Building blocks for a cyber security strategy

This research provides insight into how corporate organizations can develop a well-thought cyber security strategy given a cyber security ambition that supports the organization's general ambition. Literature is researched, interviews are conducted, and national cyber security strategy documents are analyzed.

Linda Peursum

August 16th, 2015

Version 1.0

Universiteit Utrecht

Author

Linda Peursum

Student master Business Informatics

3698645

Utrecht University

1st supervisor: Floris Bex

2nd supervisor: Jan Martijn van der Werf

Deloitte

Daily supervisor: Joram de Leeuw van Weenen

Amsterdam, August 2015

Preface

Finally… the last thing I have to write in my thesis is this preface. The last nine months I worked very hard on this thesis and it really opened my eyes about cyber security. My idea of cyber security was shaped by what I saw in the news, which meant always reading about prestigious companies being hacked and how many personal data was stolen. I always thought 'wow, it would be so cool to hack someone!', which funny enough meant that I actually really want to hack my twin sister's laptop (which is by the way still on my bucket list).

However, back to reality. Cyber security deals with so much more than hacking. During the period I wrote my thesis I learned a lot about cyber security and how important it is for organizations to protect themselves from cyber-attacks. So hereby I present to you my thesis about how corporate organizations can develop a cyber security strategy to be more resilient to an emerging threat landscape.

I could not have performed this research without the help of certain people. First, I would like to give my thanks to all the experts who participated in this research. Furthermore, I would like to thank my first supervisor Floris Bex for his useful guidance and feedback during the process of creating this thesis. And especially, for showing me how to write a more fun-to-read thesis. In addition, I would like to thank Jan Martijn van der Werf for reviewing my thesis and giving clear, usable feedback.

I got the opportunity to write my thesis at Deloitte where I really enjoyed working with all these nice and inspiring people. I would especially like to give gratitude to my daily supervisor at Deloitte, Joram de Leeuw van Weenen. I would like to thank him for the time and effort he put into supervising me with my research. He helped me a lot and gave very good constructive feedback to optimize my thesis.

Also, I would like to thank my father for explaining certain cyber security related things in 'teletubbietaal' and my mom for buying me all those chocolate bars. And finally, everyone else who has been my shoulder to cry on during this exciting and stressful time.

Enjoy reading!

Linda Peursum
Amsterdam, August 2015

Abstract

In the past decades, innovative technologies in a rapidly changing environment together with larger and more complex IT landscapes have created a challenge for companies to keep their information security and cyber security up to speed. Internal vulnerabilities can cause cyber criminals to breach into the systems or workstations and infringe the confidentiality, integrity, and availability of data and information. Meanwhile data is one of the most valuable assets of an organization which needs protection against threats from cyberspace.

We have evidence that, in order to adequately protect critical assets of an organization against attacks from cyberspace, it is of importance to have a structured approach to handle cybersecurity, i.e. a strategy. In addition, we assume that this cyber security strategy, developed for corporate organization, should be in line with a cyber security ambition and support the organization's strategy. Therefore, this research aims at developing a structured method to create a well-thought cyber security strategy based on a cyber security ambition that supports the organization's goals.

While there are many approaches to create a business strategy, we know little about how strategy is created in the cyber security domain. In order to explicate the steps necessary to come to a well-thought cyber security strategy, we reviewed existing literature in different domains (i.e. the business, military, and game theory domain), analyzed thirty-one national cyber security strategy documents from across the world, and conducted fifteen interviews with experts in the field to gain a full and diverse understanding of strategy creation. This qualitative approach resulted in a conceptual method for the creation of a cyber security strategy. To provide completeness and correctness of the developed method it was by seventeen experts in the field of cyber security and by comparing it against a real cyber security strategy of a corporate organization.

The results from these three approaches and validation resulted in a four-step approach to create a cyber security strategy. But before creating a cyber security strategy, one should take note of the following constraints:

- Without buy-in from the management board, one should not create a strategy;
- The cyber security strategy should be part of, aligned with, and support the business strategy. No exceptions;
- The cyber security strategy should be evaluated yearly (or more frequently) and renewed every three years;
- Stakeholders should be involved early in the process of creating a cyber security strategy;
- The outcomes of every step and the previous steps should be reviewed after the completion of this step;
- After completion of creating a cyber security strategy, the process of executing the roadmap should be formalized (e.g. in the form of indicating next steps).

The following four-step approach was derived from this research (for more information, see chapter 9):

1. Identify the need for a cyber security strategy and determine the cyber security ambition;
2. Define the cyber security strategy operating setup;
3. Analyze the landscape;
4. Describe multiple strategic objectives and associated activities.

Each step consists of several sub activities which are specific for creating a strategy in the cyber security field. The next page shows a quick reference card with all high-level steps and related low-level activities.

The Building Blocks of a Cyber Security Strategy: A Quick Reference Card

1. Identify the need for a cyber security strategy and determine the ambition

1.1. Consider a changing environment

1.2. Consider what strategy and controls already in place

1.3. Consider regulatory requirements

If there is a need, continue. If not, stop.

1.4. Define the scope of the cyber security strategy

1.5. Determine the cyber security ambition

1.6. Optional: determine cyber security visions per domain the cyber security ambition applies to

1.7. Define guiding principles of the cyber security strategy

1.8. Define desired outcomes of the cyber security strategy

2. Define the cyber security strategy operating setup

2.1. Determine and invite stakeholders for requirements setting

2.2. Set up definitions to use within the cyber security strategy regarding cyber security

2.3. Define the governance of the cyber security strategy

2.4. Define strategy dependencies

2.5. Describe desired interaction with key stakeholders

3. Analyze the landscape

3.1. Analyze the social, external, and internal landscape

3.2. Evaluate landscape analysis with stakeholders and adjust if necessary

3.3. Perform a gap analysis (by using a framework or performing a risk analysis)

3.4. Determine and prioritize the gap

3.5. Evaluate gap analysis with stakeholders and adjust if necessary

3.6. Define problem areas based on the landscape and gaps found

4. Describe multiple strategic objectives and associated activities

4.1. Perform a brainstorm session with stakeholders to communicate problem areas and decide on multiple strategic objectives (directions)

4.2. Evaluate results of brainstorm session and adjust if necessary

4.3. Define the business case for every strategic objective

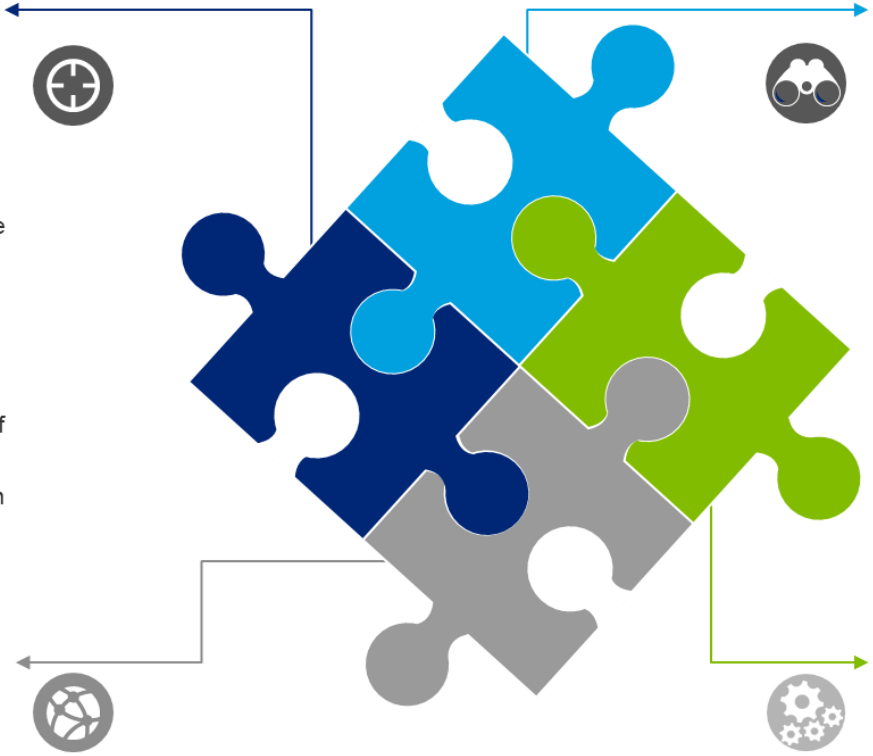
4.4. Determine high-level activities and associated options for every strategic objective

4.5. Elaborate on the high-level activities

4.6. Prioritize strategic objectives with stakeholders

4.7. Let the management board choose ultimate course of action

4.8. Describe the effect of the strategy on the organization



Glossary

Critical asset

"Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances, and reputation" (ISACA, 2014)

Cyber security

"Cyber security deals with both information based assets stored or transmitted using ICT and non-information based assets that are vulnerable to threats via ICT" (von Solms & van Niekerk, 2013)

Cyber security ambition

A certain goal or aim: something an organization wants to do or achieve with cyber security[6]

Cyber security strategy

"The direction and scope of an organization with cyber security over the long term, which achieves advantage in a changing environment through its configuration of resources and competences with the aim of fulfilling stakeholder expectations (Johnson et al., 2008)

Cyber threat landscape

The threats via cyberspace an organization is facing.

Environment

The internal and external surroundings of the organization of interest.

External environment

The external environment consists of elements that exist outside the organization that are hard to control, but do influence the organization in different ways.

Incident

"Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service" (ISACA, 2014).

Internal environment

The internal environment deals with all elements that exist within the organization.

Laws & regulations

(a system of) Rules that must be followed, induced by an authority.

Mission

A declaration of an organization's 'reason for being'" (David, 1989)

Risk

"A function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" (NIST, 2012)

Risk appetite

"The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission" (ISACA, 2014).

Roadmap

An implementation plan.

Security control

"A means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature" (ISACA, 2014)

Social environment

"The social environment encompass the immediate physical surroundings, social relationships, and cultural milieus within which defined groups of people function and interact"[7].

Stakeholder

"People or small groups with the power to respond to, negotiate with, and change the strategic future of the organization" (Eden & Ackermann, 1998, p. 117).

Strategic objective

"A broadly defined, measurable objective that an organization must achieve to make its strategy succeed"[8].

Threat

"Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service (NIST, 2012)".

Vulnerability

"A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events" (ISACA, 2014).

Table of contents

List of tables

List of figures

1 Introduction

1.1 Research trigger

In the past decades, innovative technologies in a rapidly changing environment together with larger and more complex IT landscapes have created a challenge for companies to keep their information security up to speed (Adomavicius, Bockstedt, Gupta, & Kauffman, 2008; Deloitte, 2011). Internal vulnerabilities can cause cyber criminals to breach into systems or workstations and infringe the confidentiality, integrity, and availability of data and information[1].

Data is currently one of the most valuable assets of organizations[2]. Given certain types of organizations, the most important data possessed differs. For example, the banking and finance industry deals with customer, company and market specific data with regard to their finances, and the most significant detected incident is financial fraud (PwC, 2014). Another example is public agencies, where data about citizens is highly sensitive. Unauthorized access or use of data, systems, and networks counts for a quarter of all detected incidents in this industry. Healthcare organizations store critical information about their patients, and three out of six most significant detected incidents is about stolen customer data. In the information & telecom industry services are offered and the availability of these services is important. It is therefore not a surprise that the two most significant detected incidents in telecom concerns making applications unavailable or denial of service attacks. And finally, insurance companies also store a lot of confidential data about customers. However, financial losses is the most detected incident among insurance companies (PwC, 2014). In 2014, "1.500 data breaches led to one billion data records comprised worldwide"; a 78% increase compared to 2013 (Gemalto, 2015) .

Given the importance of data and severity of some incidents, organizations should aspire and maintain a high level of cyber security to address their most relevant threats that endanger their most valuable data. Cyber security deals with both information and non-information based assets that are vulnerable via cyberspace (von Solms & van Niekerk, 2013). In the last five years, there has been an exponential growth in the amount of cyber security breaches at companies (Verizon, 2014). Several reasons for the increased number of breaches are cloud computing, bring your own device, the lack of sufficient awareness amongst employees, and the increased interconnection of critical systems (Byres & Lowe, 2004; Deloitte, 2011, 2013; Verizon, 2014).

Organizations cannot be 100% safe from cyber-attacks. Although prevention is a step that must be undertaken, many more measures are necessary to prevent a cyber-attack (Deloitte, 2013). One should focus on either decreasing or eliminating the threat, vulnerability, and/or consequence to minimize the probability and impact of a cyber-attack. Threats can be eliminated by preventing threat actors to act, vulnerabilities can be prevented by hardening targets, and consequences can be deterred or prevented by focusing on minimizing the impact of an attack (Chabinsky, 2010). To tackle this in a structured, and well-thought manner, a cyber security strategy is necessary.

