indecisive about the necessity of taking cyber security measures. Factor IV perceives IT of such an importance for the organization that measures will help to protect the business; experts have to deal with it.

Factor II is the most deviating factor regarding the correlation in table 7. The distinguishing elements are a risk avoiding nature of the respondents and the focus on awareness. Especially the avoiding nature results in many statements that indicate a nature of mitigation, as much as possible. Other factors have nuanced perspectives on how to deal with risk; retaining some risk is allowed for different reasons; factor I is indecisive, but tends to think cyber security is costly. Factor III makes a cost-benefit analysis for every measures to decide if it is profitable or not. Factor IV perceives a need for security measures as well; however, factor IV is more focussed on technical related risks instead of human related risks. End users in an organization are a source of risk, but factor I, III and IV do not think it is the only risk. Therefore, there is no need to focus solely on raising awareness. Exactly the opposite of what factor II tries to reach.

The underlying reasons for these perspectives differ as well. Factor II has important information stored in the organization. If these data leak, the organization faces big problems. Therefore, cyber security should be as good as possible and awareness is the key factor to cyber security. For factor I, cyber security can wait, because it is not *that* important. Moreover, it needs investments in effort and money to improve, without immediate return on investment; that certainly can wait. The reason to raise awareness for the other factors is prevention of core business interruption; as long as the supportive departments do their job well, there are no issues. Awareness is especially needed with the relevant people. Money is the argument for Factor III; when the revenues and profits are at stake, investment in cyber security is needed.

Factor IV sees cyber security as a task for the relevant experts in the organization, because they have the knowledge to deal with security. The managers in factor II try to mitigate the risk as much as possible. Respondents in Factor I are not really clear about the cyber security roles, they are indecisive in general. The managers in factor III perceive cyber risk as any other decisions they have to make; express the risk in money if possible and make a cost-benefit analysis. The consideration is pure rational, because profits count.

The differences described above are the main differences among the factors. These differences result in smaller differences like the way risk management is performed. It is self-evident that factor III takes

more risk and therefore likes retaining risk more than factor II. Which is characterized by avoidant behaviour. The small differences can be endless and are beyond this section.

Shortcomings

A few things are notable in the perspectives derived from the field. Factor I has contradicting statement rankings; factor II has some remarkable aspects; the managers regard themselves explicitly not as possessing enough expertise in the field of cyber security. In addition, there is also a note about combinations of perspectives. The topics will be explained point-by-point, since there is not always a clear connection among the issues.

First of all, the first perspective claims their awareness is insufficient, but they remain indecisive about measures to increase cyber security. There is probably no need to increase the security although their security is bad; perhaps there are other more important issues in the organization.

Secondly, the second perspective claims awareness as a solution for all the human relation problems; however, the managers in factor II do not perceive the category of human actions as risks (statement 4, 5 and 6). This is a contradicting way of ranking the statements. The individual statements are covered by the more general statement in statement 48. It can indicate that managers do not recognize specific threats, but know what the general threat is.

In addition, the managers from factor II differ the most from other factors, having the least correlation with other factors. The very interesting thing is they have almost completely ignored the focus on themselves. Which can indicate that the perspectives they are sketching are not their own. The reason is not clear, but it can indicate socially accepted behaviour, by answering the obvious. This factor has many similarities with perspective I from literature; this will be discussed later.

The managers from factor II and III take responsibility for cyber security; In contrast to the managers from factor IV; who are shifting the responsibilities to others, because it seems that they do not have the required knowledge. The same can be stated about the managers in factor I. It is irresponsible to leave cyber security as it is, when they know what the consequences are. However, if they have limited knowledge they should throw experts into gear. Fact is that they perceive their situation as insufficient, but lack in actions.

Factor III is presented as a rational factor that makes only decisions based on a cost-benefit analysis. However, for many cyber security topics it is hard to value the intangible goods and damage. Therefore, the consideration is not completely rational, since there are many unknowns. It is unclear how the intangible matter is expressed in a cost-benefit analysis.

Another issue: in general, there are seven respondents with a double loading, which means a blend of perspectives is possible as well. In terms of perspectives, it possibly means a manager believes awareness is the most important aspect in cyber security and, simultaneously, experts should take care of it. This is an example of a combination of factor II and factor IV. Respondent 10 in table 5 loads high on factor II and III, however the characterization of both factors seem to exclude each other. It is almost impossible to define which aspects of both factors are correlating to this respondent.

An overview of all the topics discussed in the chapter is displayed in table 8. Per level and aspect of the typology, the focus of the perspectives is presented. Per topic in the typology, the perspectives are divided based on their focus on the topic. If the perspective has a focus on a topic, the name of the perspective is presented under the relevant topic. It is like table 3 in the previous chapter.

Table 8 overview of the focus of perspectives from the field regarding topics in the cyber security typology

Level 1	Actions of people	Systems and technology failure	Failed internal processes	External events
	Perspective I, II, III	All perspectives	All perspectives	None
Level 2	Avoidance	Retention	Mitigation	Transference
	Perspective II	Perspective I, III	All perspectives	Perspective II
Level 3	Technical oriented means	Human oriented means	Organizational oriented means	Legal oriented means
	All perspectives	More or less all perspectives	All perspectives	Perspective II
Level 4	Conditions	Roles	Importance	
	Perspective III	Perspective IV	Perspective II	

Now that the perspectives from literature and the field are found, a comparison can be made. The next chapters will dive into the differences and similarities of the perspectives from the field and from literature. The perspectives will be further discussed in chapters 5 and 6.

Chapter 5: Comparison of perspectives

This chapter investigates the differences and similarities of the perspectives derived from literature and the perspectives taken from the field. The perspectives from literature are according to Herley (2009), derived in Chapter 3 through a literature review. The perspectives from the field are derived in Chapter 4, by means of the Q-method. The comparison of the perspectives from literature (perspectives) and the field (factors) will be compared in order to answer research question three. The perspectives of the factors will be identified by 'field perspective' (FP) instead of perspective and perspectives from literature by 'literature perspective' (LP), to avoid confusion.

The perspectives from the field and from literature are first compared separately; this already has been done in previous chapters. The comparison is based on the elements from the typology laid out in chapter 2; this is clearly visible in table 3 and 8, in which the different elements are divided per perspective. For the comparison in this chapter, the similarities and differences will also be based on the elements of the typology.

First similar perspectives will be outlined, followed by the differencing perspectives. Thereafter, the general similarities and differences will be explained. Last, awareness is outlined in a separate section.

Similar perspectives

Two sets of perspectives show corresponding aspects. LP I and FP II, have many similar ideas and LP III and FP III show equalities as well. Both of the matching perspectives will be briefly outlined on their equalities. Naturally, the perspectives are not perfectly equal; the differences are covered by the 'general differences and similarities' section.

The first clear similarity between the perspectives from the field and from literature is regarding LP I and FP II. Both perspectives focus on mitigation as strategy of cyber security. Moreover, both strongly aim for reducing risk related to the human factor through end user awareness. After all, the human is the weakest link in the security chain according to these perspectives. The main equality between these perspectives lies in the role of awareness, the most important factor in mitigation is cyber security awareness.

How to improve the end user cyber security awareness is however open for both perspectives. The ways to raise awareness are clearly stated in the perspective from the field. Raising awareness requires management support, but not much budget is needed. The perspective from literature is not clear about which means are the best to raise awareness; just some suggestions like training and education are suggested.

The second similar set of perspectives is composed of the third perspective from literature and the third perspective from the field. Both regard economic considerations as ideal way to decide whether a measure should be taken or not. The decisions about cyber security are just like any other aspect in the business; if the cost-benefit analysis is profitable, measures can be taken.

However, not everything is the same in these perspectives. The focus of the perspectives from the field have a broader focus. The cost-benefit analysis holds for the company, not for an individual end user. LP III focusses on measures taken for every individual end user in an organization; the concept of cost-benefit analysis is the same.

Concluding, two perspectives in the field and from literature correspond with each other. On the one hand, awareness is a big deal in mitigation means; on the other hand, economic considerations provide a base for decisions in cyber security.

Different perspectives

Three different perspectives from both fields remain. Perspective from literature number two and the field perspectives one and four. The reasons why these perspectives differ will be explained next. These differences are specific for the perspectives; general differences and similarities are outlined in the next section.

A real deviating perspective in literature is that of perspective II. This perspective focusses mainly on usability of technology as solution to the problems in cyber security. This is not reflected in any of the perspectives from the field. In the first place, it is caused in the construction of the concourse; in this step, it already became clear that none of the sources consulted was convinced of the second perspective from literature. Even in literature, researchers notice that in a long time not much progress is made in the field of usability. Parkin et al (2010), mention that in the best case 'single sign-on' is implemented, but that end users are still often forced to generate complex passwords. Practice did not adopt the perspectives of usable security software at all; this is thus reflected in the perspectives from the field.

Two perspectives from the field also differ in nature of the perspective. The first perspective from the field is deviating from the rest of the perspectives, because the managers are indecisive to take measures or not. They claim they are not aware, but they know that their cyber security situation is bad. It seems the managers find cyber security cumbersome and expensive. Therefore, no measures are taken.

The other perspective from the field is perspective IV. The managers in FP IV, are willing to take measures on cyber security. Measures may cost effort and money, because important IT resources for the organization are protected in this way. However, the managers do not consider themselves as experts in the field of cyber security; therefore, they prefer real experts to decide on measures that have to be taken.

Both perspectives related in a certain extent to expertise of the relevant people. Doing nothing to increase cyber security is not a very usual topic in the scientific landscape. When scientific literature addresses cyber security, it is usually to identify a problem and a relevant solution. The nature of scientific literature and practice conflict; therefore the first perspective from the field has no matching perspective in literature.

For the fourth perspective from the field, an equal reasoning holds. Managers consider themselves as lacking knowledge; this is not recognized in literature. Most of the papers used in this thesis are specified on cyber security and are written by an expert in that particular field. This means that a lack of knowledge is excluded in the scientific field; however, for managers in practice this does not hold. In the case of FP IV, the nature of practice and scientific literature conflict as well. Therefore, FP IV is not a reflection from literature and is thus different.

Both perspectives from the field outlined previously have different aspects that can be traced back to a perspective from literature. This will be explained in the next section about the general similarities and differences.

General similarities and differences

There are general differences and similarities between the perspectives in the field and the perspectives from literature. The number of similarities is limited and will be explained first.

Similarities

The main similarities are in the first two levels of the typology; the risks relating to humans and technology are perceived by all perspectives, more or less, the same. Both categories are imposing risks in a cyber environment. Mitigation is a risk management strategy supported by all perspectives, except FP I.

FP II is the only perspective from the field seeing technical issues to a lesser extent as a risk. LP I considers technical risks as a risk as well, the same holds for LP III. The second perspective from literature sees technical risks as the most dangerous risks. The lack of usability of technology causes important risks. The other perspectives believe technical risks form the base level of the risks in cyber security.

Both, perspectives from literature and the perspectives from the field see the risks related to technology. LP II is a deviating perspective, which considers technical related risks as most important risk. As stated before, technical measures towards cyber security are commonly accepted in literature; all perspectives (also from the field) more or less think the same about the usage of technology in the mitigation of cyber security. It seems that literature and the field agree on the use of technology in cyber security.

The risks related to human actions are also in the scope of all the perspectives. Most of the perspectives consider humans as a risk, but not as a crucial risk. Two perspectives deviate from that perspective. FP II consider human action as the key risk in an organization. The human is the weakest link. On the other hand, LP II believes end users can be held responsible for any of the issues in cyber security.

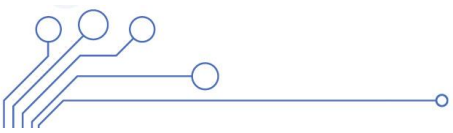
There is no clear difference between the perspectives in literature and from the field. LP I and FP II are even matching perspectives regarding human risks. Strongly deviating to all other perspectives is LP II, which recognizes almost no human risks. The remaining perspectives see humans as one of the risks.

LP I and II as well as FP II and IV all focus on mitigation of cyber risk. Even stronger, it is their focus in cyber security to mitigate the existing risk as much as possible. FP I, III, and LP III are not that sure about mitigation. It is only useful to a certain extent, they claim, namely when it is protecting -not bothering- the core business. FP I tends to see cyber security as unnecessary costs for their organization; the need is limited. Some of the perspectives on both sides prefer maximum mitigation; others have reasons to mitigate cyber risks only to a certain extent.

The perspectives from literature and the field have the same characteristics on risks regarding technology and humans. As well as the common preference of risk mitigation. However, not everything is the same, now the differences will be discussed.

Differences

For the overview, the general topics of differences are explained per separate topic. First, the lacking aspects for the perspectives are explained, followed by the difference in knowledge. Thereafter, the topic of awareness will be treated. Last, the overlap of the perspectives from the field is discussed.



Lacking aspects in the typology

Some of the elements of the typology are not recognized in literature and not in the field as well. Perspectives from literature lack the elements of organizational matters, external risks, avoiding and transference management strategies, and legislation. Perspectives from practice mainly ignore the aspect of theoretical definition.

The perspective derived from Literature lacks in several ways. First of all, the literature perspectives ignore the organizational aspects. As showed in the absolute scores (appendix I), the perspectives from the field notices cyber security is not only about IT, but also about organizational matters. This is also reflected in the approaches to mitigate risk; organizational measures are included.

LP I and II do not have an outspoken view on the use of organizational means to increase cyber security. However, LP I believes some organizational oriented means can help to raise awareness and thus indirectly increase cyber security. For LP II organizational means can be used to develop usable security software. LP III sees organizational measures as a method to reduce risk. Concluding, there is a clear difference between the perspectives in literature and from the field.

The same arguments hold for the external risks regarding cyber security. In literature, these risks have not any relevance regarding the topic of cyber security. A flooding hitting a datacentre (or anything else) is clearly another field of scientific research. However, it is a risk, which also strikes IT resources. Literature research lacks any relevant information regarding external risks and measures. Perspectives from the field have marginalized the external risks; the risks are not considered as important risks. One could argue that the results reflect the decision of science not to include external risks in cyber security.

Legislation and transference are other aspects of the typology that are completely ignored by literature; it is perceived as out of the field. For the perspectives from the field holds, legislation is necessary to create an appropriate level of cyber security in an organization. Transference, on the other hand, is an option to mitigate the residual risk. Literature excludes legislation and transference; perspectives from the field include security measures by legislation and transference.

In addition, an aspect that lacks at the side of the field perspectives. The perspectives from the field do not have anything to state about the theoretical definition of cyber security awareness, because in Chapter 4 step 2 is explained this is perceived as irrelevant by the managers. Literature perspectives do not explicitly state anything as well; except for LP I, this perspective indicates awareness is knowledge about the risks and the means to deal with the risk.

Because of the lacking aspects, the perspectives from the field and from literature do not fit neatly on each other. Therefore, a complete comparison can hardly be made. This is however an important issue of improvement for the perspectives from literature; not all relevant aspects are taken into account in the literature perspectives.

Knowledge

The second important difference between the perspectives from the field and from literature has to do with the knowledge of the managers and researchers. The researchers are expected to be experts in their field of research and thus having knowledge of the aspects of cyber security. For managers it is different, managers need to know much of many things –they are generalists-; therefore, managers are usually not specialized in a particular field. Hence, a manager can lack knowledge in the field of cyber security.

The perspectives in the field cope with managers without specialized knowledge. This is traced back to the perspective I and IV from the field. Both have a different approach; but for both, limited

understanding of the topic influences the perspective. The literature perspectives are constructed by experts, which have knowledge about the cyber security field.