1.2 Problem statement

The number of information technologies available for organizations are overwhelming and as such, the controllability of cyber security also becomes a real challenge. In addition, the rapidly changing environment and

[1] http://www.law.cornell.edu/uscode/text/44/3542 consulted on 9-12-2014

[2] http://datacentremanagement.com/news/view/securing-your-organisationas-most-valuable-asset , consulted on 9-12-2014

the amount of security breaches cannot be adequately addressed by the current organization of cyber security in an organization (Deloitte, 2013; PwC, 2014). With new evolving technologies and the professionalization of the field of cyber security (e.g. better and more sophisticated tools are used by adversaries and the knowledge and skills of adversaries have become more advanced), organizations are less flexible in handling such a rapidly changing world. 72% of companies have 'outdated and overly restrictive approaches to information security', hindering performance (CEB, 2013). The relevance of this research is to help organizations create and align a cyber security strategy with their business ambition in order to dynamically respond to changes in the IT and threat landscape and to adequately address these changes.

Currently, there are indications that most organizations do not strategically invest in cyber security nor align this strategy with their business goals or ambitions (PwC, 2014). Also, there is a 'continuing lack of understanding regarding the strategic importance of managing information security' (McFadzean, Ezingeard, & Birchall, 2007). As such, a need for a formal, structured method exists (Adomavicius et al., 2008) to help organizations strategize their cyber security in order to adequately address and maintain current and future threats and corporate ambitions. But more importantly, the rationale of an organization's willingness to strategize cyber security and the actual strategy is a key factor in, ultimately, determining the effectiveness of the implementation of a cyber security strategy and carrying out the cyber security ambition. Doing this right can give an organization a competitive advantage (McFadzean et al., 2007).

To summarize, the problem is fourfold:

- The controllability of cyber security becomes a challenge due to the growing IT landscape;
- The growing amount of security breaches and the severity of these breaches;
- There is no alignment between the business strategy and the cyber strategy;
- There is no 'good' investment in a sound cyber security strategy.

The problem statement is therefore as follows: "Currently, most organizations do not strategically invest in cyber security nor align this strategy with their business goals, or ambitions. In addition, the rapidly changing IT environment and threat landscape cannot be adequately addressed by current cyber security capabilities in an organization. "

1.3 Scope

Since the number of organizations facing cyber security is very large (one could say that nowadays every organization is vulnerable), this research focuses on corporate organizations (e.g. enterprises which employ more than 1000 employees) and how they manage their cyber security ambitions, risks, threats, etc. Small- and medium enterprises, as well as public organizations, are left out of scope, as corporate organizations are more likely to be a victim of cybercrime. In addition, the focus is on cyber security, instead of the more overall information security field. Here cyber security deals with both information based assets stored or transmitted using ICT and non-information based assets that are vulnerable to threats via ICT (von Solms & van Niekerk, 2013).

In this research, a framework is presented that discusses the presence of threats and cyber security ambitions. Besides, tools are given in order for corporate organizations to tackle a specific step in the developed method. However, specific threats and ambitions are not studied nor all possible threats and ambitions.

1.4 Relevance

1.4.1 Scientific relevance

A scan through scientific literature regarding cyber security ambitions and strategies revealed that not much research has been done in this field. Although strategic methods do exist, they only exist in different scientific fields and not in the cyber security field.

This research complements the scientific community by developing a method to develop a cyber security strategy based on the cyber security ambition, which aligns with the organization's ambition and strategy. In addition, the reasoning process behind the cyber security ambition and strategy gives practitioners new insights in the thoughts of experts concerning this subject. The originality of the cyber security strategy process method lies in its application in a rather new, and evolving field. This application cannot be found in scientific literature.

1.4.2 Social relevance

The amount of security breaches has grown extensively in the last years (Verizon, 2014), and these have not gone unnoticed by companies. Damage to the reputation of a company by not being able to deliver a service (e.g. banks that face DDoS attacks) is a well-known consequence of security breaches. Other social costs to breaches (Grant Thornton, 2011) include amongst others: lag the pace of innovation, victimization costs, crime prevention, changes in human behavior, cost of over insurance, and job losses.

In addition, financial costs to this problem also grow (Figure 1). The average loss per incident from the unauthorized access to information has become six times as large and the loss from the theft of proprietary information has doubled since 2004 (Dorantes, 2006). The average cost of the loss of a data record is $170, but is at least $100 more expensive when it is data from the healthcare or education industry (Ponemon, 2015). Taken into account that these industries mostly rely on customer data, i.e. privacy sensitive data, it is of importance to protect this data. Not only from the citizens' point of view, who does not want his/her personal data in the wrong hands, but also from a company's point of view, which does not want any reputation or financial loss due to comprised data. In order to reduce the amount of security breaches and its impact, it is necessary that companies develop a (proactive) strategic approach to this problem (Deloitte, 2013).

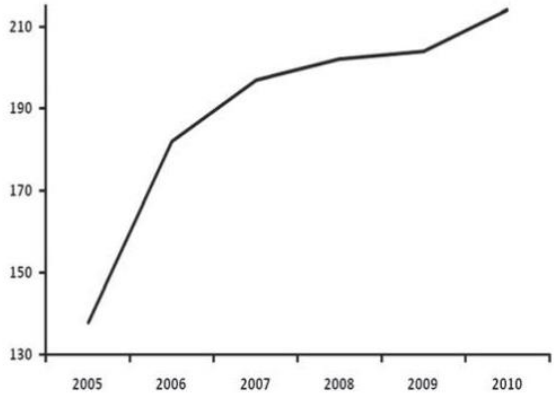


FIGURE 1: ANNUAL CHANGES IN OVERALL COSTS OF DATA BRACHES PER UNIT (US) (WALL, 2010)

1.5 Structure

To counteract the problems found in this chapter, we have conducted a research. This research is presented in the following chapters, were first the research questions (chapter 2) are presented. Next, the research approach (chapter 3) is discussed. Subsequently, an introduction to cyber security (chapter 4) is given and how to go from a vision and ambition to a strategy (chapter 5). Then, strategy creation from different perspectives (chapter 6) is discussed. Based on this, a conceptual method (chapter 7) is presented. This conceptual method is validated and these results are discussed (chapter 8) next. Finally, the final building blocks of a cyber security strategy (chapter 9), a discussion (chapter 10) and conclusion (chapter 11) are presented.

2 Research questions

2.1 Main research question

As described in chapter 1, there exists a need for a formal, structured strategy, created by following a number of detailed steps, that aligns with the cyber security ambition, corporate ambition, and corporate strategy. Figure 2 shows the relationship between these concepts. But before a strategic method can be developed, one needs to know why organizations want a certain direction with their cyber security management.

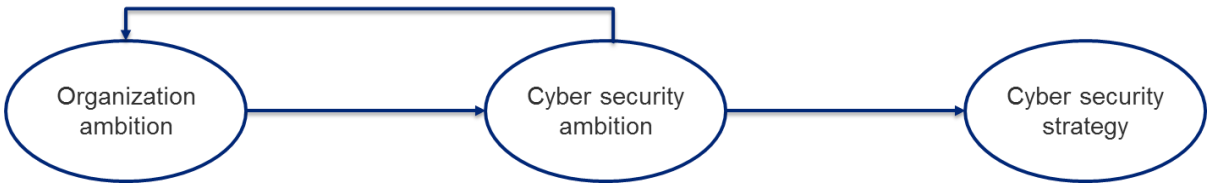


FIGURE 2: RELATION BETWEEN ORGANIZATIONAL AMBITION, CYBER SECURITY AMBITION AND CYBER SECURITY STRATEGY (RESEARCH INTENTIONS)

As such, the main research question is:

Main Research Question

How can a corporate organization develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition?

We assume that there always is an organization ambition. However, we also assume that there is not always a cyber security ambition or a cyber security strategy. This assumption is based on practical insights in the field, and is the basis of this research.

The fact that an organization wants to, for example, mature or excel in their cyber security management is usually incorporated into the organization's ambition, or more specifically, in the cyber security ambition. A cyber security ambition is composed to reduce, retain, avoid, or transfer (ISO27005) risks that organizations face. These risks may cause a threat to the confidentiality, integrity, or availability of information- and non-information based assets that are vulnerable via cyberspace.

The specific rationale of the cyber security ambition is also of importance: why do organizations have or want such an ambition? And why do they choose certain goals within this ambition? Why do they want to, for example, excel at cyber security? How do they compose their ambition and, in a further stage, their strategy based on this ambition? These are important questions to consider before making the move to actualize the ambition, by implementing security controls to mature an organization or reduce, retain, avoid or transfer risks (i.e. the strategy).

The concepts of the above stated research question are defined as follows:

- Cyber security deals with to both information based assets stored or transmitted using ICT and non-information based assets that are vulnerable to threats via cyberspace (von Solms & van Niekerk, 2013).

- A cyber security strategy's objective is "the establishment of a process driven organization with stable and efficient operations" (Mueller & Kuehn, 2013);
- An ambition is a particular goal an organization has.

This research gives more insight into the link between the organizational ambition and cyber security ambition, and how a cyber security strategy is composed. By combining these aspects, organizations should be able to make more informed decisions about their cyber security, and the associated actions involved. The goal of the research is to develop a cyber security strategy process, e.g. a method to come from a cyber security ambition to a cyber security strategy.

2.2 Sub questions

In order to answer the main research question, several sub question have to be answered. These sub questions cover the concepts posed in the main research question.

2.2.1 Sub question 1

The first sub question is:

What drives a cyber security strategy for corporate organizations?

First of all, it is necessary to assess why it is exactly that corporate organizations want or need a cyber security strategy. Diverse reasons are possible and these should support an organization's decision to develop a cyber security strategy. A list of most common drivers mentioned by experts and literature is listed as a result.

2.2.2 Sub question 2

The second sub question is:

How and to what extent are an organization's ambition and a cyber security ambition related?

This question elaborates on the relationship between an organization's ambition and a cyber security ambition, as illustrated in Figure 2. Besides this relationship, we also assume that cyber security related ambitions and strategies as an organization should put forth one vision to adhere to as a whole. The exact relationships between these concepts are proven by looking at literature and expert opinions, and are outlined in a separate section.

2.2.3 Sub question 3

Next, in different domains within organizations, strategies are developed (e.g. corporate strategy, human resource strategy, IT strategy). The general elements included in these strategies might give rise to what should be included in a cyber security strategy, and therefore what should be thought of when composing this strategy. Therefore, the third sub question is:

Which elements are included in a strategy?

This also provides an answer to what exactly a strategy is and results in a table where strategic elements found in literature are categorized into usable categories for our method.

2.2.4 Sub question 4

The fourth sub question is:

Which cyber security elements are of importance for a cyber security strategy (to be successful)?

This question dives deeper into sub question three with the context of cyber security in mind. There are different elements within cyber security which should be assessed to fully cover the cyber security domain in a strategy. This includes an analysis of current practical models to assess the common cyber security elements. In addition, input from experts and cyber security strategies are of importance. These analysis results in a table, likewise as in the previous sub question, where cyber security elements are sub divided into categories which are used in further analysis.

2.3 Relation sub questions to main question

All four sub questions are necessary to answer the main research question. First, with the main research question we assume that you should have a cyber security strategy, but is this true? The first sub question researches this. Without a need for a cyber security strategy, the main research question is not relevant at all to research. Therefore, we wish to find out what the rationale behind a cyber security strategy is. In addition, we also assumed in Figure 2 that there is a relationship between the organization's ambition, the cyber security ambition, and the cyber security strategy. We aim to prove this relationship with sub question two, which is also present in the main research question. Furthermore, because we want to know how corporate organizations can develop a cyber security strategy, it seems logical to look into existing methods to create a cyber security strategy. However, this are almost non-existent. Therefore, we look at other domains for strategic models and elements with sub question three. And finally, with sub question four we look for alternative methods to get more insight into the cyber security perspective of strategy creation.

3 Research approach

3.1 Research method

The normative research we conduct consists, first of all, of a literature review. The literature review is performed by using a snowballing technique where references within articles are further explored available on the internet or intranet. Also, current strategy processes or methods, from different domains, are researched.

In addition, expert interviews are held with security strategy experts to gain more insight in the strategy processes used in practice (in addition to what is found in the literature and current models). These experts are gathered through the network of Deloitte and others or via open channels. And finally, we look at real cyber security strategy documents to see if we can deduce a method for creating this document.