In addition, the managers act in an organizational context, which has consequences for the perspective. For example, the manager is forced to consider relevant legislation when deciding on cyber security. A researcher investigating a theoretical concept for cyber security is not bounded to legislation.

Awareness

A difference is also noticed regarding the role of awareness for cyber security among the perspectives. From the perspectives in Chapters 3 and 4, the importance for awareness easily can be derived. FP II and LP I are convinced of the crucial importance of awareness. Awareness is the key factor to an increased cyber security, because the human is the weakest link. Awareness will enhance the knowledge and reduce the risk regarding the weakest link. Awareness is also important for FP I and IV, but to a lesser extent; it is one of the means to mitigate risk.

A basic level of awareness is required by FP III and LP III. The importance of cyber security and the necessity of awareness are of a certain level; there is a balance between the measures (and thus awareness) required and the money spent on cyber security.

LP II believes awareness is incorrectly identified as the problem in cyber security; not awareness but the lack of usability in software solution is the problem. There seems to be no role for awareness in LP II, however LP II is not outspoken about the role of awareness.

In all perspectives from the field, awareness plays a more or less important role. This is a difference with the perspectives from literature, only LP I has a clear (very) important role for awareness.

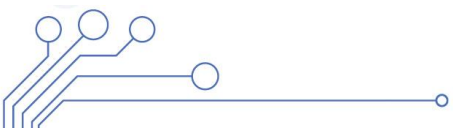
Except for the importance of awareness, also the context and roles regarding cyber security awareness are causing differences. The first perspective from literature is clear that the end user has to be aware; no other roles are mentioned. Some conditions and means to raise awareness are named in LP I, like training, education, budget and security culture. LP II and III are not conclusive about the roles and conditions regarding awareness.

On the other hand, all perspectives from the field perceive management support as important; the FPs also find money not the primary means to raise awareness. Relevant employees are in case of FP II all employees and in case of FP IV only IT personnel. Factor III is not that important; if awareness is integrated in the organizational policies and procedures, every employee is aware. In general, all IT users are important for awareness according to the managers of all perspectives.

Overlap of the perspectives

Last notable difference between the perspective from the field and from literature is the overlap of the perspectives. The managerial perspectives have much overlap as is also stated in table 5. However, the perspectives in literature are much more diverse.

The perspectives in literature seem to be a reply on each other; LP II replies on LP I; the arguing is like, LP I is not correct, there is no reason to assume the human is the weakest link, the usability is the problem. The same holds for LP III in reply on the first two perspectives from literature. LP III says it is neither the awareness nor the usability; rather, the economic aspect needs to be central in decision-making. In the field, the perspectives are all gained at the same time. This is without any reaction on each other's perspective.



There is another reason why the perspective from practice can have much overlap. A large part of the overlap can be traced to the opinions about awareness. The perspectives from the field have more or less the same perspectives on awareness in cyber security. The only differences are the extreme interpretations like FP II and the nuanced interpretation of FP III.

An explanation for the similarities in perspectives regarding cyber security awareness can be found in the paper by Florencio et al (2014). The authors express their concerns regarding FUD. FUD is the Fear, Uncertainty and Doubt for cyber risks caused by falsehoods regarding impact and frequency of cyber incidents. The falsehoods are according to Florencio based on exaggerated costs of cyber incidents and exaggerated frequencies of incidents.

These falsehoods cause an unrealistic perspective on the real issues. However, Florencio et al (2014) argue that FUD is the dominant paradigm in literature. In addition, FUD has its effect on people in the field of cyber security. It is possible that the managers are mainly influenced by the perspective sketched by Florencio et al. This perspective can be identified as LP I in this thesis. Thus, it is wrongfully argued that awareness plays a large role in cyber security. However, it is the main perspective in literature and thus it influences the managers.

Chapter 6: Conclusions and discussion

This thesis addressed the perspectives regarding cyber security and end user awareness. Now that all the research has been demonstrated, it is time to formulate an answer to the research questions; as well as to discuss the results and check whether the research can be improved.

Conclusion

In this thesis, the perspectives of science and managers are investigated. There is a need for the perspectives from the field, for there is, so far, no knowledge of perspectives in practice available. Besides, literature mostly agrees on technical aspects, and focusses in its discussion on human factors. The role of awareness appeared to be important in this thesis. Hence, the perspectives on cyber security and the role of awareness therein are investigated. The managerial perspectives are investigated through the Q-method; perspectives from science are derived through literature study. To guide the comparison of the perspectives, a typology is laid out in this thesis; this typology contains the dimensions of cyber security identified in literature.

As main research question, the following sentence was formulated in order to investigate the perspectives:

What are the managerial and scientific perspectives regarding (organizational) cyber security and end user cyber security awareness?

Main research question is answered in three smaller research questions.

1. *What are the perspectives regarding cyber security and the role of end user awareness in scientific literature?*

Scientific literature delivered three different perspectives regarding cyber security and the role of end user awareness. The different perspectives will be briefly explained; the full explanation is stated in Chapter 2.

Perspective I – The human is the weakest link

This perspective focusses on the incompetence of the end users. The end users of IT systems are lazy or do not have the required knowledge; therefore, the end users make mistakes and appear to be the weakest link in the security chain. Improving their cyber security awareness will increase their knowledge and skills regarding cyber security. In short, the users are the single weakest link, which can be resolved by improving their awareness.

Perspective II – Usability of security

In contrast to the first perspective, this perspective believes the end user is not to blame. The main issue in cyber security is the usability of security systems. The systems are too complex to use and therefore users make mistakes. Improving end user awareness will not mitigate the problem. Instead, security software development with the user as basis is the solution, which is called user-centered security software.

Perspective III – Economic perspective

The third perspective aims to a lesser extent on mitigation of cyber risk. Because this perspective believes the 'facts' about impact costs for an organization are exaggerated. Even the advantages of the security measures are undue. Too many security measures can harm, instead of help, organizations. Decisions about security measures should be based on a *true* cost-benefit consideration. This is until

now not the case. Which will lead to far less security measures than currently is the case. In addition, end users make decisions about complying with security measures based on their effort. When measures are effort-neutral, complying is no issue for the end user. However, current measures cost the end user too much effort.

2. *What are the perspectives of managers regarding cyber security and the role of end user awareness in practice?*

Four perspectives are found by means of the Q-method in Chapter 4. The perspectives describe four different kinds to consider cyber security and end user awareness. The four perspectives will be summed up very briefly. A full explanation can be found in Chapter 4 step 6.

Perspective I – Clear in recognizing risks, inconclusive about measures.

Managers correlating to this factor are aware that the cyber security situation in their organization can be improved. They are even most self-critical of all factors. However, they are inconclusive if and which measures they want to take to improve the cyber security. Cyber security seems to be of low priority.

Perspective II – Awareness as primary means in a strong avoidance strategy

Respondents in factor II are very risk avoidant. Interruption of services is not a big problem but integrity and confidentiality are very important aspects to retain. Every possible measure can be taken to reduce the risk as much as possible. However, the focus is on the mitigation of the risk of human actions. This is done by raising awareness through the organization; awareness is perceived as the only option to reduce the risk relating to humans in the organization.

Perspective III – Economic considerations as base for cyber security decisions

Summarized, the managers in factor III are aware of the cyber risks. Risks exist and the managers simply have to deal with these risks. The considerations for managing risks are mainly based on economic grounds. The consequences for the company are thereby taken into account. The managers push the boundaries of taking risks as long as the cost-benefit analysis is positive. IT availability is important, because the paying customers have to have its service. Money is thus the key factor in the considerations.

Perspective IV – Cyber security is a matter for experts

Summarized, the managers in this factor think IT is a pillar for their core business. To improve security, measures have to be taken. However, the managers do not consider themselves as designated persons to solve these problems. Experts have to take over the work; they have the knowledge for the complex matter of cyber security. Alternatively, in case of a knowledge gap external experts can be used.

3. *What are the differences and similarities between the preceding perspectives in literature and practice?*

The perspectives from the field and from literature are derived in the preceding research questions. A comparison is made based on the aspects of the framework from Chapter 2. First, the differences and similarities for the particular perspectives will be explained, followed by the general similarities and differences.

The first perspective from literature and the second perspective from the field are very similar. Both believe in end user awareness as primary solution for the weakest link in cyber security. The perspective from the field adds an avoiding attitude regarding cyber risk. Both perspectives are

deterred by the cyber risks; therefore, everything has to be focussed on improving awareness and thus mitigating risk.

Perspective III from the field and perspective III from practice have many similarities. They base their considerations for cyber security both on economic reasons. When it is cheaper to take risk, take risk; and vice versa. The main concept of both perspectives is thus the same, they have however a difference. LP III claims that current knowledge of cyber security is based on falsehoods; FP III does not mention this at all. Their focus is from a corporate perspective and thus organization-oriented.

The second perspective from literature is not recognized in the perspectives from the field. LP II differs too much regarding the role of awareness and focusses too much on usability of technology. However, merely technological measures are perceived impossible in the field, even when the measures are usable. Therefore, human oriented means in form of awareness play a role in every perspective from the field. The role of end users cannot be avoided in practice.

Which leaves two perspectives from the field as remainder. FP I and IV are both in between the other perspectives. These perspectives are not recognized in literature, because the perspectives do not completely focus on cyber security and the managers perceive they have a limited understanding of awareness. The organizational part in these perspectives are important, but are excluded by the perspectives from literature. Therefore, these perspectives do deviate on their core concept from the perspectives in literature.

The general similarities between the factors in the field and in literature are the focus on the risks of human- and technical problems. The main strategy in all perspectives is the mitigation of risk; technical mitigation means are in all perspectives used as basis for cyber security.

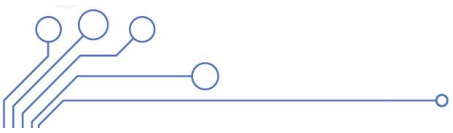
General differences between the field perspectives and literature perspectives are lacking aspects in the typology, the level of knowledge, awareness and the overlap of the perspectives. The differences are briefly outlined.

A few aspects of the typology are lacking in the perspectives in literature; legislation, transference, external risks and organizational oriented risks are missing. These are perceived to be out of the field, while the aspects are relevant proved in the typology. The same holds for the theoretical meaning of cyber security and awareness by managers; they do not perceive the theoretical issues as relevant for their security situation.

Literature perspectives are written by experts, whereas field perspectives are not; this causes differences in perspectives. FP I and FP IV, clearly state they have a lack of expertise regarding cyber security. Therefore, the perspectives are not a reflection of literature.

The perspectives in literature do not overlap because the perspectives are a reply on each other. LP II is a reaction on LP I and LP III criticizes both other perspectives. This is not the case for the field perspectives. Besides, the perspectives in the field, all seem to be influenced by the dominant paradigm in literature (LP I), which focusses on awareness.

The role of awareness is recognized by any of the perspectives in the field. LP I and FP II attach great importance to the role of awareness is cyber security; it is even perceived as the only way to increase cyber security. FP I, III and IV recognize the importance of awareness in an approach to increase cyber security, just like any other means. LP II and III are inconclusive about the role of awareness.



With all the research questions answered, the main research question is also answered. The scientific and managerial perspectives regarding cyber security are stated; even as the role of end user awareness in cyber security.

Discussion

In this section, the relevance of the results of this thesis will be discussed. First of all, compared to perspectives from literature the results from the field show additional value. This value lies mainly in the typology and human factors section. Because, as mentioned before, in literature there is not much of a discussion about technical issues and measures regarding cyber security. Technical measures are seen as a first step in cyber security; this is also recognized in practice.

Therefore, the discussion in literature is mainly about human factors. That is why the perspectives from literature mainly focus on human risks and human oriented means. Three different perspectives have been found in literature; the perspective with most scholarly literature is about awareness as solution of human risks. In front, it was expected that awareness is also important in the perspectives in the field. It turned out that this expectation is true. Awareness is also believed to be important in cyber security among all perspectives of managers. The reason why it is dominant in the field is not known; it can be that managers only are aware of the dominant perspective in literature.

Both other perspectives are marginal in literature; this can imply the marginality of the perspectives in practice as well. However, the economic (third literature) perspective is recognized in practice (third field perspective). However, causality is hard to uncover from the results in this thesis.

Next to awareness, the typology of cyber security contains many more elements. Practice includes more elements of the typology in the perspectives than literature does. However, literature perspectives are therefore introduced in this paper as generalizations. The perspectives are more nuanced than the literature perspectives. This is shown in the perspectives, but also in respondents that have correlation with multiple perspectives. It is not mutually exclusive, but there are multiple possibilities.

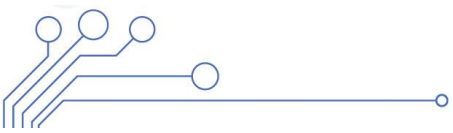
Although the literature perspectives are generalized, some elements of the typology are missing in the perspectives. External risks, legislation options, insurance strategies and organizational issues are mainly ignored by literature. Field perspectives perceived these elements as valuable in their approach. Therefore, the field perspectives can be an enrichment for perspectives from literature; science should investigate to what extent it is possible to develop a perspective based on all elements of the typology.

In line with the last issue: the typology laid out in this thesis, can be a tool for reflection by literature perspectives. Many aspects are elements are included in the typology; decision makers can use the typology to reflect the elements of their own perspectives.

In the end, the perspectives found in the field were unknown preceding this research not known. The knowledge about managerial perspectives regarding cyber security was non-existent; the results of this thesis are a first step in knowledge about the cyber security perspectives of managers in the field. As responsible actor for cyber security in an organization, they have a large role in decision-making about security. With the perspectives from the field, insight in managerial perspectives is gained.

Limitations

The first issue is in the comparison of perspectives. The literature perspectives are generalized perspectives derived from one source; which are consequently verified in literature. Herley (2009) is the source and he provides the views; however, it is possible literature is considered in a tunnel vision



by the author. When investigating literature the perspectives of Herley are leading; consequently, there is no blank view anymore.

In addition, the perspectives from literature are written and developed by experts from all over the world. This stands in contrast to the managers from the field. They are from all kinds of levels of understanding of cyber security and only from the Netherlands. The context of the two different sources is different, which makes the comparison not entirely flawless.

In the set of statements, relatively many statements are about awareness; indirectly this can cause a focus on awareness as mitigation means. If the topic of awareness was treated as the other mitigation means, would the results be different? In the current results, the focus is on awareness. This can either be caused by a focus on awareness in the set of statements, or because the respondent find awareness important. This said, it is hard to determine if there is a link between these two issues. Nevertheless, the possibility should be taken into account.

The typology of cyber security includes many aspects. Because of the many aspects, the Q-set of statements covers a wide range of topics. The Q-sort may have been more focussed if some topics were dropped. In line with the preceding statements about awareness, perhaps fewer statements about awareness should be included in the Q-set.

Because cyber security and cyber risk are delicate topics in organizations, respondents could have based their Q-sort on an 'ideal' perspective. Ranking the statements to a socially accepted result based on unreal assumptions. Maybe the respondents in factor II slightly adjusted their rankings to socially accepted behaviour. The results seem a little unrealistic and one-dimensional. However, socially accepted behaviour is not made explicit and therefore respondents have to be trusted in their honesty.

Recommendations

The results in the conclusion and the discussion sections are reason for the recommendations in this section. The recommendations consists of dialogue among researchers and professionals from the field; a pledge for pluralism; and a call for improving the accuracy for impact and frequency estimation.

As stated in the result section many differences exist between the perspectives in literature and the perspectives from the field. Many aspects of the typology developed in this thesis are considered as irrelevant by perspectives from literature. The lack of these aspects is a lead for improvement of the perspectives in literature; especially on the topics of organizational and external risk, transference and legislation.

Vice versa, perspectives in the field ignore the perspective regarding the usability of security in literature. This is considered by managers as irrelevant, or at least not the solution for cyber security. For both preceding topics hold, the missing topics can have additional value for the lacking perspectives. A dialogue between researchers and experts from the field can help to foster interaction and add nuances in the perspectives. At the same time, the gaps in the perspectives can be noted by the dialogue among the domains. The dialogue can be based on the aspects of the typology from Chapter 2, since this typology provides a context for all aspects of cyber security; including the gaps.

Moreover, the perspectives from the field are all based on the perception that awareness is important for cyber security. However, this assumption is quite linear and according to Herley (2009) and Florencio et al (2014) based on falsehoods. It is worrying that all perspectives in the field are influenced by the literature perspective aiming for awareness. This implies little diversity in perspective; which is confirmed by the correlation numbers in table 5. Science also shows the drawbacks of the perspective focussing on awareness. Therefore, it is recommendable to foster diversity in the set of perspectives

of managers in the field. A focus on only awareness is too specific and as seen in the typology cyber security consists of many more factors. Pluralism in perspectives can cause a more nuanced and thus more realistic perspective of cyber security. Fostering pluralism is therefore very important.

In line with the preceding recommendations, the basis of a more nuanced perspective regarding cyber security is an alternative for FUD knowledge. The statistics are now exaggerated according to Florencio et al (2014). Therefore, alternative methods to estimate incident impact and incident frequency realistically have to be used or developed.

The recommendations are based on the important lacks in the perspectives. First, the literature perspectives ignore topics included in the typology of cyber security; as well as field perspectives lack aspects. Secondly, perspectives from the field are mainly influenced by literature perspective I; to change, pluralism in perspectives have to be established. An alternative method to estimate impact and frequency of incidents can be the first step to improve the general perspective.

Further research

For some issues this thesis has no explanation, therefore, further research is needed. For example, it is unknown if the current perspectives from the field are actually based on FUD as it is suggested by Florencio et al (2014). It is unknown on what the shared perspective of awareness in the field is based on. Further research can investigate the origin of the perception of awareness by managers in the field. It can provide more insight in the question whether the perspectives from the field are based on FUD or not; if not, what else could cause the focus on awareness.

The third perspective from literature is mainly based on the perception FUD is harmful (Florencio et al, 2014). However, the existence of methods to 'properly' measure impact and frequency of cyber incidents is limited. Investigations for reliable measurement methods are needed.

Research could be conducted based on the typology of cyber security developed in this research. For example, to what extent it is possible to develop a perspective on cyber security including every aspect of the cyber security typology. In the end, some aspects lack in the perspectives, so there are leads to improve the perspectives from literature.

In this section, several recommendations for further research are proposed. A wider context for this thesis is possible, as well as investigations specifying on the overlap in perspectives from the field. In addition, the typology can be used to improve the perspectives in literature.

Bibliography

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *45*(12), 40–46.

Akhtar-Danesh, N., Baumann, A., & Cordingley, L. (2008). Q-Methodology in Nursing Research. *Western Journal of Nursing Research*, *30*(6), 759–773.

Anderson, R., & Moore, T. (2007). Information Security Economics - and Beyond. In A. Menezes (Ed.), *Advances in cryptology* (pp. 68–91). doi:10.1007/978-3-540-74143-5

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget. In *Proceedings of the 2008 workshop on New security paradigms - NSPW '08* (p. 47). doi:10.1145/1595676.1595684

Becker, G. S., & Ehrlich, I. (2015). Market Insurance , Self-insurance , and Self Protection. *Journal of Political Economy*, *80*(4), 623–648.

Besterfield, D. (2009). Documentation of Quality Management System. Retrieved October 28, 2015, from https://totalqualitymanagement.wordpress.com/2009/02/27/documentation-of-quality-management-system/

Boundless Business. (2015). Management Levels: A Hierarchical View. Retrieved October 29, 2015, from https://www.boundless.com/business/textbooks/boundless-business-textbook/management-8/types-of-management-61/management-levels-a-hierarchical-view-293-7468/

Bray, T. J. (2002). Security Actions During Reduction in Workforce Efforts: What to do When Downsizing. *Information Systems Management*, *19*(3), 1–5. doi:10.1201/1078/43201.19.3.20020601/37174.11

Braz, C., & Robert, J. (2006). Security and usability. In *Proceedings of the 18th international conference on Association Francophone d'Interaction Homme-Machine - IHM '06* (pp. 199–203). doi:10.1145/1132736.1132768

Brown, S. . (1993). A primer on Q methodology. Operant Subjectivity. *Operant Sub/ectIvlty, 16*(1), 91–138.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2011). Information Security Policy Compliance: an Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548. doi:10.1093/bja/aeq366

Casmir, R. (2005). *A Dynamic and Adaptive Information Security Awareness (DAISA) Approach*. Stockholm University/Royal Institute of Technology.

Cebula, J., Young, L., & Popeck, M. (2010). *A Taxonomy of Operational Cyber Security Risks*. *Advances in Information Security*. Pittsburgh. doi:10.1007/978-1-4419-7133-3

Chaplin, M., & Creasey, J. (2011). *The 2011 Standard of Good Practice for Information Security*. Retrieved from https://www.uninett.no/webfm_send/730

Cherdantseva, Y., & Hilton, J. (2013). A Reference Model of Information Assurance & Security. *2013 International Conference on Availability, Reliability and Security*, 546–555. doi:10.1109/ARES.2013.72

Choi, N., Kim, D., & Goo, J. (2006). Managerial Information Security Awareness' Impact on an Organization' s Information Security Performance. In *Americas Conference on Information Systems (AMCIS)* (p. Paper 406). Acapulco, Mexico.

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing. *Information Management & Computer Security*, *16*(5), 484–501. doi:http://dx.doi.org/10.1108/09685220810920558

Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. doi:10.1016/j.istr.2010.04.004

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. doi:10.1287/isre.1070.0160

Dinev, T., & Hu, Q. (2007). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386–406.

Dominguez, C. M. F., Ramaswamy, M., Martinez, E. M., & Cleal, M. G. (2010). A framework for information security awareness programs. *Issues in Information Systems*, *11*(1), 402–409.

Dryzek, J. S., & Berejikian, J. (1993). Reconstructive Democratic Theory. *The American Political Science Review*, *87*(1), 48–60. doi:10.2307/2938955

Exel, J. Van, & de Graaf, G. (2005). Q methodology : A sneak preview. *Social Sciences*. Retrieved from www.jobvanexel.nl

Faily, S., & Fl??chais, I. (2011). User-centered information security policy development in a post-Stuxnet world. In *Proceedings of the 2011 6th International Conference on Availability, Reliability and Security, ARES 2011* (pp. 716–721). doi:10.1109/ARES.2011.111

Görling, S. (2006). the Myth of User Education Görling the Myth of User Education. In *Virus Bulletin Conference* (pp. 1–4).

Greisiger, M. (2010). Cyber risks how to protect your business in the digital age. *Crain Communications*. Retrieved from http://www.businessinsurance.com/whitepapers

Gutmann, P., & Grigg, I. (2005). Security usability. *IEEE Security and Privacy*, *3*(4), 56–58. doi:10.1109/MSP.2005.104

Hansch, N., & Benenson, Z. (2014). Specifying IT security awareness. In *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA* (pp. 326–330). doi:10.1109/DEXA.2014.71

Häussinger, F. (2015). *Studies on Employees' Information Security Awareness*. Georg-August-Universität Göttingen.

Hellqvist, F., Ibrahim, S., Jatko, R., Andersson, A., & Hedström, K. (2013). Getting their Hands Stuck in the Cookie Jar. *International Journal of Public Information Systems*, *2013*(1), 1–19.

ITU. (2009). Definition of cybersecurity. Retrieved May 2, 2015, from http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126. doi:10.1145/1435417.1435446

Jones, J. (2005). An Introduction to Factor Analysis of Information Risk (FAIR). *Risk Management Insight*.

Krebs, D., Berger, M., & Ferligoj, A. (2000). Approaching achievement motivation - comparing factor analysis and cluster analysis. *New Approaches in Applied Statistics*, 147–171. Retrieved from http://mrvar.fdv.uni-lj.si/pub/mz/mz16/krebs.pdf..

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. doi:10.1016/j.cose.2006.02.008

Lelarge, M., & Bolot, J. (2009). Economic incentives to increase security in the internet: The case for insurance. In *Proceedings - INFOCOM 2009* (pp. 1494–1502). IEEE. doi:10.1109/INFCOM.2009.5062066

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers and Security*, *28*(3-4), 215–228. doi:10.1016/j.cose.2008.11.003

Lim, J. J. S., Ahmad, A., Chang, S., & Maynard, S. B. (2010). Embedding Information Security Culture Emerging Concerns and Challenges. *Pacis 2010*. Victoria: The University of Melbourne. Retrieved from http://www.pacis-net.org/file/2010/S11-03.pdf\nhttp://www.scopus.com/inward/record.url?eid=2-s2.0-84855993316&partnerID=40&md5=142363e45290b5e2475ef5a60ea4fbe3

Madigan, E. M., Petrulich, C., & Motuk, K. (2004). The cost of non-compliance - When policies fail. In *Proceedings of the 32nd annual ACM SIGUCCS conference on User services* (pp. 47–51). ACM. doi:http://doi.acm.org/10.1145/1027802.1027815

Majuca, R. P., Yurcik, W., & Kesan, J. P. (2005). The evolution of cyberinsurance. *Information Systems Frontiers*. National Center for Supercomputing Applications (NCSA).

McAfee. (2014). Net Losses : Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, (June).

McCoy, C., & Fowler, R. (2004). "You are the key to security": establishing a successful security awareness program. In *Proceedings of the 32nd annual ACM SIGUCCS fall conference SE - SIGUCCS '04* (pp. 346–349). doi:doi: 10.1145/1027802.1027882

McNeese, M., Cooke, N. J., D'Amico, A., Endsley, M. R., Gonzalez, C., Roth, E., & Salas, E. (2012). Perspectives on the Role of Cognition in Cyber Security. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 56, pp. 268–271). doi:10.1177/1071181312561063

Meehan, C. L. (2015). Flat Vs. Hierarchical Organizational Structure. Retrieved October 27, 2015, from http://smallbusiness.chron.com/flat-vs-hierarchical-organizational-structure-724.html

Mintzberg, H. (1975). The Manager's Job: Folklore and Fact. *Harvard Business Review*, *53*(4), 49–61. doi:10.1016/S0267-3649(00)88914-1

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3-4), 103–117. doi:10.1016/j.ijcip.2010.10.002

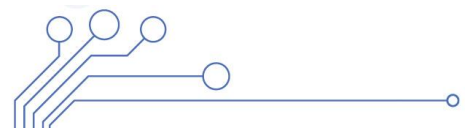
Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*(1), 11–26. doi:10.1016/j.dss.2013.04.004

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Guidelines for usable cybersecurity: Past and present. In *Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, CSS 2011* (pp. 21–26). doi:10.1109/CSS.2011.6058566

Okenyi, P. O., & Owens, T. J. (2007). On the Anatomy of Human Hacking. *Information Systems Security*, *16*(6), 302–314. doi:10.1080/10658980701747237

Parkin, S., van Moorsel, A., Inglesant, P., & Sasse, M. (2010). A stealth approach to usable security: helping IT security managers to identify workable security solutions. In *Proceedings of the 2010 workshop on New security paradigms* (pp. 33–49). ACM. doi:10.1145/1900546.1900553

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37–49.



Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers and Security*, *31*(4), 597–611. doi:10.1016/j.cose.2011.12.010

Prasad, R. S. (2001). Clinical research and methods: Development of the HIV/AIDS Q-sort instrument to measure physician attitudes. *Family Medicine*, *33*(10), 772–778.

Robb, D. (2014). Sony Hack: A Timeline. Retrieved May 19, 2015, from https://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview-north-korea-1201325501/

Rotvold, G., & Braathen, S. (2008). Teaching Business Students Safety for Today's Cyberworld. *M-PBEA Journal*, *3*(1), 45–51. Retrieved from http://www.mpbea.org/journal/Journal_Final_EJournal_2014.pdf#page=25

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-Crimes and their Impacts : A Review. *International Journal of Engineering Research and Applications*, *2*(2), 202–209.

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

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. doi:10.1016/j.compedu.2008.06.011

Siegel, C. A., Sagalow, T. R., & Serritella, P. (2002). Cyber-Risk Management: Technical and Insurance Controls for Enterprise-Level Security. *Information Systems Security*, *11*(4), 33–49. doi:10.1201/1086/43322.11.4.20020901/38843.5

Simmering, M. J. (2006). Management Levels. Retrieved October 27, 2015, from http://www.referenceforbusiness.com/management/Log-Mar/Management-Levels.html

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. doi:10.1108/09685220010371394

Siponen, M. T. (2001). Five dimensions of information security awareness. *ACM SIGCAS Computers and Society*, *31*(2), 24–29. doi:10.1145/503345.503348

Smetters, D. K., & Grinter, R. E. (2002). Moving from the design of usable security technologies to the design of useful secure applications. In *Proceedings of the 2002 workshop on New security paradigms - NSPW '02* (p. 82). doi:10.1145/844115.844117

Gautier, A., Roussel, R., Ducluzeau, P. H., Lange, C., Vol, S., Balkau, B., & Bonnet, F. (2010). Increases in waist circumference and weight as predictors of type 2 diabetes in individuals with impaired fasting glucose: Influence of baseline BMI - Data from the DESIR study. *Diabetes Care*, *33*(8), 1850–1852. doi:10.2337/dc10-0368

Soo Hoo, K. (2000). *How much is enough? A risk management approach to computer security*.

Spurling, P. (1995). Promoting security awareness and commitment. *Information Management & Computer Security*, *3*(2), 20–26. doi:10.1108/09685229510792988

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133. doi:10.1016/j.cose.2004.07.001

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*. *Nist Special Publication* (Vol. 800–30). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.6062&rep=rep1&type=pdf

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MISQ Quarterly*, *22*(4), 441–469. doi:10.2307/249551

Thomas, D. B., & Baas, L. R. (1992). The issue of generalization in Q Methodology: "Reliable Schematics" revisited. *Operant Subjectivity*, *16*(1/2), 18–36.

Tøndel, I. A. (2015). Report Using Cyber-Insurance as a Risk Management Strategy : Knowledge Gaps and Recommendations for Further.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2010). Aligning Security Awareness with Information Systems Security Management. *Journal of Information System Security*, *6*(1), 36–54.

Turle, M. (2009). Data security: Past, present and future. *Computer Law and Security Review*, *25*(1), 51–58. doi:10.1016/j.clsr.2008.11.001

Venter, H. S., & Eloff, J. H. P. (2003). A taxonomy for information security technologies. *Computers and Security*, *22*(4), 299–307. doi:10.1016/S0167-4048(03)00406-1

Vidyaraman, S., Chandrasekaran, M., & Upadhyaya, S. (2008). Position: The user is not the enemy. In *Proceedings of the 2007 Workshop on New Security Paradigms - NSPW '07* (p. 75). doi:10.1145/1600176.1600189

Nierstrasz, O., & Rieger, M. (2006). On the effectiveness of clone. *Online*, *18*(May 2005), 37–58. doi:10.1002/smr.317

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

Von Solms, S. H. (2005). Information Security Governance - Compliance management vs operational management. *Computers and Security*, *24*(6), 443–447. doi:10.1016/j.cose.2005.07.003

Vroom, C., & von Solms, R. (2002). A Practical Approach to Information Security Awareness in the Organization. In *Security in the Information Society* (p. 20). doi:10.1007/978-0-387-35586-3_2

Wendy Hollway, T. J. (2000). *Doing Qualitative Research Differently*. doi:http://dx.doi.org/10.4135/9781849209007

West, R., Mayhorn, C., Hardee, J., & Mendel, J. (2009). The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions. In *Social and Human elements of information security: Emerging Trends and countermeasures* (pp. 43–45). doi:10.4018/978-1-60566-036-3.ch004

Whitten, A., & Tygar, J. D. (1998). *Usability of Security : A Case Study*. *Computer Science*.