Combining this information results in the creation of an own conceptual method. This method is validated using a real case to compare our method with the one used in practice, and by having a workshop session with experts in the field of cyber security. Feedback from these validations is used to update the model.

This approach resembles the technology transfer model by Gorschek, Wohlin, Garre & Larsson (2006), where a problem is seen in an industry. The problem is then defined and studied on an academic level. The created candidate solution is both validated in academia and in practice. Finally, a practical solution is provided to the industry. Figure 3 shows how the technology transfer model relates to our research method as described above. Only the validation in academia is not present because there are no scientific resources available related to the creation of a cyber security strategy method which we can compare our method with.

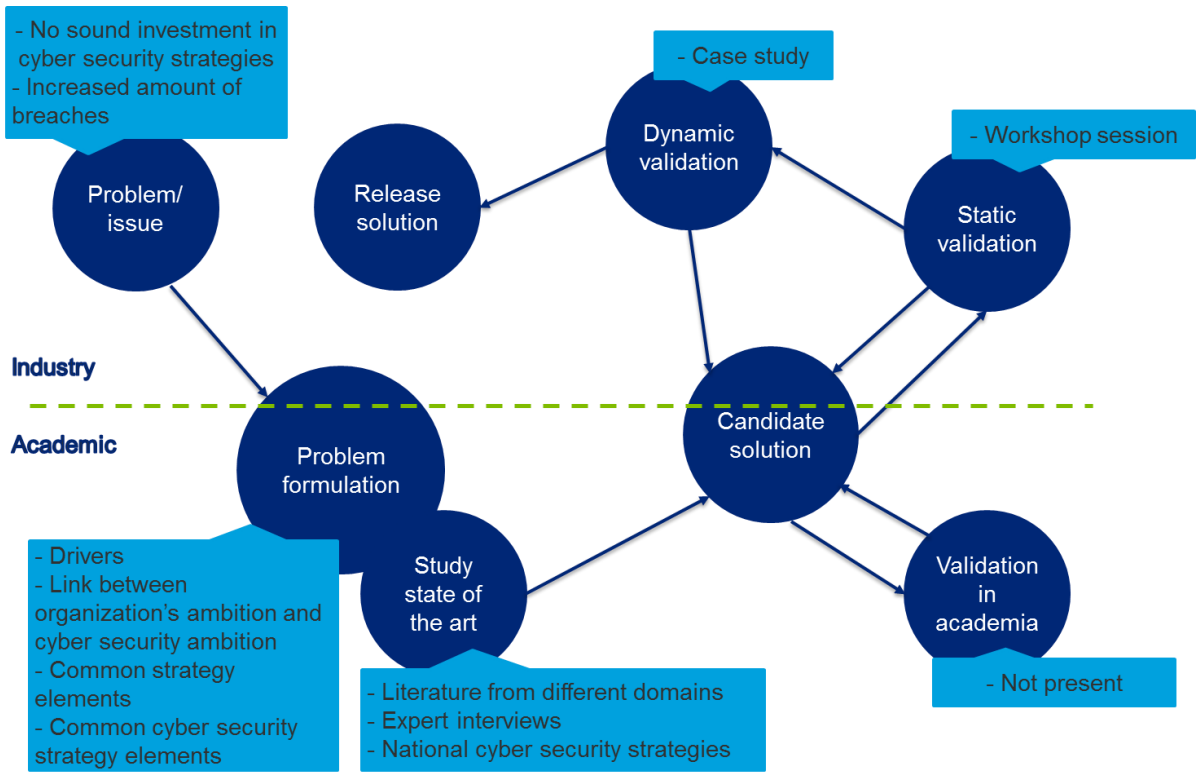


FIGURE 3: THE TECHNOLOGY TRANSFER MODEL APPLIED TO OUR RESEARCH

3.2 Research design

Since there is not much scientific literature regarding cyber security ambitions and strategies, a method is constructed to close this gap. To design and develop such a method, the guidelines for design science in information systems research by Hevner, March, Park, and Ram (2004) is used. The design science is composed of seven guidelines, listed in Table 1. Design-science requires that an artifact is created (guideline 1) to solve a certain problem (guideline 2), which is thoroughly evaluated by the researcher (guideline 3). This artifact should contribute to science by offering a more effective or efficient way of solving a problem (guideline 4). In addition, the construction and evaluation of the artifact should be based upon rigorous methods (guideline 5). Moreover, to construct the artifact, a search process is (guideline 6) needed whereby a problem space is constructed (Hevner et al., 2004). Lastly, the results of the design-science should be able to be communicated to both technical and non-technical audiences (guideline 7). This means that our research method is tailored in a way that we comply with the guidelines of Hevner et al. (2004).

TABLE 1: DESIGN-SCIENCE RESEARCH GUIDELINES APPLIED TO OUR RESEARCH (FROM HEVNER ET AL., (2004))

Guideline	Description	Our research
Guideline 1: Design as an Artifact	Design-science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.	We aim to develop a method to create a cyber security strategy for corporate organizations.
Guideline 2: Problem Relevance	The objective of design-science research is to develop technology-based solutions to important and relevant business problems.	In this research we develop a solution (however, not technology-based) to important and relevant business problems as indicated in chapter 1.
Guideline 3: Design Evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.	The method developed is evaluated twice. First, a workshop session is held with experts in the field of cyber security who give feedback on the method. Second, the method is evaluated by comparing it with a real-life cyber security strategy of a corporate organization.
Guideline 4: Research Contributions	Effective design-science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.	The method we create extends the body of knowledge about strategy creation and specifically in the field of cyber security. In addition, it helps corporate organizations to be more resilient to an emerging threat landscape and a well-thought cyber security strategy adds value to the organization.
Guideline 5: Research Rigor	Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.	For the construction of the method we use triangulation, by using literature, conducting expert interviews, and assessing national cyber security strategies. In addition, validation is done by means of a workshop session and case study.
Guideline 6: Design as a Search Process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.	The search for an effective method is done in the literature, via experts, and in national cyber security strategies. As far as we know, there are no laws in the problem environment that must be satisfied.
Guideline 7: Communication of Research	Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.	The created method is presented to technology-oriented audiences via a process-deliverable diagram. The method is presented to management-oriented audiences in plain text.

In this research, the artifact to be designed is a method to develop a cyber security strategy based on a cyber security ambition, while supporting the organization's ambition. The problem's relevance was discussed in section 1.4. In addition, the design evaluation is discussed in chapter 8. The research contributions are discussed in chapter 10. The research rigor and search process are discussed in chapter 3. Lastly, the results of the research are communicated to both technical and non-technical audiences in a final presentation (see chapter 7, 9, and 11).

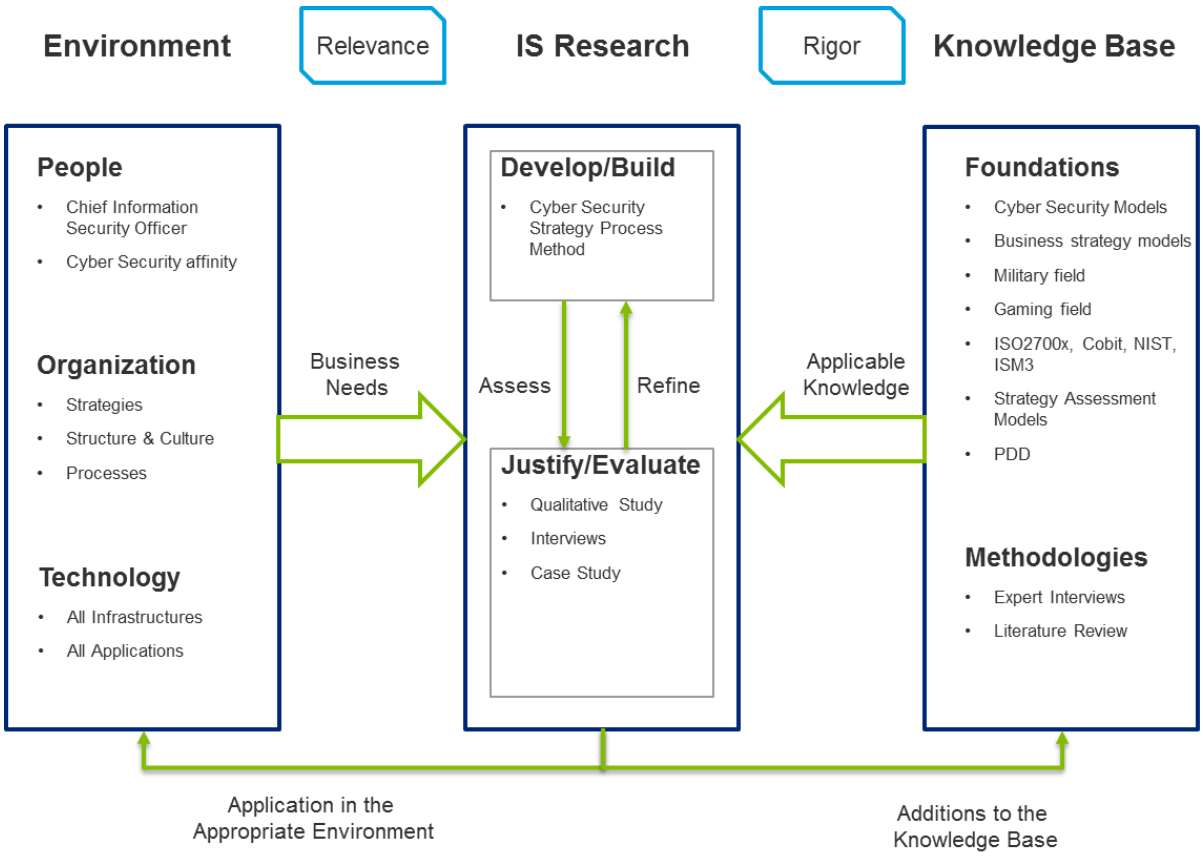


FIGURE 4: CYBER SECURITY STRATEGY RESEARCH FRAMEWORK

Figure 4 illustrates the Information Systems Research Framework by Hevner et al. (2004) adjusted to the research topic presented in this document. This framework helps to define and scope the research. First of all, the environment defines the problem space (Hevner et al., 2004), which consists of people, organization and technology. In the case of method to construct a cyber security strategy, the people that are involved in this research are Chief Information Security Officers or other strategy related employees of corporate organizations with a cyber security affinity. The method takes strategies in mind across the organization, structure & culture, and processes. In addition, all infrastructures and applications are taken into account when creating the method. The created cyber security strategy process method is justified based on a qualitative study (e.g. literature study and interviews) and evaluated by means of a focus group with experts and a case study at a corporate organization. The rigor of the method can be found in the usage of grounded strategy assessment models like the BCG matrix (Hedley, 1977), the 7-S framework of McKinsey (Waterman, Peters, & Phillips, 1980), and Porter's five forces (Porter, 1979).

3.2.1 The literature review

There are two ways to perform a literature review, structured and unstructured (or random). A structured literature review is a "form of secondary study that uses a well-defined methodology to identify, analyze, and interpret all

available evidence related to a specific research question in a way that is unbiased and (to a degree) repeatable" (Kitchenham & Charters, 2007). A structured literature review offers the advantage of looking at useful literature in a structured way, so that most useless literature is quickly excluded. However, a quick scan through relevant literature revealed that not much literature is available and therefore a systematic literature review is not effective since more specific searches are needed than just one. Therefore, we perform an unstructured literature review, meaning that we search through literature by using different terms and by using the snowballing technique.

The search engine that is used to search for literature is Google Scholar. Subscriptions of Utrecht University is used to gain access to journals and other databases. Google Scholar is a hub that incorporates all scientific papers from scientific journals. It is therefore not necessary to look for another search engine, such as the ACM library.

The results from a search are first screened on the basis of the title and abstract. Only those articles that are considered relevant enough, and are available (i.e. meaning a PDF is available), are read in full-text. Notes and annotations are used in Mendeley (reference manager) to easily track articles and their subjects. The results from the unstructured literature review are presented throughout chapters 0, 0, and 0.

In addition, we use these articles to further search for relevant papers, i.e. the snowballing technique. Snowballing refers to the approach where one seeks for other relevant scientific literature in the references of already found interesting literature. In addition, casual searches (not systematic) are carried out when certain information is needed.