Wilson, B. M., & Hash, J. (2003). *Information Technology Security Awareness, Training, education and certification*. *iTL Bulletin*.

Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (1998). *Information Technology Security Training Requirements: A Role- and Performance-based Model*. *NIST Special Publication 800-16*.

Zurko, M. E., & Simon, R. T. (1996). User-Centered Security. *ACM*.

APPENDICES

Appendix A: Summaries of interviews

These interviews are held for gaining information to develop statements in the concourse. Many of the statements are derived from the interviews; the statements can probably not be found one-on-one in the summaries. Because it is a sensitive subject, the respondents are anonymous and named by their initials.

Summary interview G.H.

A cyber incident is according to G.H.: obtaining information by third parties who are not allowed to see the information. The situation to prevent such incidents is very complex, but starts with simple measures. For example to lock your computer when you are leaving your workplace, even for a moment. That means that with many people the chance is high on compliance errors; forgetting to lock your computer is an easily made mistake.

The situation in the hospital G.H. works is in even more complex. 650 different applications are used; for the most important application, the support has to be perfect. That is why several suppliers have instant access to the network of the hospital, remote controlled.

The IT department is responsible for business like remote control and access control. For employees there is a standardized protocol based on their function. The access protocols depend on the necessity of access of certain information. When it is not necessary, you do not get access to patient personal data.

Threats

The biggest threats for the hospital are phishing and spam; for this holds as well that 2000 employees cause a big risk for the security of the hospital. There is a high chance someone makes a mistake, but it is even worse when an employee does not dare to report the mistake. Reasons can be shame or something like that. This is an important reason why there always will be a risk of spam and phishing. A DDoS attack is not a likely event; the hospital is politically relatively neutral. Besides, it is worse when personal data of patients leak.

Measures

There are many measures; G.H. does not know them all by himself as well. Some examples are VPN + token to remote login on the network, double and triple redundant systems, authorisation per function, complex password requirements and network is monitored via a central portal.

People also get informed by email and newsletter about the importance of cyber security awareness. G.H. does not know what awareness exactly is, but he will take a guess; the definition of awareness is about knowing the risks and solutions, but you should also act according to your knowledge. The theoretical definition is not very relevant. However, is awareness the main issue? Gerard is more focussed on procedures than awareness.

At this moment, awareness is raised by mailing information and mentioning cyber security on the quarterly meeting of the complete staff. Also on the intranet of the hospital cyber security is mentioned. The board of directors is not very aware; they should investigate in the cyber security awareness more as well.

Cyber risk

Avoidance is done by blocking several internet addresses. Retention by never having 100% security and the hospital is not interesting as a target for hacks etc. Transferring risk is not interesting, because it costs money. It is only interesting when there are people claiming against the hospital; then reputation damage can emerge. The reason for transference is not pure economic, when an insurer

can help with expertise. Mitigation of the risk is something the hospital focusses on. Technological it is fine, the hospital is certified and thus secure. The only thing left is staff.

Employees are not aware, they think nothing can happen or they blame IT. That is not what the ideal situation is. There are policies and procedures employees have to follow; but employees do not. However, the procedures are not completely clear and can be improved. There is an obligation to report incidents, but does not work out perfect every time. In the bureaucracy, the notification can 'disappear'. The service manager is always alerted when an incident happens.

Awareness

Informing people is at this moment enough to foster behaviour change. However, the current information is not yet up-to-date, the news mail etc. have to be renewed. It is hard to focus attention on cyber security because cyber security is not part of the primary business process of the hospital. It has to be in the future.

As organisation, a risk and safety culture are important in a hospital. It is very delicate and sensitive when information leaks. IT should be in the primary process of the hospital, patient information is namely part of the primary process. Unfortunately, it is not considered like a primary issue, until now only IT is involved.

Software security usability is not good, but it is always a consideration between usability and security. We intend to introduce a new system with login only with cards. That is limited to doctors. It is more usable and quicker for the users, but also has its cons. There is a lot room for improvement, like open and closed systems. Encryption per department, zoning of Wi-Fi and security of workplace on wheels. Which is a moveable computer and usable everywhere in the department.

IT personnel

IT personnel does not have to understand the user, there are other people who do that. IT employees have to do their job. Doctors have much influence in the hospital even in IT; they have a lot of authority, because they are also involved in the primary process.

The system is certified according to NEN 7510 and ISO 27001. Policies are made by a security officer, which gets its input from Gerard and the IT department. In the future, it may be a security department. In the end, there is no real danger for the hospital according to G.H.; other institutions are more likely to be attacked.

Summary interview D.L.

This company is a software developing and hosting organization, active in the healthcare business. Core product is a secure message system for healthcare professionals in especially the Netherlands. A large percentage of the secure messages among doctors, GP's, and hospitals is flowing through this service. It is a SaaS solution and unauthorized access by third parties would be destructive for our organization. The organization is ISO 27001 and NEN7510 certified. Approximately 200 employees in different functions execute the tasks that are characteristic for a real IT company, from developing, maintenance, debugging but also sales.

Security is a broad thing, for us security is always also cyber security. Security is part of our core business, when it goes terribly wrong it has financial impact and impact on patients as well. We are an easy target for people arguing against the EPD or something else. That is why I do not mind that we do not have a lot of exposure in the Netherlands. Hacking is a factual risk; reputation damage can destroy our business in a split second.

Roles, knowledge and awareness

Every new employee in the organization is obligated to attend a cyber security awareness training, which takes 2 hours. This training focusses on probable threats like phishing, physical access and compliance to procedures. It is very important to acknowledge that the human is the weakest link in the security chain. Social engineering is an important risk. Employees learn how to recognize threats and how to act when a threat is faced. Reporting security incidents is actively stimulated; in this way, a safe environment is fostered. The numbers about safety and security are reported to the complete organization every quarter. In addition, we scan our potential employees thoroughly on potential risk for the organization. An unreliable employee or an employee with an evil motive can cause a lot of damage to the organization.

In the management team, a security officer is included; I think every MT should include one. It is the highest level of decision and thus of escalation; for us is security crucial. In every layer, a security manager is reporting to the security officer. There is also a dedicated security incident manager, to respond quickly in case of an incident.

Awareness is very dynamic; everybody has constantly update his knowledge about threats and vulnerabilities. Threats and vulnerabilities are always in development and thus, you should be as well. New technologies imply new threats, which is often not recognized. However, outdated software is also a real threat. Safe behaviour can also annoy at a certain point in time; one can forget to lock his computer, or just do not want to do it anymore.

Goal of awareness is security through the organization. Because awareness changes the behaviour of people into security safe behaviour. Awareness can also be integrated into organizational processes. Everything has to be considered very well.

Conditions

To get a safe environment in your organization, someone has to take the lead. A manager who acts like a role model. Besides, test your own network on vulnerabilities, this leads to awareness about the possible threats as well. Certifying the company is a long and intensive process in which awareness is also raised effectively. It causes transparency about the processes of the organization. Everything becomes clearer, even the measures already taken. Certification requires protocols and documentation of every security process and measure.

Risks and measures

Possible risks are financial risks, commercial risks and reputation damage. Patients also can be endangered, for example, when our services are unavailable and doctors cannot use our databases with crucial information.

Several risks can cause serious danger. Internet or power interruption, fire, ransom ware, hackers, sabotaging employees. DDoS is devastating for our availability. The risk that is caused by software of third parties is also important, but hard to estimate what the risk exactly is.

Measures taken to mitigate these risks are: Diesel generators to respond to power cuts, redundant datacentres, power and internet cables to different sides of the building, scan of employees, network monitoring, detection, and DDoS prevention. Many more measures are taken.

Transference

Transference is insurance and for us in almost any situation too late. It is only interesting when the damage that is left is covered. It depends on what is covered and what it costs; it is hard or impossible

to estimate such costs. Knowledge from other parties is not necessary, because we do everything by ourselves.

Risk and damage can be caused by third parties, which is not your responsibility. Nevertheless, it will hurt you, so you have to control such risks as much as possible; the choice for third parties is in the end your responsibility.

Avoid risk

Completely avoiding risk is impossible, but some sub-risks can be avoided. We do not save some of the data we do not have to save. When storing backup tapes in the safe is done by two persons instead of one, much risk is avoided as well. Access control based on function is also avoiding risk, authorisation levels can help a lot. Non-disclosure agreements, VOG, redundancy and self-recovering software and encryption are all measures to avoid risk.

Reduce risk

Some of the issues discussed before can also be included in reduction. Some other reduction measures are also noted, like technology and human oriented measures. There are more possibilities. Like legal possibilities, but it should not be necessary. CBP has to be careful that legislation is about the better security and not about punishing organizations. The goal is to reduce data breaches and it is not about earning money through fines. I hope it helps to reduce breaches. I am a little sceptical and not every obligated measure is a good one.

Organisation

Several things can be done throughout an organization to improve security. Provide resources like money to improve security and awareness. Management should be involved in making policies for security. Reporting incidents can be obligated for every employee. In software development, we can enforce to check if top 10 security holes are covered etc. Certifying the company is a decision that affects the whole organization.

Finally yet importantly, there always is some residual risk. Continually improving technology implies continually improving vulnerabilities. It is always a consideration about impact and possible costs. There is no trigger to cover literally every risk, because it is relatively expensive. Most important issue is that almost any company has issues similar to an IT company and thus should be protected like an IT organization does.

Summary interview M.D.

M.D. works at ‘Rijkswaterstaat’ (RWS), which is part of the Dutch ministry of infrastructure and environment. The organization is responsible for the execution of the ministry’s policy. Within the organization many different department exist, M.D. is working at the department for software validation and verification. RWS is an organization with approximately 9000 employees.

Cyber definitions

Cyber includes any automatized hardware and software, but it also affects the users and other aspects connected to users. Security for cyber includes a set of measures that can be taken to prevent a cyber incident. But the interviewee does not see the relevance for practice in a theoretical definition.

Cyber risk

Risks for RWS regarding cyber incident are loss of data by users and theft of data. More important is the availability of the systems, since RWS controls some of the ‘critical infrastructures’ in the Netherlands. For these risks, measures are taken. It has to be noted that there is no such thing as complete security, but that is acceptable at a certain level. RWS reached the level of security that some

of the risks are acceptable. RWS estimates that only other states and organized crime are able to affect the network and systems. Concrete risks are external events, like hackers or power interrupt that influence the systems. In addition, users that do not know about any risks on the internet cause danger to the network, because hackers mainly focus on individuals or individual systems. However, sometimes it does not matter how skilled anybody is, anybody can make a mistake. Therefore, everybody is vulnerable for an attack. Notable as well, most of the employees are not completely compliant regarding cyber security. M.D. notices some employees who disable their virus scanner to use certain software packages.

Impact

When a system fails or is being interrupted, it is not our business. The scale is usually to large and thus the responsibility for a separate department. This department has expertise to recover quickly from a cyber incident. The knowledge for prevention, detection and recovering from a cyber incident are all in-house. Which has many advantages, because you can act quickly and relatively cheap.

Measures

M.D. gives some examples of precautions taken by RWS. This will not be in detail, because it is sensitive information. Part of the systems is separated from the internet; in this way, it is almost impossible to enter the system from outside RWS. Some systems are only accessible with login + token verification, which also hardens the attempts to hack. USB's are all encrypted; losing sensitive information is through that a lot 'safer'. The network is monitored real-time. RWS is also certified according the BIR norm, which is for governmental organizations and based on ISO 27001. RWS has its own penetration testing facility, which tests all the systems and departments periodically.

Awareness

Behaviour is an important aspect in cyber security according to M.D. It is about knowing what the risks are, so that one can recognize. Also about how to act, when a risk is identified. To let people comply with this behaviour, knowing why one has to take actions is crucial. Acknowledging the reasons why you have to be aware causes a behaviour change. Awareness is important, but it is very important to act correctly. Therefore, procedures have to be followed. Which implies every possible scenario has to be included in the procedures. Protocols and procedures help people to act 'safe'. An example are the policies about passwords, a complex password is required in this organization. By knowing why you have to change your password, the employees will also change his password in a correct way. Not by only by adding +1 to his year of birth.

User-centered technology

It is not about adapting the technology to the user, which is too expensive. Only when there is unlimited budget is this perhaps possible. Namely, it is also hard to prove that such technology is safer. The ideal option is indeed to have everything protected by technology.

Risk treatment

It is impossible to avoid risk completely. Mitigation of risk is already treated and has many possibilities. The main consideration for mitigation or retain risks is money, when a probable risk has an expected impact and the protection turns out to be cheaper, the risk should be mitigated. Residual risk can eventually be transferred, but is not necessary. Insurance is only interesting when an organization does not have all the expertise to deal with cyber security and incident management.

Management vs. operations

Every operations department has its own focus; management has to focus on general security. Because when it goes wrong, it is the responsibility of the management. Management has the possibilities to switch to any corporate resources to mitigate the risk or to responds to an accident. Reputation has to be kept safe at any costs. A separated department for cyber security is a good option in every organization, in this way relevant expertise is also present in management.

According to the management, improving awareness is important, but it is only partially a solution. Software has to be appropriate and is according to M.D. the best and most complete solution. However, it is often not possible, because it is too expensive.

Summary interview H

Interviewee is service manager in a large insurance company in the Netherlands. He has to deal with the company's facilities and the relation to the business.

Cyber security and risks

Cyber security is a set of measures to protect against cyber risks. Awareness is the knowledge, which risk there are, however risks are always developing and one have to update his risk continuously. There are several cyber risks, but cyber risks are tight related to normal risks. Like open doors that provide access to rooms with crucial computer systems. These risks are definitely cyber risk related. A few concrete examples of risks: Employees with own USB's, which can be infected; a leak in the security of our systems; DDoS attacks on the availability of our systems; dissatisfied employees who have access to crucial systems; software that is bought from other companies; suppliers with other systems; auditors that check our systems; compliance problems with employees; software that is built without safety standards; saving passwords on sticky notes; unaware employees and unreported incidents. Too much to name.

How to deal with risks

Because there are many different risks, there are also many ways to deal with risk. Our company distinguishes internal and external risks and have these subdivided as well. External risks can be dealt with for example by contracts with third parties. Main external issues are hackers and technical failures, examples are power breakdowns, DDoS attacks and hacks. Our systems are improved by periodically test our systems by external parties, every time another third party. Mitigation of risk is thus of high priority. Our systems are able to resist DDoS attacks, because availability of our systems is very important. Besides, backups all over the world are available within 24 hours (for the complete operational system). The interviewee thinks the cyber security is very well arranged and he states that the system is very safe. 'We are hard to hack'.