3.2.2 A cross-border analysis of national cyber security strategies

In order to get more insight into how strategies are created in the cyber security domain, we ought to look at real cyber security strategies from corporate organization. However, no cyber security strategies from corporate organizations could be found online. These documents could give indirect insights in the elements that are important in creating a cyber security strategy. However, due to the transparent nature of public organizations, and their social responsibility towards citizens, it is not surprising that in the public domain cyber security strategies are generally published. Besides, citizens are one of the most important stakeholders in governmental cyber security strategies. Therefore these published strategies are a good basis for the understanding of a cyber security strategy. This understanding can create a basis for discussion about cyber security strategy in corporate organizations. By analyzing the strategy documents on content, and identifying what is generally described (e.g. strategic objectives, cyber threat landscape for a specific country), one can externalize the critical factors taken into account when constructing a security strategy and what steps were followed.

A search was performed via Google, by using the search term 'cyber security strategy'. With this search, two hubs for national cyber security strategies were found, namely the website of ENISA[3] and the website of the NATO Cooperative Cyber Defense Centre of Excellence[4]. Scanning through these sites resulted in 31 adequate national cyber security strategies, meaning that they fulfilled the inclusion criteria. The national security strategies were included when:

- they would discuss the topic of either information security or cyber security;
- the strategy is published in Dutch or English;
- a PDF version is available;
- the strategy document is final.

[3] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world , consulted on 17-02-2015
[4] https://ccdcoe.org/strategies-policies.html , consulted on 17-02-2015

The national cyber security strategies that were excluded from the analysis are listed in Table 2.

TABLE 2: EXCLUDED NATIONAL CYBER SECURITY STRATEGIES

Country	Exclusion criteria
India	Only a draft version (notification) is available
Luxembourg	Only published in French
Malaysia	Only a summary is available
Romania	Only published in Romanian
Russia	Only available in plain HTML
Rwanda	Only a draft version is available
South Africa	Only a draft version is available

The goal of the analysis is to deduce the critical factors taken into account when constructing these national cyber security strategies. By analyzing what is discussed, one can translate this back to what is thought of when creating the strategy document. This was done by highlighting all important aspects that are discussed in the strategy documents. In this case, it did not matter what the exact directions are or content is of a certain section. Only the general content, like the fact that in section 1 strategic drivers were discussed, matters.

The analysis resulted in 48 unique concepts that were grouped into 6 general steps, when it became apparent that this would provide additional information. During the grouping process, the concepts were organized based on their logical connection and on the order distilled from the strategy documents.

3.2.3 Interviews

Expert interviews were necessary because of limited literature available about the creation of a cyber security strategy. Due to the explorative nature of the interviews, questions were asked in a semi-structured manner. At first, specific questions are posed to the interviewee, but later on, questions may vary between interviews. In addition, other questions are asked to evoke additional information from the interviewee.

Due to limited time and resources, participants are chosen on the basis of purposive sampling. Purposive sampling is a non-probability based sampling method and is especially effective when experts are needed to be interviewed in a certain domain (Flick, 2009; Tongco, 2007). Participants are selected based on two criteria: their function and their knowledge about creating a (cyber) security strategy. Consultants in the field of cyber security and Chief Information Security Officer (CISO) were considered as suitable interviewees in order to gain answers and insights into the methods used to create a cyber security ambition and strategy. However, it was needed that these potential interviewees were familiar with creating a (cyber) security ambition or strategy.

Every interviewee was sent the questions up front. The interview existed of four questions about ambition and six questions about strategy. Before the formal questions were posed, interviewees were given a definition of cyber security ambition and strategy. During the interview the following definitions were used:

- An ambition is “a certain goal or aim: something an organization hopes to do or achieve”;
- A strategy is “a plan, method, or series of maneuvers or stratagems for obtaining a specific goal or result”.

The interviewees were asked whether they agreed with this definition. This was necessary so that every interviewee had the same understanding of these definitions and there was little chance of misunderstandings.

Table 3 shows the selected participants for the qualitative research. Fifteen interviews were held with security officers and consultants. However, two of those interviews were held in the beginning of the process to gain background information about the subject and to assess the feasibility of the study.

Every interviewee was sent the questions up front. The interview existed of four questions about ambition and six questions about strategy. Before the formal questions were posed, interviewees were given a definition of cyber security ambition and strategy. During the interview the following definitions were used:

- An ambition is “a certain goal or aim: something an organization hopes to do or achieve”[5];
- A strategy is “a plan, method, or series of maneuvers or stratagems for obtaining a specific goal or result[6]”.

The interviewees were asked whether they agreed with this definition. This was necessary so that every interviewee had the same understanding of these definitions and there was little chance of misunderstandings.

Table 3: Selected participants for the qualitative research

	Role	Sector or industries	Via list?
Expert 1	Information security officer	Public sector	Yes
Expert 2	Consultant	Insurance sector, public sector, computer industry	Yes
Expert 3	Security officer	Public sector	Yes
Expert 4	Consultant / ex-information security officer	Electronics industry, transport industry	Yes
Expert 5	Consultant / ex-CISO	Transport industry, defense industry, energy industry	Yes
Expert 6	CISO / ex-consultant	Financial industry	Yes
Expert 7	Security and policy advisor	Public sector	Yes
Expert 8	Risk officer	Financial industry	Yes
Expert 9	Consultant	Public sector, insurance sector	Yes
Expert 10	Consultant	Electronics	Yes
Expert 11	Consultant	Electronics	Yes
Expert 12	Consultant / ex-CISO	Public sector, financial industry	Yes
Expert 13	Security manager	Insurance sector	No
Expert 14	Consultant	Defense industry	No
Expert 15	Consultant	Electronics	No

All interviews were recorded and transcribed afterwards. These transcriptions can be found in the Appendix. All data gained from the interviews is analyzed with NVivo. NVivo is a qualitative analysis tool used to code data. The data is coded in nodes resembling the questions asked. After this first set of nodes, every node is coded again to identify categories and concepts in the data per question. This is a useful way to structure and to analyze interviews.

3.3 Method creation

The conceptual method is based upon the information found in the literature, national cyber security strategy documents, interviews, and own knowledge on the subject. The method is presented using a process-deliverable diagram (van de Weerd & Brinkkemper, 2008). This diagram combines an activity diagram and a class diagram, both UML standards. It is especially designed to link activities with concrete deliverables. During the creation of a cyber security strategy, the organization of interest should document all decisions. As such, a process deliverable diagram is perfectly suitable for presenting our method.

3.4 Validation method

The created method should also be validation to prove its scientific correctness and completeness. This is done by a workshop session with experts and by using case studies.

[5] http://www.merriam-webster.com/dictionary/ambition , consulted on 4-7-2015
[6] http://dictionary.reference.com/browse/strategy , consulted on 4-7-2015

The workshop session was held with 17 experts from the cyber and privacy advisory team of Deloitte. The experts were given a brief presentation of the conceptual method. In addition, plain text versions of the conceptual method were given. After the presentation, the experts were asked to form groups of 2 or 3 persons, resulting in 6 groups. This was done to stir up discussion about the presented method within the groups and afterwards between groups. Each group was given a form with two questions about the completeness, six questions about the correctness, and two questions about the acceptability of the conceptual method. Also, a question to discuss a certain topic was posed. The group of experts were asked to fill in the questions in a 30 minute time span. Due to this time limitation, every group was asked to start at a different set of questions. This is done because if time ran out, all questions were answered at least once. The full results of the workshop validation can be found in section 13.3.1.

In addition to a workshop session, one case study was performed. Case studies offer the advantages of (George & Bennett, 2004):

- potentially achieving high conceptual validity;
- having strong procedures for fostering new hypotheses;
- having value as a useful means to closely examine the hypothesized role of causal mechanisms in the context of individual cases;
- having the capacity for addressing causal complexity.

During the case study, the created method was used to assess if the cyber security strategy of the case company followed a likewise method. The network of Deloitte was used to select a case company. The results from the case studies are used to update and finalize the method. Unfortunately, due to time constraints, only one case study can be performed. In addition, confidential information in the cyber security strategy of the case organization is disclosed, no information about the case company is given except that it is a large, corporate, Dutch organization.

Based on this validation, the model is updated according to proposed moderations and additions.

4 Introduction to cyber security

Before we start to go into depth in order to answer the research question and sub questions as presented in chapter 1.5, we first give a short introduction about cyber security. In this chapter, cyber security in relation to information security is discussed. Furthermore, the concepts related to the field are discussed. And lastly, the cyber threat landscape is covered.

4.1 Information security vs. cyber security

Information security and cyber security are often used interchangeably. However, they do not indicate the exact same thing. It is important that the reader is on the same page as the writer while reading this research. Therefore, the difference between information security and cyber security is discussed.

While cyber security is related to protecting information and non-information based assets which are processed, stored, and transported via the internet (ISACA, 2014), information security takes a broader perspective by focusing on "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability". The key differences between these terms is the perspective of information and non-information, and access through the internet or other sources. Although some might refer to information security as an umbrella term for ICT security and cyber security, information security expands on the concepts of ICT security. And cyber security, in addition, expands on the concepts of information security (von Solms & van Niekerk, 2013). Figure 5 shows the relationship between information, ICT, and cyber security.

Information security deals with both analogue and digital information (von Solms & van Niekerk, 2013). For example, leaving a paper report at a printer can pose a threat to the confidentiality of the information stored in the report.

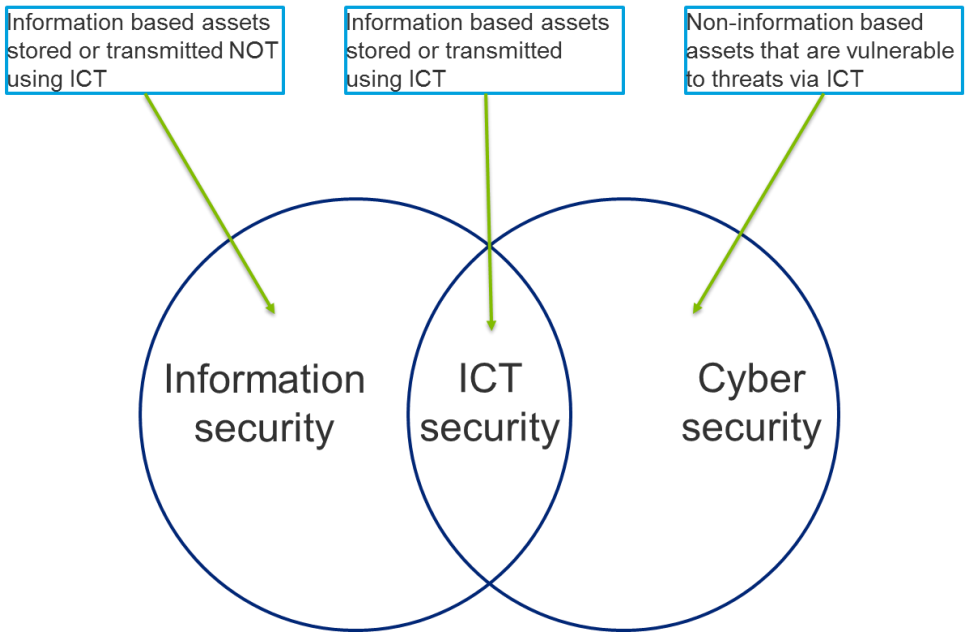


FIGURE 5: THE RELATION BETWEEN INFORMATION SECURITY, ICT SECURITY, AND CYBER SECURITY (von Solms & van Niekerk, 2013)

ICT security deals only with information based assets stored or transmitted using ICT, i.e. digital information. For example, passwords stolen by hackers can pose a threat to the integrity of the digital information. And lastly, cyber security deals with both information based assets stored or transmitted using ICT and non-information based assets that are vulnerable to threats via ICT (von Solms & van Niekerk, 2013). This means that also humans are an important factor in cyber security as they can be vulnerable for, for example, phishing mails. Cyber security is thus solely focused on threats from and happening in cyberspace. For example, the Stuxnet worm made use of the internet to attack Iran's nuclear centrifuges. Machines were not built with cyber security taken into mind. SCADA (Supervisory Control And Data Acquisition) systems, or simply said 'control systems' were therefore targeted via cyberspace by the Stuxnet worm.

Cyberspace is the "realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online" (Singer & Friedman, 2014). One of the key elements of cyberspace are humans, the people behind the computers and who connect to the internet. Cisco (2011) predicts that by 2020 there will be about 50 Billion of internet connected devices versus a population of 7.6 Billion people; the amount of devices connected to cyberspace is continuously growing and evolving.

4.2 Security concepts

With the growth of cyberspace, organizations need protection against threats from cyberspace. Every organization has valuable assets that are worth protecting against threat agents who wishes to damage or abuse the asset. They will do that by exploiting vulnerabilities that exist in the asset or the environment. Security controls can be imposed to reduce the number of vulnerabilities and thereby reducing risk to an acceptable level. Figure 6 shows the general concepts of information and cyber security which are used in the evaluation model of Common Criteria (1999).

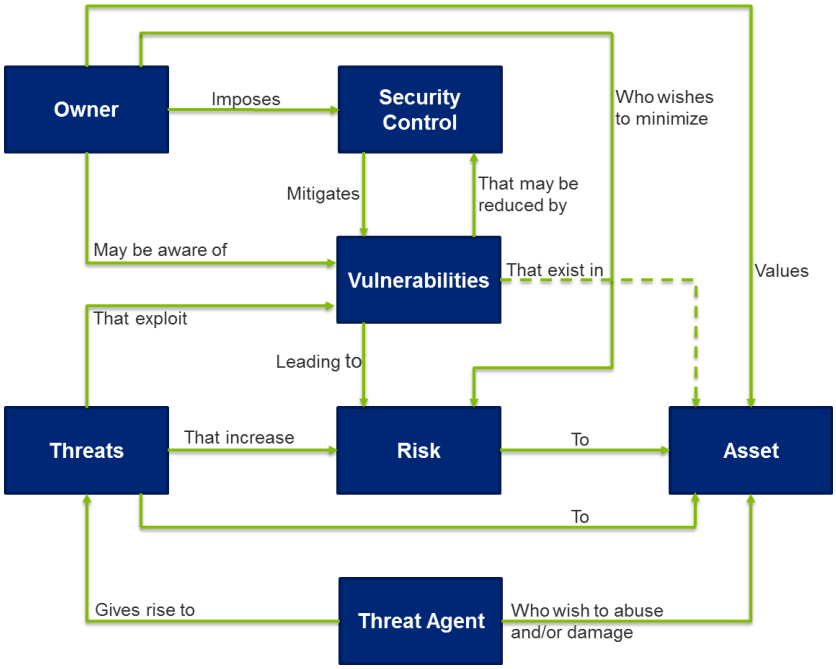


FIGURE 6: SECURITY COMPONENTS AND THEIR RELATIONSHIPS (EL AOUFI, 2009 ADAPTED FROM COMMON CRITERIA, 1999)

4.2.1 Owner

The owner of the asset values their asset and analyses possible threats. Based on this analysis, the owner imposes one or more security control(s) that mitigates vulnerabilities in order to minimize the risk of a threat occurring. The CobiT framework states that “if IT is to successfully deliver services to support the enterprise’s strategy, there should be a clear ownership and direction of requirements by the business (the customer) and a clear understanding of what needs to be delivered, and how, by IT (the provider)” (IT Governance Institute, 2007). This also accounts for security where information and non-information based assets need to be protected according to the owner’s wishes and needs. The owner of the asset is a stakeholder who has the most gain or loss in the information stored, processed or transmitted via the asset. All information assets should be managed at the organizational level according to the ISO 27001 standard (ISO, 2013).

4.2.2 Asset

The owner of the asset is responsible for valuing the assets on their confidentiality, integrity, and availability. An asset is defined as “something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances, and reputation” (ISACA, 2014). According to the ISO 27001 standard, information based and non-information based (physical) assets should be valued based on the information stored on, processed or transmitted via the asset (ISO, 2013). Security control can be imposed to protect assets.

4.2.3 Security control

Implementing security controls in order to comply with the cyber security strategy can be costly. It is therefore important that the owner of an asset imposes security controls based on a risk analysis (e.g. based on CIA) on the critical assets (Shimeall & Spring, 2014). A security control is “a means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature” (ISACA, 2014). In plain English, a security control is basically a countermeasure to reduce, retain, avoid, or transfer a security risk. A security control mitigates vulnerabilities in the organization.

4.2.4 Vulnerabilities

During an attack, threat agents wish to abuse and/or damage assets in a system. Therefore, a threat agent gives rise to threats that exploit vulnerabilities. A vulnerability is “a weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events” (ISACA, 2014). These vulnerabilities lead to certain risks. The information owner may be aware of these vulnerabilities and can impose a security control to handle the vulnerabilities. Factors contribution to the vulnerability of an asset are, as identified by OWASP (2014), the ease of discovery, ease of exploit, awareness, and intrusion detection.

4.2.5 Risk

Vulnerabilities in systems can cause threats to the confidentiality, integrity, and availability of data. There is a certain risk, where valuable data or information is lost, this might happen. According to the National Institute of Standards and Technology (NIST) a risk in the IT domain is “a function of the likelihood of a given threat-source’s exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization” (NIST, 2012). The accepted standard for measuring risks is done by calculating the likelihood of an event occurring *times* the impact on the business when the event occurs (Byres & Lowe, 2004).

The outcome of the formula can be mapped on a risk severity matrix, by using the likelihood and impact. Figure 7 illustrates a simple risk severity matrix. For instance, a DDoS attack has a medium likelihood for corporate banks and a high impact since the services will be unavailable for all its customers. This means that the severity is medium and action is needed (e.g. reduce, retain, avoid, or transfer risks).

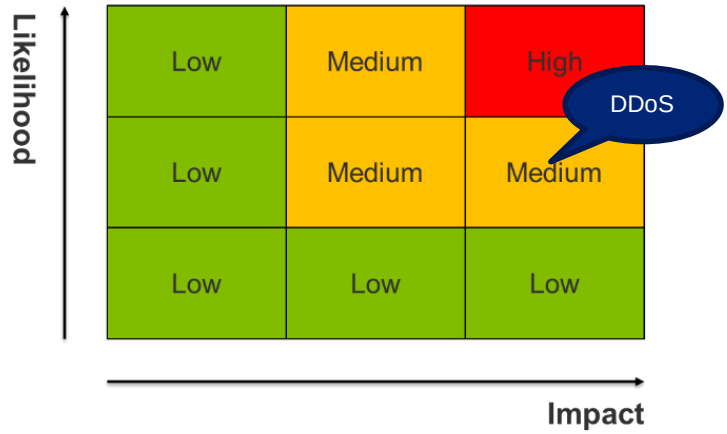


FIGURE 7: RISK SEVERITY MATRIX

In addition, the likelihood of a successful attack and the impact can be measured by different variables. For instance, Byres and Lowe (2004) suggest that the likelihood of a successful attack can be measured by the threat, vulnerabilities, and target attractiveness.

Another proposed risk assessment method is Mehari, which stands for Method for Harmonized Analysis of Risk, based on the ISO2700x standards and NIST's SP 800-30, to help manage the security of information, IT resources, and its associated risks (Mehari, 2010). Mehari's proposed risk assessment consists of four steps, namely:

1. Analyze the major stakes (analyze security stakes and dependencies of business processes to information);
2. Analyze the vulnerabilities (search for weaknesses and defects of current security measures);
3. Decrease and manage the risks (identify risks, evaluate risks, and reduce risks);
4. Monitor the security of information (define action plan, measure, and benchmark results).

Besides the general method from Byres and Lowe (2004) and the four step-method from (Mehari, 2010), OWASP (The Open Web Application Security Project) developed a practical, but more extensive risk assessment method, the OWASP Risk Rating Methodology. OWASP (2014) proposes a six step method, based on the general formula where risk is the function of the likelihood and the impact of an event. OWASP also proposes an extension of the general method of 'Risk is Impact x Likelihood' (see Figure 8). They measure the likelihood of an event occurring based on threat agent actors (e.g. size, skills, motive, and opportunity) and vulnerability factors (e.g. ease of discovery, ease of exploit, intrusion detection, and awareness). In addition, impact is measured by the technical impact (e.g. impact on the confidentiality, integrity, and availability (CIA) of information) and business impact (e.g. financial damage, reputation damage, non-compliance, and privacy violation).

A well-known concept within risk management is the risk appetite. A risk appetite is composed that indicates to what degree an organization accepts a certain risk per critical asset. Besides assessing the likelihood and impact of a risk, organizations also define a risk appetite for their organization's assets.

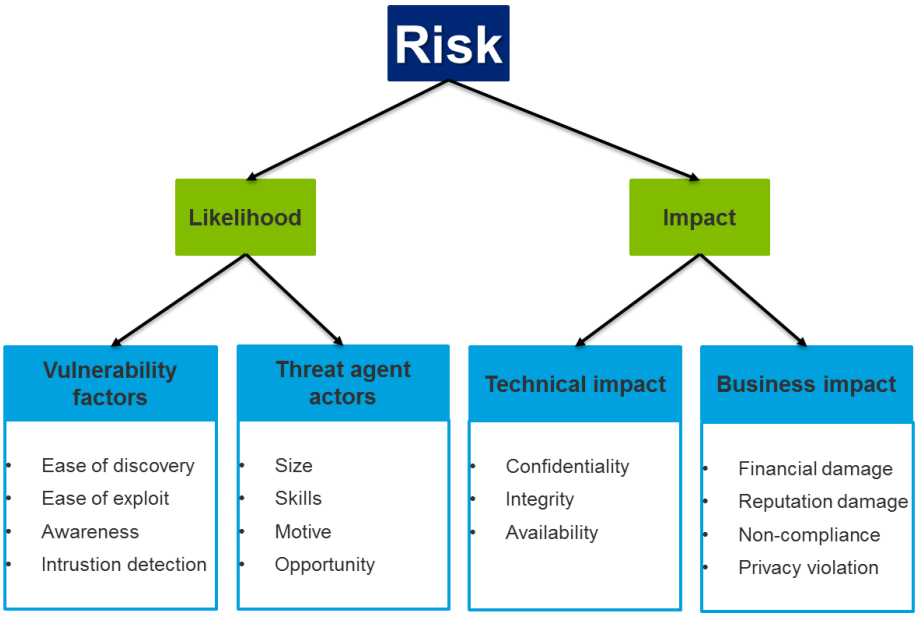


FIGURE 8: OWASP RISK RATING METHODOLOGY

4.2.6 Threat

Threats increases risks. A treat can be defined as “any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service” (NIST, 2012). A threat can cause the unauthorized disclosure, modification, removal or destruction of assets (ISO27002). In section 4.3, the current threat landscape is outlined as described in scientific literature. Threats are given rise to by threat agents.

4.2.7 Threat agents

A threat agent is “someone or something with decent capabilities, a clear intention or manifest a threat and a record of past activities in this regard” (ENISA, 2014). Several types of agents, identified by ENISA, can initiate an attack. On the one hand there are nation states who want to start electronic warfare by spying on other nation state, and on the other hand there are script kiddies who hack for fun.

Other characteristics of threat agents to measure risks are the size of the group operating, their skill level, and whether the opportunity to exploit a vulnerability is ‘easy’ or not (OWASP, 2014).

In addition threat vectors should also be held into account. A threat vector is “a path or a tool that a threat actor uses to attack the target” (Withers, 2011). By placing the risk variables and threat vectors across each other, a strategy can be defined per variable and threat vector. Examples of threat vectors are supply chains, remote access, proximity access, and insider access (Chabinsky, 2010).

4.3 The cyber threat landscape

Cyberspace provides several advantages above the ‘real’ physical world: it is timeless, borderless and anonymous. However, cyberspace was ‘not designed with security in mind’ according to the UK’s National Audit Office (2013). Cyberspace was never designed for tracking and tracing user behavior, nor to resist highly untrustworthy users

(Lipson, 2002). In addition, the current threat environment far exceeds cyberspace's design parameters and high-speed traffic hinders tracking (Lipson, 2002).

It is thus not surprising that cybercrimes followed rather quickly after the 'commercial' introduction of the internet. One of the first recognized cybercrimes, a worm, was the Morris worm in 1988 (Orman, 2003). Since then, the number of attacks has grown exponentially, especially in the 21st century. In addition, the skills needed to perform an attack has become significantly less (Figure 9). For example, the ZeuS bot (Choo, 2011a) made it possible for less skilled hackers to distribute the malware and steal tons of personal identity information (PII) and financial identity information (FII).