Therefore, it is useless to transfer our residual risk to (another) insurance company. It is an economical decision, but for our company it will not result in any advantages. All expertise is inside the company, they can deal with almost any known issue related to cyber security. Although, there is always residual risk. Risk is not acceptable when the impact is immaterial, when the reputation of the company is at stake. Another reason for prevent from risk is the legal issue. When there is an obligation to reduce or avoid risk, the company should do that. Sometimes it is hard to be compliant to the legal measures and it often costs a lot of money. That also holds for employee awareness. Security costs money, it is better to invest more in protection for applications that are crucial for business than other applications. Main internal issues are non-compliant employees and unsatisfied employees, which have access to the system. We have internal requirements for software that has to be built to prevent software security issues.

Employees

Employees are an important resource for the company, but they cause a lot of risk as well. Because there are many of them, an accident easily occurs. The company tries to reduce such errors by awareness improvement programs and comprehensive procedures and policies. For almost every situation a procedure is available, also organizational processes are audited and monitored. Every employee has to follow a cyber risk course for awareness improvement. In addition, the intranet is a valuable source of documents regarding awareness and cyber risks. The company stimulates the employees to report their own and each other's incidents. Because the company is in the domain of insurance, trust is important. Therefore, the company intends to have a safety culture. Everything has to be focussed on awareness. The employees have a lot of responsibility regarding cyber security; only the real important breaches reach the top management. The rest of the incidents are handled by lower management or even employees themselves, this is all defined in procedures.

Security department

Security is very important and the company is large, therefore the company has its own security department. This department defines sharp requirements for IT systems and employees, also legislation is taken into account. Procedures for any situation are made by this department. They are represented in the top of the management and there is in this way enough knowledge in the top of the management. The interviewee thinks that the board of directors is aware of the cyber risks that apply on their company.

Because the company is present in several countries, all kinds of legislation apply on the company as well. The security department considers the different legal issues. A separate department has many advantages; the knowledge is centralised and present in the company. Which is identified as a part of the economies of scale that the company has.

Summarized, the interviewee thinks the company has arranged the cyber security well. A specialized department for security spreads the knowledge among the employees. The employees need extra attention because of the potential risk. Having comprehensive procedures provides an extra layer of secure behaviour.

Appendix B: Questionnaire

The questionnaire is about your view on cyber security in organizations. This will be captured by a small list of questions and a questionnaire. The results are used to inventory the perspectives of managers regarding cyber security. To complete the complete questionnaire, around 30 – 40 minutes is needed. Because of the sensitivity of cyber security, the questionnaire will be anonymous.

Contextual questions:

Organizational size and sector

What is the size of the organization? (approximately) …… FTE

In which sector is the organization active?

……

Cyber security in the organization

In our organization the cyber security is the responsibility of:

- O A security officer
- O A security management
- O IT-department
- O Nobody
- O Different, namely……..

Data as core business

Is the treatment of personal data core business? (Does the organization processes personal data of more than 5000 persons a year)

Yes / No / Do not know

Legislation

Are there any legal requirements for the cyber security in your organization, regarding processing of personal data? Legal requirements can be obligated by, for example: College Bescherming Persoonsgegevens, Rijksoverheid (BIR), Autoriteit Financiële Markten and foreign law enforcers.

Yes / No / Do not know

Certification

Does your organization have a certification for IT systems? If yes, which one?

- O No certification
- O NEN 7510
- O ISO 27001
- O ISO 27002
- O Different, namely……..

IT in function

Are there any IT related tasks in your daily job?

No / Yes, my daily tasks that involve IT are:

……..

Training in cyber security

Did you attend to any cyber security training in the organization?

Yes / No

Q-sort

This questionnaire contains 48 statements about cyber security and an accompanying scheme to sort the statements. The idea is to visualize your perspective on cyber security based on 48 statements. It is important that you judge the statement from your own personal view on the topic of cyber security. The next steps will guide you to complete the questionnaire:

Step 1: Read every statement and sort them in three separate categories. The categories are: agree, for the statements you agree on; neutral, for the statements that are unclear to you or you do not have an opinion about; and disagree, for the statements you disagree on. Count the statements for each category and write the numbers down.

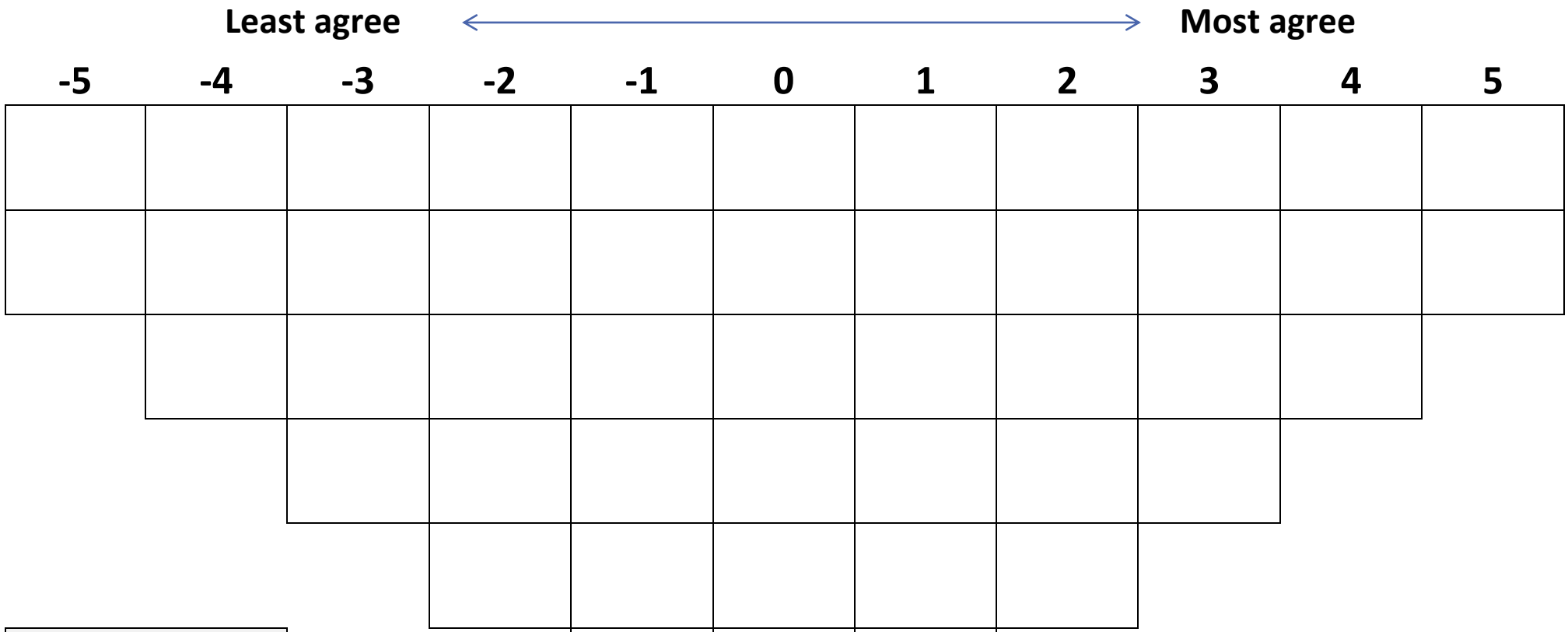
Step 2: Take the pile of statements in the category 'agree' and read them again. Sort the statements in the structure that is displayed on the scheme. That means for every empty box, there is a place for a statement. Sort the statements from the **right-hand** outside to the inside, until you run out of statements.

Step 3: Take the pile of statements in the category 'disagree and read them again. Sort the statements in the structure that is displayed on the scheme. That means for every empty box, there is a place for a statement. Sort the statements from the **left-hand** outside to the inside, until you run out of statements.

Step 4: Take the rest of the statements and fill the gap between the statements that you agree or disagree on.

Step 5: If you are done, check the complete scheme again and decide if you still agree on the sorting. Change the sort in whatever is needed to match your viewpoint.

Step 6: Explain your choices and doubt about your choices. Does the arranged scheme impersonate your view on cyber security?



Amount agree:
Amount neutral or not relevant:
Amount disagree:

Respondent number:

Appendix C: Answers on contextual questions

Table 9 overview of percentages of the answers given by respondents on the question from Appendix B

	Factor I	Factor II	Factor III	Factor IV	No Factor	Total
FTE						
0-10	29%	17%	0%	14%	23%	18%
11-100	29%	50%	14%	14%	23%	25%
101-500	29%	17%	29%	43%	38%	33%
501 and above	14%	17%	57%	29%	15%	25%
Responsibility security						
A security officer	0%	17%	14%	14%	31%	18%
A security management	0%	17%	43%	0%	0%	10%
IT-department	57%	0%	29%	57%	38%	38%
Nobody	29%	17%	0%	0%	15%	13%
Different,	14%	50%	14%	29%	15%	23%
Data as core business						
Yes	57%	33%	86%	29%	62%	55%
No	43%	50%	14%	71%	23%	38%
Don't know	0%	17%	0%	0%	15%	8%
Legislation obligations						
Yes	29%	83%	86%	57%	46%	58%
No	29%	0%	14%	29%	38%	25%
Don't know	43%	17%	0%	14%	15%	18%
Certification						
No certification	71%	50%	57%	57%	54%	58%
NEN7510	14%	17%	0%	0%	15%	10%
ISO27001	14%	17%	0%	14%	31%	18%
Different,	14%	17%	0%	14%	15%	5%
Don't know	14%	33%	43%	29%	8%	23%
IT tasks in job						
Yes	43%	33%	71%	57%	92%	65%
No	57%	67%	29%	43%	8%	35%
Cyber security training						
Yes	0%	17%	71%	29%	31%	30%
No	100%	83%	29%	71%	69%	70%
#Respondents	7	6	7	7	13	40

Appendix D: Free distribution data

Respondent	*Mean*	*Standard deviation*
1	0,000	2,609
2	0,000	2,609
3	0,000	2,609
4	0,000	2,609
5	0,000	2,609
6	0,000	2,609
7	0,000	2,609
8	0,000	2,609
9	0,000	2,609
10	0,000	2,609
11	0,000	2,609
12	0,000	2,609
13	0,000	2,609
14	0,000	2,609
15	0,000	2,609
16	0,000	2,609
17	0,000	2,609
18	0,000	2,609
19	0,000	2,609
20	0,000	2,609
21	0,000	2,609
22	0,000	2,609
23	0,000	2,609
24	0,000	2,609
25	0,000	2,609
26	0,000	2,609
27	0,000	2,609
28	0,000	2,609
29	0,000	2,609
30	0,000	2,609
31	0,000	2,609
32	0,000	2,609
33	0,000	2,609
34	0,000	2,609
35	0,000	2,609
36	0,000	2,609
37	0,000	2,609
38	0,000	2,609
39	0,000	2,609
40	0,000	2,609

Appendix E: correlation of respondents

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
1	100	50	37	25	30	44	17	44	5	54	20	28	55	28	20	32	19	38	35	52	34	52	56	10	41	37	49	50	49	19	52	27	40	31	17	55	20	7	3	18
2	50	100	59	26	34	55	34	62	42	64	58	51	44	39	20	46	45	49	50	62	47	52	80	30	51	59	63	32	57	47	58	40	40	47	30	70	50	28	25	56
3	37	59	100	30	17	38	42	44	39	51	59	38	35	42	29	37	17	26	59	53	23	57	55	31	47	48	55	19	33	35	46	58	38	27	19	67	37	28	17	52
4	25	26	30	100	23	38	-1	25	33	20	3	42	25	24	34	20	26	13	22	8	28	38	19	14	40	9	25	-4	2	15	48	17	34	28	2	35	21	12	-9	23
5	30	34	17	23	100	49	17	37	4	23	29	28	14	25	20	21	38	24	35	31	31	35	44	29	34	30	16	28	14	12	43	12	44	32	29	22	-9	19	19	9
6	44	55	38	38	49	100	11	29	21	58	15	57	56	37	36	46	44	32	43	21	32	56	56	4	32	51	19	22	27	18	61	14	39	31	47	35	39	17	22	36
7	17	34	42	-1	17	11	100	25	11	20	35	38	-11	23	-9	9	24	25	38	30	8	20	24	11	38	8	27	33	26	9	13	22	26	15	20	30	28	15	14	29
8	44	62	44	25	37	29	25	100	17	28	58	25	29	22	14	19	9	42	45	75	49	44	47	40	39	49	55	43	34	43	40	48	47	54	31	59	29	20	32	31
9	5	42	39	33	4	21	11	17	100	32	30	39	2	9	35	22	2	-1	24	19	16	0	33	27	2	33	45	4	12	10	15	33	43	28	24	34	35	-1	5	19
10	54	64	51	20	23	58	20	28	32	100	37	59	48	32	30	50	44	32	46	41	28	59	63	18	22	63	50	41	54	21	56	21	48	43	35	58	44	17	5	49
11	20	58	59	3	29	15	35	58	30	37	100	32	4	35	20	37	11	21	60	50	31	32	43	41	49	44	52	16	24	44	27	46	18	39	17	48	33	44	39	35
12	28	51	38	42	28	57	38	25	39	59	32	100	28	28	33	49	31	14	37	19	7	43	40	6	37	43	41	25	31	12	47	22	36	31	30	29	45	22	-2	46
13	55	44	35	25	14	56	-11	29	2	48	4	28	100	20	21	54	27	22	34	29	26	60	54	5	24	43	33	32	41	13	64	37	32	25	22	45	27	25	10	40
14	28	39	42	24	25	37	23	22	9	32	35	28	20	100	34	27	29	52	30	22	5	42	38	25	36	14	34	21	23	21	39	1	18	48	22	48	30	34	15	46
15	20	20	29	34	20	36	-9	14	35	30	20	33	21	34	100	31	17	-6	17	10	18	32	15	16	23	8	31	21	-4	1	43	9	36	25	17	26	-3	8	10	31
16	32	46	37	20	21	46	9	19	22	50	37	49	54	27	31	100	24	5	49	22	19	44	62	16	41	28	36	19	43	7	50	28	28	29	18	45	29	25	-8	50
17	19	45	17	26	38	44	24	9	2	44	11	31	27	29	17	24	100	34	29	14	22	35	40	4	37	22	8	23	28	4	50	-11	27	28	17	37	17	18	20	48
18	38	49	26	13	24	32	25	42	-1	32	21	14	22	52	-6	5	34	100	16	40	3	32	47	30	38	34	37	36	32	33	39	12	32	45	31	50	40	8	33	34
19	35	50	59	22	35	43	38	45	24	46	60	37	34	30	17	49	29	16	100	42	48	49	60	34	54	41	43	25	26	40	48	49	36	33	20	56	38	33	27	35
20	52	62	53	8	31	21	30	75	19	41	50	19	29	22	10	22	14	40	42	100	39	44	55	47	39	43	57	44	55	18	49	39	48	52	26	68	26	13	13	30
21	34	47	23	28	31	32	8	49	16	28	31	7	26	5	18	19	22	3	48	39	100	30	37	25	27	16	30	16	12	44	28	20	28	27	18	32	20	23	17	7
22	52	52	57	38	35	56	20	44	0	59	32	43	60	42	32	44	35	32	49	44	30	100	52	22	59	43	39	42	41	26	70	31	36	37	31	57	32	24	24	49
23	56	80	55	19	44	56	24	47	33	63	43	40	54	38	15	62	40	47	60	55	37	52	100	35	43	62	56	35	66	28	60	43	52	44	39	71	44	33	16	52
24	10	30	31	14	29	4	11	40	27	18	41	6	5	25	16	16	4	30	34	47	25	22	35	100	27	21	51	25	32	26	27	39	32	38	17	39	8	29	2	18
25	41	51	47	40	34	32	38	39	2	22	49	37	24	36	23	41	37	38	54	39	27	59	43	27	100	16	37	24	18	32	57	31	19	27	10	46	24	31	26	47
26	37	59	48	9	30	51	8	49	33	63	44	43	43	14	8	28	22	34	41	43	16	43	62	21	16	100	47	25	46	32	52	52	46	47	33	47	51	23	34	44
27	49	63	55	25	16	19	27	55	45	50	52	41	33	34	31	36	8	37	43	57	30	39	56	51	37	47	100	47	44	38	44	43	49	50	12	54	40	16	-1	33
28	50	32	19	-4	28	22	33	43	4	41	16	25	32	21	21	19	23	36	25	44	16	42	35	25	24	25	47	100	39	-3	29	6	43	29	31	37	14	-1	7	21