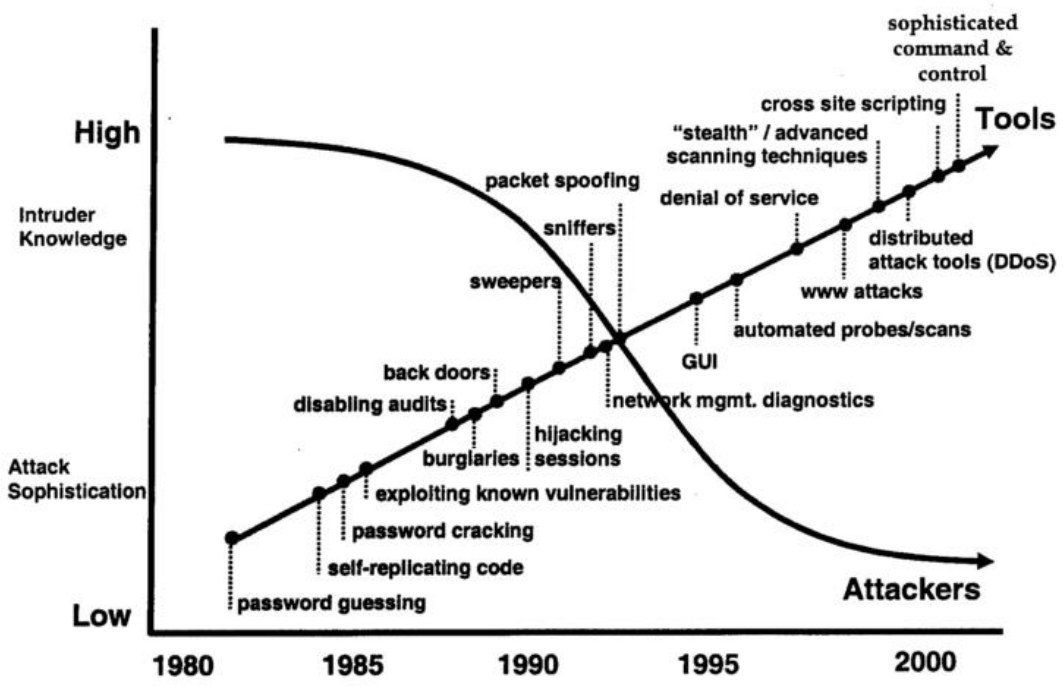


FIGURE 9: ATTACK SOPHISTICATION VS. INTRUDER TECHNICAL KNOWLEDGE (Lipson, 2002)

Security breaches can be externally, internally, accidental or on purpose initiated. Before the '00s there was an even split between the amounts of internal, external, and accidental initiated breaches (Byres & Lowe, 2004). A study by the FBI and the Computer Security Institute on Cybercrime in 2000 showed that 71% of these breaches were internally initiated. However, from 2001 to 2003, there has been a major shift where 70% of all events were externally initiated, instead of 31% before the 00's. This trend has continued, where from 2004 until 2013, most breaches were initiated by external actors. Table 4 shows the percentage of breaches per threat actor category over time of the total amount of breaches reported. There is only one exception, in 2007, there were more internal initiated breaches than external. Several researches indicated the danger and power of internally initiated attacks (e.g. Cohen, 2001; Colwill, 2009; Greitzer et al., 2008; Sarkar, 2010; Wall, 2010; Woollacott, 2007).

TABLE 4: PERCENTAGE OF BREACHES PER THREAT ACTOR CATEGORY OVER TIME (Verizon, 2014)

	2004	2005	2006	2007	2008	2009	2010
External	92%	72%	68%	41%	82%	86%	94%
Internal	8%	25%	31%	56%	62%	23%	14%
Partner	4%	15%	8%	6%	16%	2%	0%
Unknown	0%	0%	0%	0%	0%	1%	0%

In the past years, the threat landscape has changed by economic-, technological-, market-, and legal developments (KPMG, 2014) and has been characterized by phishing and malware. In 2009 and 2010, Australia's industry was dominated by malware attacks (Choo, 2011b). This meant a 71% increase in malware attacks compared to 2008. The period of 2004-2008 was also characterized by malware attacks, in most cases targeting the financial services industry (Choo, 2011a). Besides malware, phishing attacks was listed in the top five most expensive crime in 2009 and 2010 in Australia (Choo, 2011b). However, the amount of fully automated attacks decreased (Potts, 2012). Also, in recent years, the motivation for committing a cybercrime shifted from curiosity and fame seeking to financial gain (Choo, 2011a). The UK's National Audit Office (2013) saw that 'serious organized crime using the internet to steal personal or financial data to commit fraud, steal corporate intellectual property, or launder money; political activists hacking and using the internet to steal information or damage computer systems to serve political agendas; and state supported espionage and attacks on critical national infrastructure' are existing and evolving threats to the internet.

In addition, a research by Gragido (2011) stated that the current threat landscape is shaped by the growing availability and consumption of enterprise technologies and the increasing sophistication of cyberattacks. Besides that, web applications remain the main target of cyberattacks and legacy threats are in revival (Gragido, 2011).

And what about the future? The Internet of Things (IoT), smart devices, cloud computing, consumerization of IT (e.g. BYOD), and social media will soon shape the cyber threat landscape (Choo, 2011a, 2011b; Contreras, Denardis, & Teplinsky, 2013; Gragido, 2011; Kellerman, 2010; Potts, 2012; Victoria & Florin, 2012; Zimski, 2011).

It must be noted that many studies by private companies are available that seek to illustrate the threat landscape (Deloitte, 2011; Ponemon, 2013; PwC, 2014; Verizon, 2014). However, identifying and reporting cyber-attacks or breaches is still not the status quo. Many companies do not report breaches because they fear, amongst others, reputation damage. Unfortunately, this results in incomplete and scarce information about the real number of cyber-attacks and security breaches. For instance, this is also notable in the Verizon security breaches report published every year, where data is only available from 2004 onwards. However, in the Netherlands a new law ('wet meldplicht datalekken') is imposed where organizations are obliged to report security breaches. This strongly reduces the gap in actual security breaches and reported breaches, in the near future.

4.4 Conclusion

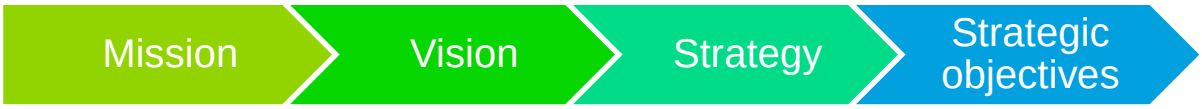
The discussion listed above shows how cyber security is different from information security. Information security deals with information based assets, like leaving a paper at the printer may cause a threat to the confidentiality of the information. Cyber security deals with information and non-information based assets, for example the stuxnet worm made use of the cyberspace to attack a SCADA system. But the key difference is that in cyber security the attacker uses the cyberspace as a vehicle to place its attacks. Cyberspace is not only the internet but also all devices connected to the internet, like you mobile phones and laptops.

Every company has valuable assets that are worth protecting against threat agents who wishes to damage or abuse the asset. They will do that by exploiting vulnerabilities that exist in the asset or the environment. Security controls can be imposed to reduce the number of vulnerabilities and thereby reducing risk to an acceptable level. It must be concluded that cyberspace was never designed with security in mind. In addition, cyberspace is timeless, borderless, anonymous, and most of the times wireless, so it is a perfect vehicle to abuse. Currently, the threat landscape is characterized by malware and phishing attacks, but soon will be shaped by abusing the internet of Things, smart devices, cloud computing, consumerization of IT, and social media.

5 From vision and ambition to strategy

The goal of this research is to figure out how corporate organizations can develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition. Therefore, we must first define exactly how strategic concepts like ambition and strategy are related.

Vision, missions, and strategies are used by organizations with the purpose of communicating, and propagating the strategic direction of the organization to its stakeholders, and to guide the implementation. At the highest level, mission statements are formulated (what are we?), then the vision is formulated (what do we want to become?), and based on that a strategy is formulated (what will we do to achieve our vision?). This strategy consists of strategic objectives, which is "a broadly defined, measurable objective that an organization must achieve to make its strategy succeed"[7].



The Cookie Factory

ABC, founded in 1901, is a family business with specialties in baking all sorts of cookies. During all these years, ABC has developed itself into a very modern company with access to the best materials to bake the cookies. The cookie recipe is stored in the machine and therefore, drives and controls the machine. All processes in the factory happen autonomous and the machines can be managed remotely after working hours. In addition, cookies can nowadays be ordered online by direct customers or retailers. This year, the cookie factory had a revenue of 15 million euros in the Netherlands.

5.1 The mission

David (1989) defines a mission statement as "a declaration of an organization's 'reason for being'". A mission statement can help focus the organization to its real purpose of existence for itself and stakeholders (Ireland & Hirc, 1992). In a survey by David, 181 organizations elaborated on what components should be included in company mission statements. The survey showed that, amongst others, customers, products or services, technology, and concern for survival are the most commonly found components of mission statements (David, 1989). This is in line with an earlier research done by David and Cochran where 64-65% percent of the sample mission statements included technology, concern for survival and public image. Reasons for having a mission statement are, amongst others, to guide strategic planning or to give strategic direction to the organization (Baetz & Bart, 1996, p. 528). However, formulating a mission statement for your company is difficult; the environment is ever changing which makes it challenging to decide on a mission (Ireland & Hirc, 1992). In addition, there is no need to establish a separate

The mission of ABC is: "We provide the most delicious cookies to our customers."

[7] http://www.businessdictionary.com/definition/strategic-objective.html , consulted on 08-06-2015

mission related to cyber security, because we think cyber security in itself is not a mission for a company as it is not its primary business.

5.2 The vision and ambition

Whereas the mission statements answers the question 'what are we?', the vision statement expands on this by asking 'what do we want to become?'. A mission statement is different from a vision statement in that a mission is something to be accomplished whereas a vision is something to be pursued to achieve that accomplishment. According to Wilson (1992), a vision must be coherent, powerful, realistic, and should clarify what the organization should be.

In addition, ambitions of an organization are also made explicit. An ambition is what you aim to achieve. It is a future goal and therefore resembles the vision statement. A domain-specific ambition should support the organization's ambition.

> *"You should first determine what exactly the ambition of the organization itself is, what the goal is. Once you know that, you must think about what is really important in that process. Suppose we talk about that cookie bakery. Where lies the key value? The formula of the cookies is very important, raw materials must be good, or everyone should always be able to order cookies online. If one of these is the business goal, then you have to make sure it becomes a key element [to the organization]. That way, you try to define a number of assets which you have to protect."* – *Expert 4*

Furthermore, according to the experts the cyber security ambition should answer the 'why' question and contain an ambition level, it should be presented in a narrative fashion with which employees can relate. However, the ambition statement should still be specific, measurable, acceptable, realistic, and time-oriented (SMART). And ultimately, an ambition statement should drive the strategy.

> *"An [cyber security] ambition statement should contain an ambition level that you wish to achieve, why you want to achieve that level, and which conditions apply. How you will do this will be your strategy."* – *Expert 10*

The vision of ABC is:
"We want to be the biggest online cookie seller in Europe."

However, we think it is better that the ambition is not yet presented in a SMART manner. We support the vision of Wilson (1992) that the vision or ambition, also the cyber security vision, should be coherent, powerful, realistic, and should clarify what the organization should be. It is not necessary to have an ambition which is specific, measurable, acceptable, and time-oriented as an ambition is a general view of the future state and direction. Therefore, it is not possible to make it SMART. Short term derivatives of the ambition should be SMART.

5.3 The strategy

While the ambition is concerned with where an organization wants to go or which goal they wish to achieve, a strategy expands in this by showing how to achieve this goal in broad terms. A strategy is therefore guided by the mission and vision of the organization and the domain specific ambition. For the construction of a strategy, many tools, techniques, and theories are available. Several definitions of strategy have been proposed by researchers in the field of strategic management:

> "Strategy is the direction and scope of an organization over the long term, which achieves advantage in a changing environment through its configuration of resources and competences with the aim of fulfilling stakeholder expectations" (Johnson, Scholes, & Whittington, 2008).
>
> "Strategy is the creation of a unique and valuable position, involving different set of activities" (Porter, 1996).
>
> "The match an organization makes between its internal resources and skills… and the opportunities and risks created by its external environment" (Grant, 1991)
>
> "An organization's strategy describes how it intends to create value for its shareholders, customers, and citizens" (Kaplan & Norton, 2004)

In this research, we use the definition of Johnson et al. (2008), as we think this definition includes the concepts stressed as important in the other definitions, namely value creation, internal and external environment, and the inclusion of stakeholders.

Unfortunately the reality of strategic management is that not all strategies work out as planned. Intended strategies that are realized are often called deliberate strategies. However, the chance of perfectly realizing an intended strategy is close to zero (Mintzberg, Ahlstrand, & Lampel, 1998). Unrealized strategies are, for example, due to unrealistic expectations or changes in the internal or external environment (Mintzberg, 1978). An emergent strategy is a strategy that emerges along the way and was never intended. Reasons for such emergent strategies are, according to Ward & Peppard (2008), imposed changes, new opportunities, unexpected constraints or options, or failed implementation. This theory has to be taken into account when creating a method to develop a cyber security strategy. In our opinion, the created method must withstand or adequately deal with these imposed changes, new opportunities, unexpected constraints or options, or failed implementations, in the form of reviewing and evaluating results of the cyber security strategy.

ABCs business strategy is: "By using the online environment, we will gain market share and brand recognition in Europe, outside the current countries. We will do this by using our famous cookie recipe."

> *"The rationality of a particular strategy depends on its specific historical, social and cultural context. Strategic behavior is embedded in a network of social relations that includes cultural norms, class and educational background, religion and so on. Hence what is labelled as irrational behavior in one context may be perfectly rational in another".* (Whittington, 2001)

As such, there are many approaches to and rationales behind substantiating a strategy. It is a challenging process, but some researchers have tried to get grip on the process of formulating a strategy. Someone who has thought elaborately about this is Mintzberg.

5.3.1 The 10 schools of thought on strategic management

Through the history of strategic management, many scientists have tried to develop their way of strategy formation. Mintzberg tried to group these existing approaches into the so-called 'ten schools of thought on strategic management'. According to Mintzberg, these ten schools are the design, planning, positioning, entrepreneurial, cognitive, learning, power, cultural, environment, and configuration school; each one of them propagating a different approach to the creation of a strategy.

The design school sees strategy formation as a process of conception, meaning that they seek to reach a fit between internal capabilities and external possibilities. The planning school sees strategy formation as a formal

process, where a SWOT model is used as a basis to form well-articulated steps, objectives and plans. In addition, the positioning school resolves around analytical processes and focuses on the position of the organization in its industry. These three schools have quite clear processes and have a structured and formal approach to strategy creation. Another way of creating strategy is by perceiving strategy formation as a visionary process where the basis lies on intuition, judgement, wisdom, experiences and so forth. The cognitive school views strategy formation as a mental process. To understand how strategies are formed under other circumstances, one should consider how humans think. Furthermore, the learning school views strategy formation as an emergent process and the organization learns over time what works and what doesn't. The power school recognizes strategy formation as a process of negotiation where politics and power play a big part in establishing or negotiating strategies. In addition, the cultural school sees strategy formation as a collective process, where the focus lies on the common interest; i.e. "a process of social interaction between members of the organization" (Mintzberg et al., 1998, p. 267). The environmental school sees strategy formation as a reactive process. Whereas other schools see the environment as a factor, the environmental school views the environment as the central actor (Mintzberg et al., 1998). And lastly, the configuration school sees strategy formation as a process of transformation. The configuration school is a hybrid of all other schools and its message is 'each school at its own time, in its own place' (Mintzberg et al., 1998). All schools have limitations to it and relying on schools to explain an organization's situation is not realistic as it does not reflect it 100%.

The ten schools of thought on strategic management shows that there are many different approaches in formulating a strategy. However, many researchers critique the classification of Mintzberg (Mintzberg et al., 1998). But what we can learn from these schools is that there is no one best method to create a strategy. Throughout our research, we mainly focus on creating a structured process to establish a proactive cyber security strategy. This resembles the first three schools, namely the design, planning, and positioning school. Because a cyber security strategy is a defense against (threats of) attacks and this resembles the way military organizations create strategies. Military organizations use a proactive and structured approach[8], which is in contrast with the remaining schools.

5.4 Drivers of a strategy

Different motivations underlie the need for a strategy. Not much literature is available about what exactly the drivers of a strategy are. However, literature about open data policies shows that, in that field, strategy is externally driven whereas boundaries exist internally (Huijboom & Broek, 2011). In the field of business strategy, Skrt and Antoncic (2004) found several drivers for strategy creation in small firms. Strategy was, for instance, driven by the vision and objectives of the entrepreneur or the entrepreneurial team. Also, the entrepreneur's wish for achievement of planned growth and higher profits, opportunities in the market, and imitation of other firms and competitor were, amongst others, listed as drivers for the creation of a strategy.

In addition to what could be found in literature, the Information Security Forum also presented a workshop paper about information security strategy (ISF, 2007). They list six important drivers for an information security strategy. These drivers with their description can be found in Table 5. This list also shows a balance between internal (i.e. corporate governance, audit, and management) and external drivers (i.e. legal, regulatory, and peer and media pressure).

[8] Opentuition.com/wp-content/blogs.dir/1/files/group-documents/23/1271485643-MINTZBERGTENSCHOOLOFTHOUGHTFORSTRATEGYFORMATION.pdf , consulted on 4-7-2015

TABLE 5: INFORMATION SECURITY STRATEGY DRIVERS AS FOUND BY (ISF, 2007, P. 7)

Driver	Description
Corporate governance	Corporate codes often imply the need for a strategy for effective risk management
Legal	Some industry-related laws have requirements for an information security strategy
Regulatory	Regulations may have requirements for an information security strategy
Audit	Audit reports may require a strategy as part of overall good governance
Management	Executive management may require information security to have a strategy as part of an overall strategic cascade
Peer and media pressure	Peer organizations and oversight bodies may create pressure to adopt a strategy

In addition, experts gave a number of diverse motivations for the creation of a cyber security strategy during the interviews. There are many possible drivers for creating a cyber security strategy. It may be driven by a person, department, organization or the government, or it may be driven by incidents, reputation, the business or risks. A consultant explained how a cyber security strategy is driven by an organization's risk appetite:

> *"It is driven by the willingness of an organization to take risks. What if the web portal of a cookie factory is not available and this is really bad for the organization, then the security strategy is driven by the fact that you would want to invest a lot of money to improve the availability of the web portal. But if it is not bad at all, then it won't be a problem in my opinion. The question is: how important is something at the moment it is not available anymore? That is actually a risk analysis. What risk is acceptable? Is it acceptable to be offline for 2 days? Or for a month? On the basis of that, your risk appetite, you will determine what your strategy should be" – Expert 4*

Another example is that many cyber security strategies are driven by external regulators. The 'De Nederlandse Bank' requires that Dutch financial institutions comply with certain laws.

> *"In practice, it [the cyber security strategy] is often initiated because regulators want it. This is what I see in most organizations. Whether it is a regulator or a government, that is how it usually starts. When people are working on this strategy and are thinking about it, only then a naturally intrinsic motivation will occur." – Expert 6*

Cyber security experts identified seventeen unique drivers. The mentioned drivers in the interviews can be divided in 'who' drives the strategy and 'what' drives the strategy. External regulators, the management board, the security department, the government, the organization itself, and the IT department are internal initiators of formulating a cyber security strategy. According to the interviewees, they want a cyber security strategy because, for instance, the law or regulations demand this, cyber security incidents, or because they want to retain a good reputation.

Table 6 shows all drivers with between brackets the number of experts mentioning this driver.

TABLE 6: DRIVERS OF A CYBER SECURITY STRATEGY MENTIONED BY THE INTERVIEWEES

Who	What
External regulators (8)	The law and regulations (8)
The management board (5)	Incidents (8)
The security department (4)	Risks or the risk appetite (5)
The government (2)	The business operations or the business goals (5)
The organization itself (2)	For the usefulness and necessity of a cyber security strategy (4)
The IT department (1)	To retain a good reputation (3)
	Threats to the critical assets of the organization (2)
	To promote arrangements with regard to cyber security (2)
	Media attention (2)
	The willingness to be compliant (2)
	The inadequacy of the former cyber security strategy (1)

The drivers mentioned by security experts support the drivers mentioned by the Information Security Forum (2007), in our opinion. 'Corporate governance' and 'management' is congruent to 'for the usefulness and necessity of a cyber security strategy' and 'the business operations or the business goals'. In addition, 'legal' and 'regulatory' corresponds to 'the law and regulations' mentioned in the interviews. 'Audit' refers to 'the willingness to be compliant'. And lastly, 'peer and media pressure' addresses 'to retain a good reputation', 'media attention', and 'to promote arrangements with regard to cyber security'.

ABC wants a cyber security strategy, because: "To become the biggest online cookie seller, ABC needs to make sure the online portal is always available, integrity of orders is guaranteed, and confidentiality of customer data and online transactions is to the highest standards. In addition, the famous recipe must be protected as well as the way the production environment is controlled as both are key to the success of the end product."

Table 7 shows all the drivers for creating a cyber security strategy as found in the literature and interviews, which we therefore consider as valid. According to the experts, the strategy is or should be initiated by external regulators, the management board, the security department, the government, the organization itself, or the IT department.

Furthermore, one of the drivers of a cyber security strategy is the organization's goals. The research model we used in this research assumes there is a direct relationship between the organization's ambition or strategy and the cyber security ambition or strategy.

TABLE 7: THE DRIVERS FOR CREATING A CYBER SECURITY STRATEGY

Driver	Description
Corporate governance	Corporate codes often imply the need for a strategy for effective risk management
Legal	Some industry-related laws have requirements for an information security strategy
Regulatory	Regulations may have requirements for an information security strategy
Audit	Audit reports may require a strategy as part of overall good governance
Management	Executive management may require information security to have a strategy as part of an overall strategic cascade
Peer and media pressure	Peer organizations and oversight bodies may create pressure to adopt a strategy. In addition, media attention to security breaches may drive a strategy.
Incidents	Cyber security incidents may call for immediate action and the creation or the update of a (new) strategy
Risks or the risk appetite	The degree to which an organization is at risk or the amount of risk that an organization is willing to accept may require a strategy
Threats to the critical assets of the organization	Threats to the critical assets of the organization may call for a strategy
The inadequacy of the former cyber security strategy	The inadequacy of the former cyber security strategy can require a new strategy to adequately address threats

5.5 Link between the organization's ambition and the cyber security ambition

In the previous section we already mention that the organization's goals are drivers to the cyber security ambition. In this chapter we try to prove this relationship. However, since there is no literature available on the specific relationship between organizational goals and cyber security goals, we first discuss the alignment of business and IT. Next, we make a translation to understand the link between cyber security and the business.

In 1999, Henderson & Venkatraman already stressed the importance of aligning business strategy with the organization's IT strategy (Figure 10). They argue that the misalignment between business strategies and IT strategies causes the inability to leverage IT investments by organizations. However, business and IT strategy are still not aligned in most companies (Silvius, 2007). In our opinion, a business strategy should be delegated to all sub divisions within an organization, to let all departments and employees work towards that same strategy.

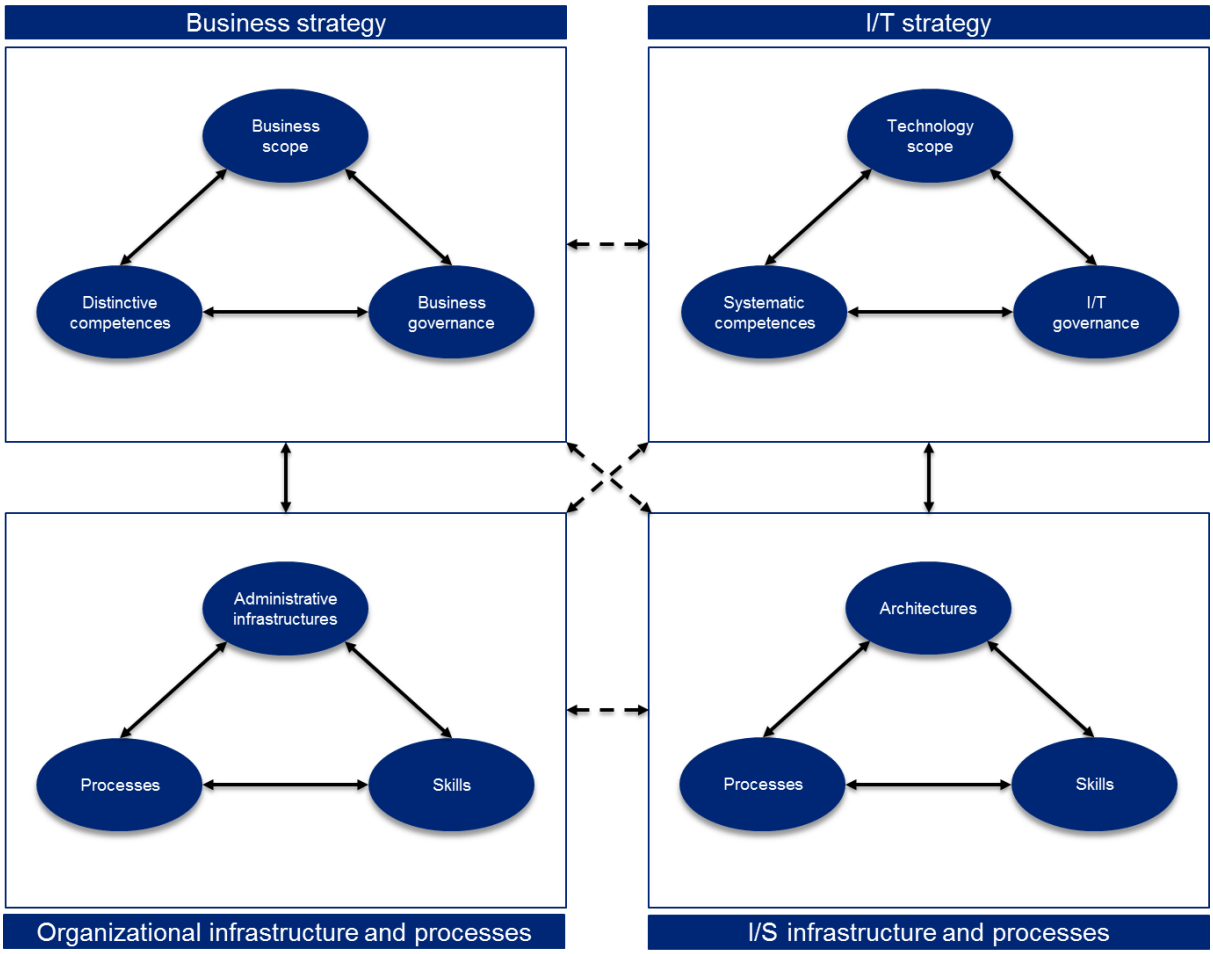


FIGURE 10: BUSINESS AND I/T STRATEGY ALIGNMENT MODEL (HENDERSON & VENKATRAMAN, 1999)