29	49	57	33	2	14	27	26	34	12	54	24	31	41	23	-4	43	28	32	26	55	12	41	66	32	18	46	44	39	100	0	47	26	38	40	25	55	31	11	-9	39
30	19	47	35	15	12	18	9	43	10	21	44	12	13	21	1	7	4	33	40	18	44	26	28	26	32	32	38	-3	0	100	16	28	-4	7	-5	20	33	22	32	20
31	52	58	46	48	43	61	13	40	15	56	27	47	64	39	43	50	50	39	48	49	28	70	60	27	57	52	44	29	47	16	100	36	56	55	28	65	34	21	22	64
32	27	40	58	17	12	14	22	48	33	21	46	22	37	1	9	28	-11	12	49	39	20	31	43	39	31	52	43	6	26	28	36	100	41	36	14	49	29	33	25	32
33	40	40	38	34	44	39	26	47	43	48	18	36	32	18	36	28	27	32	36	48	28	36	52	32	19	46	49	43	38	-4	56	41	100	55	46	53	28	-3	-6	42
34	31	47	27	28	32	31	15	54	28	43	39	31	25	48	25	29	28	45	33	52	27	37	44	38	27	47	50	29	40	7	55	36	55	100	28	56	46	19	29	43
35	17	30	19	2	29	47	20	31	24	35	17	30	22	22	17	18	17	31	20	26	18	31	39	17	10	33	12	31	25	-5	28	14	46	28	100	29	32	19	35	29
36	55	70	67	35	22	35	30	59	34	58	48	29	45	48	26	45	37	50	56	68	32	57	71	39	46	47	54	37	55	20	65	49	53	56	29	100	41	26	20	54
37	20	50	37	21	-9	39	28	29	35	44	33	45	27	30	-3	29	17	40	38	26	20	32	44	8	24	51	40	14	31	33	34	29	28	46	32	41	100	25	27	43
38	7	28	28	12	19	17	15	20	-1	17	44	22	25	34	8	25	18	8	33	13	23	24	33	29	31	23	16	-1	11	22	21	33	-3	19	19	26	25	100	28	30
39	3	25	17	-9	19	22	14	32	5	5	39	-2	10	15	10	-8	20	33	27	13	17	24	16	2	26	34	-1	7	-9	32	22	25	-6	29	35	20	27	28	100	17
40	18	56	52	23	9	36	29	31	19	49	35	46	40	46	31	50	48	34	35	30	7	49	52	18	47	44	33	21	39	20	64	32	42	43	29	54	43	30	17	100
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**

Appendix F: Statements and their factors scores

		Factor			
	Statements	**I**	**II**	**III**	**IV**
1	Our organization is well protected against cyber risks.	-1,47	-0,08	0,49	-0,55
2	IT is very important in our organization.	1,92	0,46	1,35	1,95
3	My cyber security awareness is high enough.	-1,20	0,28	0,05	-0,55
4	The end user does hardly know anything about cyber risks and he does not know anything about dealing with the risks.	1,18	-0,44	-0,72	-0,48
5	Many employees in a big organization implies a high chance on a cyber incident, because not everybody is compliant to the rules.	0,32	-0,33	0,49	-0,49
6	A risk that has insufficient attention is the risk of unsatisfied employees that have access to sensitive data and systems.	0,30	-0,26	0,71	-0,26
7	An underestimated risk is the risk of new technologies that cause new cyber risks.	0,50	0,50	0,35	0,68
8	Outdated software is a big risk for cyber security.	0,03	1,15	0,58	1,96
9	Unavailability of our services due to technical failure or cyber attack has huge consequences.	1,55	0,07	1,43	2,29
10	Top management underestimates the cyber risks.	0,66	-0,35	-1,19	-0,28
11	Cyber security policies and procedures in our organization are not sufficiently developed.	1,36	-0,59	-0,61	0,32
12	Cyber security is seen as IT only problem too often. It is also about governance, leadership, culture, awareness and behaviours. Which are often forgotten.	0,64	2,07	1,24	0,79
13	Unavailability of our services due to external events like flooding, fire or Internet disruption is serious. We need to have a high level of up time.	0,98	-0,91	1,18	1,51
14	Suppliers and other third parties can be a serious risk for our organisation, due to their own bad/insufficient cyber security.	0,28	0,86	0,96	0,90
15	Uncoupling several IT systems is a good way to avoid a part of the cyber risks.	-0,09	-0,56	-0,79	0,56
16	It is better to prevent suffering from cyber attacks than to recover from cyber attacks.	0,93	1,34	1,16	1,65
17	An organization has to avoid risk as much as possible, for example do not save personal data that is not necessary to save.	-0,17	0,75	-1,25	0,27
18	An organization's cyber security cannot be 100% safe. There is always residual risk, which is acceptable.	1,47	0,08	1,76	0,40
19	Organizations do not have to protect against risks, which never will be encountered.	-0,57	-0,87	-0,70	-1,09
20	There is a possibility that cyber risks can be accepted, when the costs of securing are higher than the possible impact.	0,20	-1,12	1,34	-0,43
21	Nowadays almost every organization is an IT company, which implies every organization has to reduce risk by taking cyber security measures equal to an IT company.	-0,37	0,66	-0,82	1,12
22	Cyber insurance is useless; the (cyber) damage already had its impact.	-0,73	-1,78	-0,45	-0,42
23	Cyber insurance is not needed. The premiums are high and the chance on breach in our cyber security low. It is economical not interesting.	-0,91	-1,89	-0,53	-0,99
24	The role of insurances in cyber security and risk management is unclear to me.	0,33	-0,49	0,36	-0,05

25	Insurers can help organizations with cyber risk management; insurers have a lot of knowledge in the fields they insure.	-0,46	0,33	-0,61	-1,50
26	IT systems in cyber security should be tested regularly to foster the safety.	1,32	0,74	0,57	0,93
27	Total cyber security can best be reached through technological means.	-0,96	-1,23	-1,69	-1,44
28	When technical means are certified, they can be perceived as completely safe.	-1,62	-1,86	-1,89	-1,78
29	It is sufficient to raise cyber security awareness of employees by informing the employees by newsletter or mail. In which cyber risks and dealing with risks is explained.	-1,38	-1,13	-1,69	-1,03
30	Cyber security awareness training has to be mandatory for every employee in an organization.	-0,76	0,66	0,08	-0,61
31	When employees comply with the policies and procedures regarding cyber security, sufficient mitigation of human errors is reached.	0,23	-0,63	-0,94	-0,23
32	The knowledge to manage all aspects of cyber security should be present in the company itself.	-1,19	0,24	-0,28	-1,10
33	Organizations cannot without integral cyber security approach; cyber security has to be throughout the whole organization.	0,16	1,57	1,45	0,74
34	For every cyber scenario that is possible, even the unlikely ones, there have to be extensive procedures.	-1,85	0,32	-1,09	-1,64
35	Some cyber security measures are mandatory by law. That they are mandatory is also the only reason they are taken.	-0,89	-1,45	-1,28	-1,57
36	Legislation is not necessary to achieve an acceptable level of cyber security.	-0,76	-1,10	0,41	-0,79
37	It is necessary to define cyber security contracts with employees and third parties. Contracts that define cyber security measures that have to be taken by the relevant parties.	0,00	1,12	0,21	0,42
38	Employees have to be stimulated to report each other's' cyber incidents.	0,87	0,54	0,53	0,18
39	Management support is important to increase the cyber security awareness in an organization.	0,73	0,66	1,74	0,51
40	Much budget has to be available to improve the cyber security awareness in an organization.	-1,16	-0,32	-0,74	-0,30
41	Cyber security awareness has to be formally integrated in business processes. In this way, no one can ignore security awareness.	0,64	1,48	0,70	-0,05
42	All users in an organization have to be cyber security aware for the purpose of cyber security.	0,82	1,56	0,09	1,05
43	Cyber security is pushed off to the IT department. This department has to be cyber security aware, the rest of the employees do not matter.	0,57	-0,14	0,36	0,15
44	For good cyber security in an organization a separate department or function needs to be cyber security aware. For example a cyber security officer or a cyber security department.	-1,20	0,16	-0,21	-0,31
45	In every board of directors or management, team there has to be a security officer, which is cyber security aware. Only then, cyber security is guaranteed.	-1,90	0,07	-1,46	-0,55
46	For me it is not clear what the use of cyber security awareness is.	-0,73	-1,96	-1,19	-1,04
47	The human is the weakest link in cyber security; cyber security awareness can be a partial solution for that.	1,37	0,44	0,97	1,02

48	People in an organization are the biggest risk, which is why everything has to be focussed on increasing cyber security awareness of users.	1,01	1,37	-0,44	0,12

Appendix G: Calculations threshold for single loadings

Highest number of single factor loadings is for the threshold ">0.41", this threshold is used to select respondents per Factors.

Resp.	Factor I	Factor II		Factor III		Factor IV		>0.39	>0.4	**>0.41**	>0.42	>0.43	>0.44	>0.45	>0.46	>0.47	>0.48	>0.49	>0.5
1	0.34930	0.08892	0.03157	0.43682	0.04656	0.29815	-0.01064	1	1	**1**	1	1	0	0	0	0	0	0	0
2	0.32226	0.46252	-0.01997	0.38074	0.09704	0.53243	-0.00110	2	2	**2**	2	2	2	2	2	1	1	1	1
3	0.21410	0.52098	-0.02794	0.20868	0.05522	0.47810	0.01996	2	2	**2**	2	2	2	2	2	2	1	1	1
4	0.43694	0.20358	-0.05637	0.08985	0.01042	0.02837	0.01098	1	1	**1**	1	1	0	0	0	0	0	0	0
5	0.47891	0.11295	-0.01198	0.36532	-0.01315	-0.04728	0.14304	1	1	**1**	1	1	1	1	1	1	0	0	0
6	0.70717	0.02617	0.11217	0.15532	-0.03587	0.38217	-0.05463	1	1	**1**	1	1	1	1	1	1	1	1	1
7	0.05806	0.31744	0.00011	0.19703	0.03878	0.15112	0.00097	0	0	**0**	0	0	0	0	0	0	0	0	0
8	0.17355	0.50116	0.01901	0.59297	0.03032	0.11636	0.05448	2	2	**2**	2	2	2	2	2	2	2	2	2
9	-0.00353	0.15849	-0.01411	0.18266	0.00194	0.38675	-0.00477	0	0	**0**	0	0	0	0	0	0	0	0	0
10	0.40250	0.05871	0.06934	0.29960	-0.00102	0.66078	-0.02216	2	2	**1**	1	1	1	1	1	1	1	1	1
11	0.05578	0.80535	0.09636	0.15346	-0.04321	0.26741	-0.01061	1	1	**1**	1	1	1	1	1	1	1	1	1
12	0.37253	0.09682	0.02419	0.09106	-0.01146	0.58518	0.01837	1	1	**1**	1	1	1	1	1	1	1	1	1
13	0.49512	-0.04254	0.11728	0.20128	-0.01289	0.42247	-0.04186	2	2	**2**	2	1	1	1	1	1	1	1	0
14	0.38350	0.30009	-0.03758	0.20982	0.05498	0.12099	0.01946	0	0	**0**	0	0	0	0	0	0	0	0	0
15	0.49122	0.09227	-0.02610	0.06988	-0.00987	0.04590	0.00110	1	1	**1**	1	1	1	1	1	1	1	1	0
16	0.39769	0.12511	-0.00484	-0.01903	-0.04312	0.59547	0.04361	2	1	**1**	1	1	1	1	1	1	1	1	1
17	0.52282	0.04727	0.02487	0.13038	0.00187	0.16218	-0.01028	1	1	**1**	1	1	1	1	1	1	1	1	1
18	0.20098	0.22136	-0.00931	0.54572	0.01638	0.06413	0.06906	1	1	**1**	1	1	1	1	1	1	1	1	1
19	0.35811	0.54073	-0.06233	0.14042	0.05596	0.35010	-0.00571	1	1	**1**	1	1	1	1	1	1	1	1	1
20	0.06967	0.34193	-0.02539	0.70901	-0.01582	0.22467	-0.03127	1	1	**1**	1	1	1	1	1	1	1	1	1
21	0.24283	0.31423	-0.01933	0.23329	0.05426	0.09041	0.02401	0	0	**0**	0	0	0	0	0	0	0	0	0
22	0.65246	0.24019	-0.01257	0.24978	0.04669	0.29437	-0.01107	1	1	**1**	1	1	1	1	1	1	1	1	1
23	0.34658	0.29486	-0.00322	0.40473	0.07747	0.59394	-0.01468	2	2	**1**	1	1	1	1	1	1	1	1	1
24	0.01504	0.41172	0.02882	0.36528	0.02061	0.09011	0.00693	1	1	**1**	0	0	0	0	0	0	0	0	0
25	0.54266	0.48979	-0.13326	0.10324	-0.00290	0.09662	-0.02708	2	2	**2**	2	2	2	2	2	2	2	1	1
26	0.16294	0.24339	-0.01741	0.32479	0.02805	0.58548	-0.00352	1	1	**1**	1	1	1	1	1	1	1	1	1
27	0.05802	0.38746	-0.01310	0.48927	0.03175	0.44697	-0.04471	2	2	**2**	2	2	2	1	1	1	1	0	0

28	0.18451	-0.01292	0.00426	0.56601	-0.02770	0.16835	-0.01293	1	1	**1**	1	1	1	1	1	1	1	1	1
29	0.04829	0.00032	-0.03695	0.50578	-0.08268	0.54591	-0.12145	2	2	**2**	2	2	2	2	2	2	2	2	2
30	0.06178	0.63824	0.02775	0.01655	-0.03884	0.07346	-0.01457	1	1	**1**	1	1	1	1	1	1	1	1	1
31	0.72311	0.14823	0.05741	0.34849	0.03234	0.33463	-0.00487	1	1	**1**	1	1	1	1	1	1	1	1	1
32	0.01028	0.46854	-0.00001	0.17647	0.01296	0.39551	0.01817	2	1	**1**	1	1	1	1	1	0	0	0	0
33	0.27084	-0.01452	0.01640	0.65289	-0.03369	0.33133	-0.06180	1	1	**1**	1	1	1	1	1	1	1	1	1
34	0.27160	0.26347	-0.00659	0.56303	0.05036	0.18359	0.03790	1	1	**1**	1	1	1	1	1	1	1	1	1
35	0.25175	0.05484	0.02182	0.34410	0.03466	0.19196	-0.00198	0	0	**0**	0	0	0	0	0	0	0	0	0
36	0.30205	0.39780	-0.00727	0.52741	0.09482	0.38960	-0.00762	2	1	**1**	1	1	1	1	1	1	1	1	1
37	0.08692	0.33704	-0.02544	0.16789	0.02094	0.48247	0.02914	1	1	**1**	1	1	1	1	1	1	1	0	0
38	0.24469	0.42571	-0.08925	-0.08328	-0.01181	0.15736	-0.02002	1	1	**1**	1	0	0	0	0	0	0	0	0
39	0.13406	0.39676	-0.01409	0.11875	0.01166	-0.05450	0.02590	1	0	**0**	0	0	0	0	0	0	0	0	0
40	0.39216	0.28154	-0.02470	0.16722	0.06086	0.42623	-0.00420	2	1	**1**	1	0	0	0	0	0	0	0	0
						Number of single loadings:		22	25	**27**	26	25	23	24	24	24	24	23	21

Appendix H: Concourse (Dutch)

0	Onze organisatie is goed beveiligd tegen cyber gevaren.
0	IT is erg belangrijk voor onze organisatie.
0	Mijn cyber security awareness is hoog genoeg.
0	Onze organisatie heeft een risico assessment nodig, aangezien we niet goed weten wat precies de risico's zijn en impact daarvan is.
0	Het buit maken en misbruiken van gevoelige informatie is het grootste gevaar voor onze organisatie.
1,1	Wachtwoorden opslaan in mijn iPhone is handig, dan heb ik mijn wachtwoorden altijd bij de hand.
1,1	Iedereen kan slachtoffer worden van een cyber aanval.
1,1	De gebruiker weet vrijwel niets van cyber gevaren en al helemaal niet hoe daarmee om te gaan.
1,1	Eindgebruikers van IT systemen kennen de gevaren van de cyber omgeving niet.
1,1	Phishing is een belangrijk probleem voor onze organisatie.
1,1	Veel werknemers in een organisatie betekent een grote kans op een cyber incident, omdat niet iedereen zich aan de regels houdt.
1,1	Social engineering is een groot gevaar voor onze cyber veiligheid.
1,1	Veilig gedrag versloft.
1,1	Wij scannen onze medewerkers uitvoerig, een medewerker die kwaad in de zin heeft is erg gevaarlijk.
1,1	Een gevaar dat onvoldoende aandacht heeft is het gevaar van boze/ontevreden medewerkers met toegang tot gevoelige data en systemen.
1,1	Onder de werknemers heerst het gevoel dat de regels op cyber security gebied niet voor hen geldt.
1,1	Het cyber security beleid wordt niet door iedere werknemer nageleefd.
1,1	USB-stickjes die door werknemers gevonden worden of meegenomen worden en hier gebruikt worden is een reëel gevaar.
1,1	Medewerkers die kwaad in de zin hebben zijn een groot gevaar voor de internet cyber veiligheid van de organisatie.
1,2	Hackers focussen zich voornamelijk op applicaties op een individuele computer.
1,2	Dat nieuwe technologieën telkens nieuwe cyber gevaren met zich meenemen is een onderschat gevaar.
1,2	Verouderde software is een groot risico voor de cyber security.
1,2	Onbereikbaarheid van onze diensten door technisch falen of een cyber aanval heeft grote gevolgen.
1,2	Een aanval op ons netwerk behoort tot een reëel risico.
1,2	Een succesvolle Distributed Denial of Service aanval is funest voor onze bereikbaarheid.
1,2	Beperken van fysieke toegang heeft net zoveel met cyber security te maken als een firewall.
1,2	Social engineering wordt steeds geavanceerder en vraagt daarom awareness op alle niveaus binnen de organisatie.
1,2	Ook ransom-ware maakt graag gebruik van zwakheden in verouderde software.

1,2	Software moet volgens bepaalde veiligheidsstandaarden geprogrammeerd worden. Als dat niet gebeurd kunnen er eenvoudig te kraken lekken in de software aanwezig zijn.
1,2	Een lek in onze technische beveiliging kan betekenen dat een hacker ongeautoriseerd toegang tot data krijgt, dat moet voorkomen worden
1,2	DDoS aanvallen op de IT infrastructuur kunnen de voor ons belangrijke continuïteit beschaden, dat zou schadelijk zijn voor onze business
1,3	Top management verschilt van mening met IT-management op het gebied van cyber security, dat is een gevaarlijke barrière.
1,3	De top van het bedrijf onderschat het gevaar van cyber risico's.
1,3	Werknemers houden zich onvoldoende aan de cyber security maatregelen en procedures.
1,3	De cyber security procedures en organisatorische maatregelen binnen onze organisatie zijn niet voldoende uitgewerkt.
1,3	Top management heeft geen zicht op de cyber incidenten die zijn voorgevallen.
1,3	Cyber security te vaak gezien als alleen een IT-probleem. Het gaat juist ook over governance, leiderschap, cultuur, bewustzijn, gedrag en fysieke veiligheid. Dat wordt vaak vergeten.
1,3	Als cyber security faalt in een organisatie, zal het de organisatie ook aantasten als dat al niet is gebeurd
1,3	Cyber risico en security moet begrijpelijker worden gemaakt voor top management.
1,3	De raad van bestuur zou meer aandacht moeten hebben voor Cyber security.
1,3	De veiligheidsdoelstellingen en business doelstellingen komen niet overeen
1,3	Cyber security moet behandeld worden als elk ander risico
1,3	management weet onvoldoende over cyber security
1,3	Er zouden ook tests op het gebied van performance, acceptatie testen, keten testen en doet een review op documentatie, daar kunnen eventuele risico's in schuilen
1,3	Er vindt geregeld een audit plaats die onze organisatorisch beveiligingsprocessen doormeet en checkt op fouten of tekortkomingen.
1,4	Dat onze services onbereikbaar zijn door een fysieke externe oorzaak, zoals het uitvallen van het Internet, is een serieus gevaar. Wij moeten een hoge uptime hebben.
1,4	Cyber security moet net als elk ander belangrijk risico, zoals brand of stroomuitval, worden behandeld
1,4	Wij hebben het risico op stroomuitval afgedekt, wij kunnen de continuïteit van onze diensten garanderen
1,4	Software van derden kan een cyber risico opleveren, omdat je nauwelijks kunt controleren of er geen lek in zit
1,4	Als het internet langdurig zou uitvallen, hebben we een enorm probleem
1,4	leveranciers en andere derde partijen kunnen door hun eigen slechte/matige cyber veiligheid een serieus risico voor onze cyber veiligheid vormen
1,4	Onze organisatie stelt duidelijke veiligheidseisen aan de software die wordt gebouwd of wordt ingekocht bij andere partijen. Die software kan namelijk ook lekken bevatten
2,1	De reputatie van de organisatie is het belangrijkste, cyber risico zoveel moet zoveel mogelijk gemeden worden.
2,1	Reputatieschade is desastreus voor onze organisatie.
2,1	Een deel van het Internet blokkeren is een goed middel om de cyber veiligheid te verhogen.
2,1	Compleet vermijden van alle cyber gerelateerde risico's is niet mogelijk voor een organisatie.
2,1	Een aantal IT systemen loskoppelen van het Internet is een goede manier om een deel van cyber risico's te vermijden.

2,1	het voorkomen van een cyber aanval is beter dan er van te genezen.
2,1	Compleet vermijden van cyber risico is niet mogelijk, gedeeltelijk risico vermijden wel en is wenselijk.
2,1	Risico vermijden kan op sub-domeinen, zoals bij een financiële transactie het 4-ogen principe toepassen.
2,1	Compleet vermijden van de cyber risico's zou betekenen dat er ook geen voordelen van het Internet benut kunnen worden.
2,1	Risico kan vermeden worden door bijvoorbeeld meerdere datacentra te gebruiken, of een deel van het Internet te blokkeren.
2,1	Een organisatie moet cyber risico zoveel mogelijk vermijden, bijvoorbeeld door alle data die niet opgeslagen hoeft te worden ook niet op te slaan.
2,2	Onze organisatie is niet interessant voor een cyber aanval van buiten.
2,2	Er zijn andere organisaties dan wij, die interessanter zijn om cyber aanvallen op uit te voeren.
2,2	De cyber beveiliging van een organisatie kan nooit 100% waterdicht zijn. Er blijft altijd een klein risico over, dat is acceptabel.
2,2	Wij hebben genoeg maatregelen genomen, het restrisico is verwaarloosbaar.
2,2	Er is altijd een trade-off om je te beschermen tegen risico, je kunt economisch niet verantwoorden alles af te dekken.
2,2	Een organisatie hoeft zicht niet te beschermen tegen cyber risico's waarvan een organisatie denkt die risico's niet tegen te komen.
2,2	Er is een mogelijkheid dat een cyber risico kan worden geaccepteerd, als de kosten van beveiliging hoger zijn dan de mogelijke impact van het risico. Het is altijd een weloverwogen beslissing.
2,2	Je kunt risico's niet accepteren als het ook immateriële schade veroorzaakt, imagoschade moet ten alle tijden worden vermeden
2,2	Cyber risico's accepteren is niet mogelijk als er wettelijk wordt verplicht om bepaalde gegevens en infrastructuren te beschermen.
2,3	Het continue kunnen verbeteren van de cyber veiligheid, impliceert dat het cyber risico zich ook continue ontwikkeld
2,3	De top van het management weet wat er tegen cyber aanvallen gedaan moet worden
2,3	Het is niet voldoende om alleen preventieve maatregelen te treffen tegen cyber aanvallen
2,3	Cyber security is gelijk aan onze core business
2,3	In onze organisatie werken wij met verschillende autorisatieniveaus voor medewerkers
2,3	Cyber security zou onderdeel moeten zijn van het primaire bedrijfsproces
2,3	Bewustzijn bij hoger management zorgt voor betere cyber security
2,3	Het begin van een goede cyber security is bewustzijn bij top management
2,3	Tegenwoordig is bijna elk bedrijf een IT bedrijf, daarbij hoort ook de cyber beveiliging van een IT bedrijf
2,3	Wij laten onze organisatie geregeld testen op nieuwe lekken, daarbij wisselen we in bedrijven om de veiligheid in de tests te verhogen
2,3	Er worden geregeld tests gedaan om te kijken of onze organisatie nog wel bestand is tegen de nieuwste technieken om in te breken
2,4	Voor onze organisatie is een verzekering afsluiten pas een optie als er claims worden ingediend in het geval van een cyber aanval in de sector.
2,4	Verzekeren is alleen een optie als je niet alle benodigde expertise in huis hebt en het opweegt tegen de kosten.
2,4	Verzekeren heeft geen nut, het is te laat en dan is de (cyber) schade al geleden.
2,4	Verzekeren is alleen nuttig als het vanuit economisch oogpunt iets oplevert.

2,4	Of een verzekering interessant is hangt af van wat er verzekerd en wat het kan opleveren. Over het algemeen is het onduidelijk wat een cyber verzekering inhoud.
2,4	Gezien de stijgende cyber risico's kan een goede risico management strategie niet zonder verzekering.
2,4	Verzekeren is niet interessant voor ons, wij regelen alles zelf. Van risico assessment tot incident management.
2,4	Verzekeren is altijd een puur economische overweging, waarbij de mogelijke impact wordt afgewogen tegen de kosten die nodig zijn om tegen het risico te beschermen.
2,4	Verzekeringen zijn niet nodig: De kans dat iemand door onze cyber beveiliging is klein en een premie kost geld, economisch levert het niets op.
2,4	Het is niet duidelijk wat een cyber security verzekering inhoudt en wat een verzekering mogelijk kan opleveren.
2,4	Verzekeraars kunnen organisaties helpen met het risico management op het gebied van cyber risico, aangezien ze veel kennis hebben van het gebied waarin ze verzekeren.
2,4	Door een kortingsincentive in cyber verzekeringen kunnen verzekeraars zorgen voor een betere algemene cyber security
3,1	Er moeten geregeld cyber security tests op de IT systemen worden uitgevoerd om de veiligheid verder te waarborgen.
3,1	Monitoren van het netwerkverkeer is essentieel om eventuele aanvallen snel te detecteren.
3,1	De digitale systemen zouden redundant of vaker uitgevoerd moeten worden om de continuïteit van de service te waarborgen.
3,1	ISO 27001 is een achterhaalde standaard, het gaat niet meer om alleen een technische benadering van cyber security.
3,1	Totale cyber security kan het beste tot stand komen door technologisch alles dicht te timmeren.
3,1	Het netwerk moet geregeld getest worden op lekken en oneffenheden.
3,1	Stroomstoringen zouden geen probleem moeten zijn voor organisaties die veel met data werken, een eigen back-up stroomvoorziening is een must.
3,1	Het is belangrijk een DDoS aanval te kunnen weerstaan
3,1	Intrusion detection speelt een belangrijke rol in onze cyber beveiliging.
3,1	Cyber veiligheid wordt op dit moment vooral gefaciliteerd door technologische oplossingen.
3,1	Als een technisch (cyber) beveiligingssysteem officieel is gecertificeerd is het daarna ook helemaal veilig.
3,1	Om het netwerkverkeer goed in de gaten te houden kan het bijvoorbeeld via een centrale server lopen die het verkeer monitort.
3,1	Verlies van data is te omzeilen met een goede back-up van je belangrijke bestanden en goede up-to-date software
3,1	Versleuteling is nodig om belangrijke data alleen voor degenen die je toestemming geeft leesbaar te maken.
3,1	Het grootste deel van de beveiligingsmaatregelen zouden op technisch vlak moeten zijn.
3,1	Onze organisatie heeft genoeg technische cyber veiligheidsmaatregelen en is daarom goed beveiligd op het gebied van cyber security
3,1	Elke organisatie moet infrastructuren hebben om DDoS aanvallen af te slaan, continuïteit is erg belangrijk.
3,2	Gebruikers informeren over cyber gevaren en hoe daarmee om te gaan via nieuwsbrief/mail is voldoende om awareness te verhogen.
3,2	Awareness en onderwijs over cyber risk is ten dele maar een oplossing.
3,2	Cyber security awareness training moet verplicht zijn voor elke werknemer in een organisatie.
3,2	Het versturen van een nieuwsbrief is alleen een extra middel om mensen bewust te maken van cyber security.
3,2	Als werknemers de protocollen en procedures betreffende cyber security correct opvolgen, is dat voldoende om menselijke fouten te beperken.
3,2	Alle werknemers moeten verplicht op een e-learning cursus om de awareness te verhogen.

3,2	Er worden artikelen op het intranet gepubliceerd over cyber security zodat de awareness zal stijgen.
3,2	Elke werknemer moet weten hoe hij een incident kan herkennen en hoe er vervolgens gehandeld moet worden om het op te lossen.
3,2	Beperk de autorisaties op technische mogelijkheden van gebruikers die geen expertise over IT of cyber security hebben.
3,3	Iedere organisatie zou zich moeten laten certificeren op cyber veiligheidsmaatregelen.
3,3	Certificeren is een realistisch doel om cyber security proportionele aandacht te geven.
3,3	Wachtwoorden moeten aan strenge eisen voldoen om de veiligheid te waarborgen.
3,3	Cyber Incident Response plannen (een plan hoe te reageren op een cyber incident) moeten onderdeel zijn van business units, niet alleen van IT
3,3	Een cyber incident control afdeling die weet wat er moet gebeuren in het geval van een cyber aanval moet een onderdeel van een organisatie zijn.
3,3	Alleen technische maatregelen zijn al lang niet meer genoeg om beveiligd te zijn.
3,3	Cyber security moet zichtbaarheid in een corporate boardroom hebben.
3,3	Organisaties moeten beveiliging voor gebruikers makkelijker maken.
3,3	Het melden van (cyber) security incidenten moet gestimuleerd worden.
3,3	Cyber security awareness moet worden geïntegreerd in vaste processen, zo ben je niet meer afhankelijk van individuele awareness.
3,3	De kennis om alles wat cyber security te managen betreft moet binnen de gelederen van een organisatie zijn.
3,3	Management is verantwoordelijk voor het invoeren van cyber security maatregelen.
3,3	Management krijgt elk security incident te weten.
3,3	Veiligheid moet verweven zijn met de core business van een organisatie om optimale veiligheid te bereiken.
3,3	in onze organisatie leeft iedereen de veiligheidsvoorschriften na.
3,3	Organisaties kunnen tegenwoordig niet zonder een integrale cyber securitybenadering, cyber security moet door de hele organisatie verweven zijn.
3,3	In onze organisatie is een veiligheidscultuur waarin mensen elkaar aanspreken op dingen die cyber gevaren kunnen veroorzaken, zoals een computer die niet gelockt is.
3,3	De organisatorische processen worden uitvoerig gemonitord, zo kunnen we zien of er wat fout gaat bij het rapporteren of uitvoeren van veiligheidsprocedures.
3,3	Voor elk cyber scenario dat er mogelijk is, zelfs de onwaarschijnlijke, moeten uitgebreide procedures opgesteld zijn.
3,4	Als wij de cyber veiligheid niet kunnen waarborgen is een financieel risico in de vorm van boetes reëel
3,4	Medewerkers in onze organisatie moeten een geheimhoudingsverklaring ondertekenen om het risico op menselijk lekken te beperken.
3,4	Maatregelen voor een zeker niveau van cyber veiligheid zijn wettelijk verplicht voor bepaalde organisaties. Ik neem deze maatregelen alleen omdat ze verplicht zijn.
3,4	Een geheimhoudingscontract is een goede manier om menselijk lekken te beperken.
3,4	CBP moet zich focussen op het reduceren van lekken, niet op het maximaliseren van aantal gemelde lekken.
3,4	Wetgeving is niet nodig om een acceptabel niveau van cyber security te creëren.
3,4	Meldingsplicht zal mede een maatschappelijke gedragsverandering veroorzaken, bijvoorbeeld dat overheidsorganisatie en bedrijf hun ICT beter gaan beveiligen.
3,4	De overheid doet niet genoeg om cybercrime tegen te gaan.
3,4	Door wettelijke eisen aan cyber beveiliging / meldplicht datalekken kan het bedrijfsleven effectiever door de overheid worden geholpen.

3,4	Er zijn duidelijke eisen aan de veiligheid van IT systemen binnen onze organisatie.
3,4	Buitenlandse wetgeving heeft invloed op onze cyber security maatregelen.
3,4	Er moet wettelijk toezicht zijn op onze cyber veiligheid en continuïteit door diverse officiële rijksoverheid instanties die daarop ook controleren.
3,4	Het is nodig om cyber security met werknemers en derde partijen vast te leggen in contracten. Contracten die ingaan op veiligheidseisen die door de relevante partijen getroffen moeten worden.
4	Security is per definitie ook cyber security
4	Cyber security awareness houdt alleen in dat cyber gevaren worden herkend
4	Bewustzijn van de cyber gevaren door gebruikers is voldoende om je te beschermen
4	Cyber security awareness moet constant up-to-date worden gehouden, er zijn steeds nieuwe gevaren. Je bent dus nooit helemaal aware.
4	Security training helpt aan het verhogen van de veiligheid, de mens is immers de zwakste schakel.
4	Aware ben je als je kennis hebt van de cyber risico's, hoe daar mee om te gaan en als je daar naar handelt.
4	Cyber security awareness is het bewustzijn van de risico's in de online wereld.
4	Fysieke gevaren als een open deur kunnen ook cyber gevaren opleveren en moeten daarom ook meegenomen worden in awareness programma’s.
4	Awareness is het bewustzijn van gevaren, aangezien gevaren zich ontwikkelen moet je de kennis voortdurend updaten.
4,1	Doel van awareness is bewustzijn over gevaren te creeren en hoe daarmee om te gaan.
4,1	Doel van awareness is verhoogde cyber veiligheid.
4,2	Medewerkers moeten gestimuleerd worden om elkaars cyber veiligheidsincidenten te melden.
4,2	Cyber security zou niet alleen een op IT gericht moeten zijn, maar door de hele organisatie verweven. Fysieke toegang tot bijvoorbeeld een computer kan ook cyber risico opleveren.
4,2	Sterk en zichtbaar commitment moet van het top management worden vereist, om succesvolle implementatie van cyber security mogelijk te maken.
4,2	Bewustzijn bij hoger management zorgt voor implementatie van training en educatie programma's.
4,2	Alleen top management kan starten met het invoeren van beveiligingsmaatregelen en procedures.
4,2	Een vooraanstaand persoon in een organisatie moet het goede voorbeeld geven in cyber veiligheid.
4,2	Onderkennen van het nut van cyber beveiliging geeft minder weerstand in invoering en gebruik.
4,2	Cyber veiligheid verhogen tot een acceptabel niveau kost te veel geld.
4,2	Management support is belangrijk om cyber security awareness in een organisatie te verbeteren.
4,2	Cyber security is gebaat bij het vrijmaken van budgetten op organisatie niveau.
4,2	Cyber beveiliging gebeurd vanuit puur economische redenen.
4,2	Goede cyber security is erg duur.
4,2	Cyber security brengt stijgende kosten en dalende efficientie met zich mee, er moet dus genoeg geld beschikbaar zijn.
4,2	De voordelen van Cyber security zijn moelijk te meten.

4,2	Er moet veel budget beschikbaar zijn om de cyber veiligheid awareness te verhogen.
4,2	Om cyber security awareness te creeren is er een geld nodig om trainingen en educatie te faciliteren.
4,2	IT faciliteiten die belangrijk zijn voor de bedrijfsvoering worden beter beschermd dan applicaties die dat niet zijn.
4,2	Cyber security awareness moet geintegreerd worden in vaste bedrijfsprocessen, zo kan je er niet meer omheen.
4,3	Alle gebruikers van IT systemen in een organisatie moeten cyber security aware zijn ten behoeve van de cyber security.
4,3	Cyber security wordt afgeschoven op de IT afdeling. Van deze afdeling is het vereist cyber security aware te zijn, overige werknemers zijn daar vrij in.
4,3	Ik ben niet de juiste persoon om over de cyber veiligheid te oordelen.
4,3	IT-personeel hoeft niet te weten wat de gebruiker doet.
4,3	Top management is niet voldoende op de hoogte van de cyber gevaren.
4,3	Corporate boardrooms hebben cyberbeveiliging bovendien onvoldoende op het netvlies en negeren problemen.
4,3	Voor een goede cyberveiligheid in een organisatie is een aparte afdeling of aparte functie nodig die cyber security aware zijn. Voorbeelden zijn: Cyber security officer of een cyber security afdeling.
4,3	In elk board of directors of management team moet een security officer zitten die cyber security aware is. Alleen op deze manier wordt de cyber veiligheid gegarandeerd.
4,3	Security moet een eigen officer/manager krijgen om het goed te implementeren.
4,3	Het cyber security bewustzijn is bij de top van het management best wel hoog.
4,3	De afdeling die over cyber security gaat heeft erg korte lijntjes met de top van het management, dat is ook noodzakelijk.
4,3	Top management wordt alleen bij cyber security betrokken als er een incident is dat de imago van de organisatie mogelijk kan schaden
4,3	Kleine incidenten kunnen ook onder collega's onderling worden afgedaan.
4,3	Management hoeft niet op de hoogte te zijn van cyber gevaren en oplossingen, zolang de relevante stakeholders zoals cyber security officers dat maar zijn.
4,4	Voor mij is het niet helemaal duidelijk wat het belang van cyber security awareness precies is.
4,4	Technologisch is onze cyber security op orde, nu de mensen nog.
4,4	De mens is de zwakste schakel in de veiligheidsketen, cyber security awareness kan daar gedeeltelijk een oplossing voor zijn.
4,4	Gebruiksvriendelijkheid van beveiligingssoftware en cyber veiligheid sluiten elkaar uit.
4,4	Gebruiksvriendelijkheid en veiligheid sluiten elkaar niet uit, de meeste beveiligingssoftware is gebruiksvriendelijk.
4,4	Mensen in een organisatie zijn het grootste gevaar voor cyber security, daarom alles gefocust zijn op het verhogen van de cyber security.

Appendix I: Absolute scores of Q-sorts per factor

The absolute scores of the Q-sorts of the factors regarding the typology in Chapter 2. An absolute score means the sum of absolute rankings according to the Q-sort of the relevant factor. The typology is categorized in Chapter 4 step 2. In this categorization statements are divided into groups; for example, risk of human actions is level 1, category 1. All categories are presented in the tables below. The only deviating category is 4.4 in the table, which presents the extra personal statement category for the managers.

Factor I	Cat 1	Cat 2	Cat 3	Cat 4
Level 1	4	6	7	3
Level 2	3	5	1	5
Level 3	9	6	8	4
Level 4	8	11	8	12

Factor II	Cat 1	Cat 2	Cat 3	Cat 4
Level 1	3	4	8	5
Level 2	7	5	2	11
Level 3	9	7	6	10
Level 4	8	4	10	1

Factor III	Cat 1	Cat 2	Cat 3	Cat 4
Level 1	5	6	7	5
Level 2	7	9	2	3
Level 3	11	6	7	5
Level 4	11	5	6	5

Factor IV	Cat 1	Cat 2	Cat 3	Cat 4
Level 1	2	12	3	6
Level 2	7	5	3	7
Level 3	12	5	10	7
Level 4	2	6	6	7

Appendix J: Z-scores

		Factor			
	Statements	I	II	III	IV
1	Our organization is well protected against cyber risks.	-1,47	-0,08	0,49	-0,55
2	IT is very important in our organization.	1,92	0,46	1,35	1,95
3	My cyber security awareness is high enough.	-1,20	0,28	0,05	-0,55
4	The end user does hardly know anything about cyber risks and he does not know anything about dealing with the risks.	1,18	-0,44	-0,72	-0,48
5	Many employees in a big organization implies a high chance on a cyber incident, because not everybody is compliant to the rules.	0,32	-0,33	0,49	-0,49
6	A risk that has insufficient attention is the risk of unsatisfied employees that have access to sensitive data and systems.	0,30	-0,26	0,71	-0,26
7	An underestimated risk is the risk of new technologies that cause new cyber risks.	0,50	0,50	0,35	0,68
8	Outdated software is a big risk for cyber security.	0,03	1,15	0,58	1,96
9	Unavailability of our services due to technical failure or cyber attack has huge consequences.	1,55	0,07	1,43	2,29
10	Top management underestimates the cyber risks.	0,66	-0,35	-1,19	-0,28
11	Cyber security policies and procedures in our organization are not sufficiently developed.	1,36	-0,59	-0,61	0,32
12	Cyber security is seen as IT only problem too often. It is also about governance, leadership, culture, awareness and behaviours. Which are often forgotten.	0,64	2,07	1,24	0,79
13	Unavailability of our services due to external events like flooding, fire or Internet disruption is serious. We need to have a high level of up time.	0,98	-0,91	1,18	1,51
14	Suppliers and other third parties can be a serious risk for our organisation, due to their own bad/insufficient cyber security.	0,28	0,86	0,96	0,90
15	Uncoupling several IT systems is a good way to avoid a part of the cyber risks.	-0,09	-0,56	-0,79	0,56
16	It is better to prevent suffering from cyber attacks than to recover from cyber attacks.	0,93	1,34	1,16	1,65
17	An organization has to avoid risk as much as possible, for example do not save personal data that is not necessary to save.	-0,17	0,75	-1,25	0,27
18	An organization's cyber security cannot be 100% safe. There is always residual risk, which is acceptable.	1,47	0,08	1,76	0,40
19	Organizations do not have to protect against risks, which never will be encountered.	-0,57	-0,87	-0,70	-1,09
20	There is a possibility that cyber risks can be accepted, when the costs of securing are higher than the possible impact.	0,20	-1,12	1,34	-0,43
21	Nowadays almost every organization is an IT company, which implies every organization has to reduce risk by taking cyber security measures equal to an IT company.	-0,37	0,66	-0,82	1,12
22	Cyber insurance is useless; the (cyber) damage already had its impact.	-0,73	-1,78	-0,45	-0,42
23	Cyber insurance is not needed. The premiums are high and the chance on breach in our cyber security low. It is economical not interesting.	-0,91	-1,89	-0,53	-0,99

24	The role of insurances in cyber security and risk management is unclear to me.	0,33	-0,49	0,36	-0,05
25	Insurers can help organizations with cyber risk management; insurers have a lot of knowledge in the fields they insure.	-0,46	0,33	-0,61	-1,50
26	IT systems in cyber security should be tested regularly to foster the safety.	1,32	0,74	0,57	0,93
27	Total cyber security can best be reached through technological means.	-0,96	-1,23	-1,69	-1,44
28	When technical means are certified, they can be perceived as totally safe.	-1,62	-1,86	-1,89	-1,78
29	It is sufficient to raise cyber security awareness of employees by informing the employees by newsletter or mail on the topic of cyber risks and how to deal with the risk.	-1,38	-1,13	-1,69	-1,03
30	Cyber security awareness training has to be mandatory for every employee in an organization.	-0,76	0,66	0,08	-0,61
31	When employees comply with the policies and procedures regarding cyber security, sufficient mitigation of human errors is reached.	0,23	-0,63	-0,94	-0,23
32	The knowledge to manage all aspects of cyber security should be present in the company itself.	-1,19	0,24	-0,28	-1,10
33	Organizations cannot without integral cyber security approach; cyber security has to be throughout the whole organization.	0,16	1,57	1,45	0,74
34	For every cyber scenario that is possible, even the unlikely ones, there have to be extensive procedures.	-1,85	0,32	-1,09	-1,64
35	Some cyber security measures are mandatory by law. That they are mandatory is also the only reason they are taken.	-0,89	-1,45	-1,28	-1,57
36	Legislation is not necessary to achieve an acceptable level of cyber security.	-0,76	-1,10	0,41	-0,79
37	It is necessary to define cyber security in contracts with employees and third parties. Contracts that define cyber security measures that have to be taken by the relevant parties.	0,00	1,12	0,21	0,42
38	Employees have to be stimulated to report each other's' cyber incidents.	0,87	0,54	0,53	0,18
39	Management support is important to increase the cyber security awareness in an organization.	0,73	0,66	1,74	0,51
40	Much budget has to be available to improve the cyber security awareness in an organization.	-1,16	-0,32	-0,74	-0,30
41	Cyber security awareness has to be formally integrated in business processes. In this way, no one can ignore security awareness.	0,64	1,48	0,70	-0,05
42	All users of IT systems in an organization have to be cyber security aware for the purpose of cyber security.	0,82	1,56	0,09	1,05
43	Cyber security is pushed off to the IT department; which is undesirable.	0,57	-0,14	0,36	0,15
44	For good cyber security in an organization a separate department or function needs to be cyber security aware. For example, a cyber security officer or a cyber security department.	-1,20	0,16	-0,21	-0,31
45	In every board of directors or management, team there has to be a security officer, which is cyber security aware. Only then, cyber security is guaranteed.	-1,90	0,07	-1,46	-0,55
46	For me it is not clear what the use of cyber security awareness is.	-0,73	-1,96	-1,19	-1,04

47	The human is the weakest link in cyber security; cyber security awareness can be a partial solution for that.	1,37	0,44	0,97	1,02
48	People in an organization are the biggest risk, which is why everything has to be focussed on increasing cyber security awareness of users.	1,01	1,37	-0,44	0,12