Figure 10 shows the link between business, IS, and IT. It is said that the IT strategy should be based on business decisions, business and activity based, demand and supply oriented, and application and technology focused (Henderson & Venkatraman, 1999). Whereas the business strategy deals with 'where is the business going and why', the IS strategy deals with 'what is required' and the IT strategy deals with 'how can it be delivered'.

The composition of a cyber-security strategy, in addition, is a cumbersome process, with different approaches that can be used (Chabinsky, 2010). We believe that cyber security strategy deals with all questions listed above in a support-matter. Cyber security supports the business in doing their key activities, the IS department in making the information systems safe, and the IT department in carefully choosing technology.

In addition to the link between the cyber security strategy and the organization's strategy that we found in the literature, the interview results show that the cyber security ambition cannot be seen separately from the organization's ambition.

> *"The ambition should, at least, contain a translation of the company's goals" – Expert 2*

> *"One of the subjects is always 'business alignment', so how do you align your security strategy with your business strategy. What we do try, of course, is to define the common ground to, at least, translate this to 'why is security important in the context of the business strategy or philosophy?' " – Expert 11*

One expert stated that at his organization the cyber security ambition was not needed, only an organization ambition. Two experts stated that they did not have a separate cyber security ambition. They always try to support the organization ambition with their security department.

> *"I do not think that you need that kind of a vision for information security. That is your business vision. My idea is that your security strategy is actually meant to secure your company's vision and business strategy. You try to accomplish your business strategy, however, there are many threats, amongst others, from the cyber security field. These are a threat to your business goals." – Expert 6*

In addition, two experts state that it is not surprising if companies do not have a separate cyber security ambition or strategy. It is often the case that these are mentioned in a subsection of a high-level strategy document of the organization. Although we consider that having a cyber security ambition is company-dependent, we still believe that, for the completeness of our method, it is important to have a separate cyber security ambition.

Although there are different opinions in whether there should exist a separate cyber security ambition, it is clear to us however, that the cyber security ambition cannot be seen separately from the organization's ambition. Based on what we found in the literature and the interviews, we can conclude that the cyber security ambition should always directly support the organization's ambition or the cyber security ambition is derived from the organization's ambition. Furthermore, the cyber security ambition is translated to a cyber security strategy. This strategy should take in mind the organization's strategy, as concluded from the literature. In the organization's strategy specific strategic objectives and projects are listed. When an organization wants to include cyber security in these projects, then a link is made between the organization strategy and the cyber security strategy. Figure 11 shows the relationships between these concepts we proved in this section, where the dashed line represents an indirect relationship and the solid line a direct relationship.

To achieve the organization's ambition, ABC wants to have an above industry average secure online and offline environment

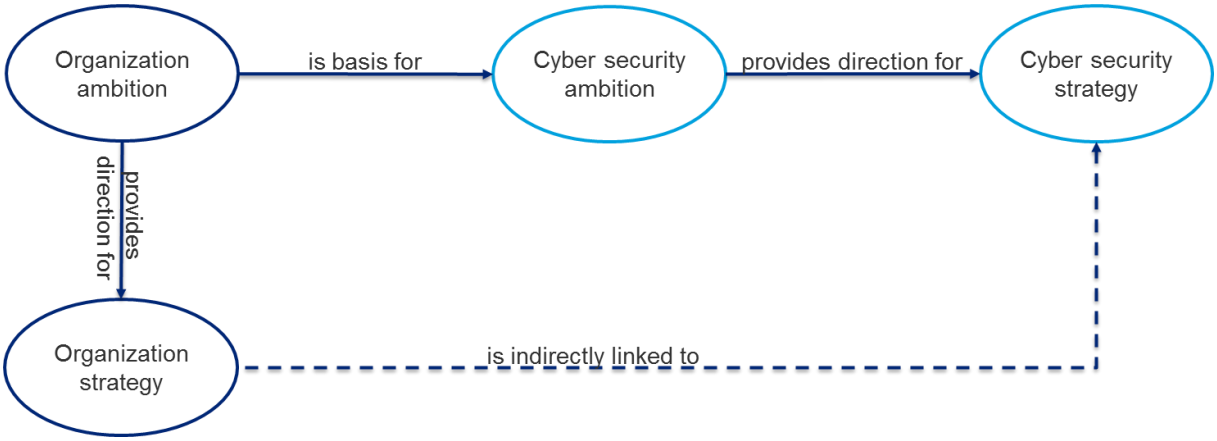


FIGURE 11: THE RELATIONSHIP BETWEEN THE ORGANIZATION'S AMBITION AND STRATEGY, AND THE CYBER SECURITY AMBITION AND STRATEGY

5.6 Conclusion

We can conclude that the mission, vision, and strategy differ on that the mission deals with 'who are we', the vision with 'who do we want to become', and the strategy with 'how do we get there'. A strategy is driven by the organization's vision, which is driven by its mission. Other drivers for a strategy, specifically a cyber security strategy, are corporate governance, legal, regulatory, audit, management, incidents, risks or the risk appetite, threats to the critical assets of the organization, and the inadequacy of the former cyber security strategy.

Nevertheless, we believe that formulating a strategy is a challenging process and literature shows that there is no one approach to this process. It is often seen that strategies do not work out as planned. A way of formulating a strategy is by linking it to the organization's ambition and strategy, as we have seen in both literature and interviews. Other ways of formulating a strategy can be derived from, amongst other, the business, game theory, and military domain. And specifically, from the cyber security domain, if available.

6 Strategy from different perspectives

Strategies are often created if a goal is to be met, combined with a specific driver as mentioned in the previous chapter. These goals can be various, and therefore strategy is created everywhere and by everyone. Whereas we are interested in the creation of a cyber security strategy, literature is almost non-existent. Therefore, as described in chapter 3, we discuss how strategy is created from different perspectives by analyzing literature in different domains, conducting expert interviews, and assessing national cyber security strategies. By using three different approaches (triangulation) and include different fields we comply with the design as a search process guideline and provide research rigor according to Hevner et al. (2004). First, we discuss important elements, from different domains, included in a strategy. And second, we discuss cyber security elements that are important for a cyber security strategy.

6.1 Strategy elements from the organizational, military, and game theory perspective

A scan through literature showed us that strategy models in the field of business, military, and game theory were the most promising in providing useful input for our strategy creation method. While the business strategy models are well-known and frequently used, the models used in the military and game theory domain are defense-based models. These models are therefore applicable to the cyber security domain, since this it is a defense strategy as mentioned in section 5.3.1.

The list of models, present in the organizational, military, and game theory domain, used is not exhaustive, but it does contain the best known strategic models according to us. In addition, all models listed are translated to the domain of cyber security, making them applicable for further analysis. This section elaborates on the strategy elements from the organizational, military, and game theory domain. First the BCG growth-share matrix, the 7-S model of McKinsey, Porter's five forces, PEST(EL) analysis, and SWOT analysis is discussed as organizational strategy models. Next, we discuss strategic theorists in the military field and the OODA loop. And lastly, game theory in relation to strategy creation is presented.

6.1.1 Strategy elements from the organizational perspective

There are many well-known strategy models in the business domain. These were once created by practitioners in the field, but have been proven its scientific relevance and effectiveness. Below we discuss the Boston Consulting Group growth-share matrix, the 7-S framework of McKinsey, Porter's five forces, the PEST(EL) analysis, and the SWOT analysis. We chose these models based on their popularity and applicability, but we acknowledge this list is not exhaustive. If an element of a business model is also applicable in the cyber security domain, we use these elements for further analysis.

The BCG growth-share matrix

In 1977, The Boston Consulting Group created an approach for organizations to develop a strategy. This approach was based on an earlier research that indicated the requirements for strategic success by organizations. According to Hedley (1977), key to strategic success is considering both the organization's growth and the market share. The growth is inherently linked to gaining market share: by expanding capacity earlier than competitors, a larger market share can be obtained. In addition, growth also provides the opportunity to invest. When a company has a high market growth, investments are necessary to keep that position, also in terms of the market share. But, this also gives an advantage for the investors who will receive larger amounts of money later on. Figure 12 shows the

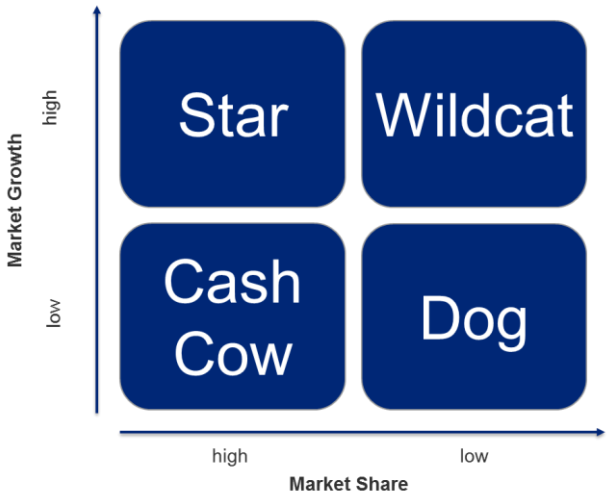


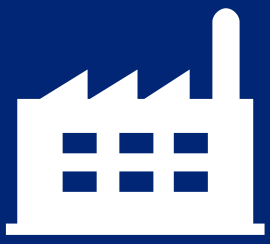
FIGURE 12: THE BOSTON CONSULTING GROUP GROWTH-SHARE MATRIX

Business Portfolio matrix. The x-axis is represented by the relative market share and the y-axis is represented by the market growth. The cells in the matrix consist of four positions of the business portfolio or strategies that can be followed: stars, cash cows, dogs, and wildcats. A star company is reflected by a high market growth and a market share. According to Ward and Peppard (2008), "star products generate significant revenue, but also require substantial investment in order to establish themselves in the markets and provide the production capacity or service delivery". If stars fail to keep a high market share, they will become dogs. However good investments will result in a cash cow position. Cash cows are characterized by low market growth and a high market share, meaning that they have already grown to such an extent that a high, and steady market share is obtained. Less investment is needed because a solid market position has been reached. Dogs are typified by a low market share and a low market growth. Not much money is made by these companies and as their growth is not high, it is very hard to gain a higher market share resulting in better incomes and cost reductions. Either a very large investment is needed, or these dogs will go bankrupt. And lastly, wildcats represent a high market growth, but low market share. Because they have a high market growth, these companies need a high investment but is not profitable due to their low market share. Therefore, this is the worst position of all if market shares won't grow. Only a selected few companies will rise to a star position, others will be divested. (Hedley, 1977) Unfortunately, the matrix by the Boston Consulting Group cannot be applied to companies in markets with high governmental control, because that control distorts the market (Ward & Peppard, 2008).

Cyber security application of the BCG growth-share matrix

Although it is hard to position an organization in the business portfolio matrix based on its security, we think it is however, a useful tool. Especially the position of the wildcat is interesting in our opinion; is there a way that a wildcat organization could not reach the star position when their cyber security is not adequate enough? And, could an organization reach a certain desired position quicker, or stay on this position longer, when security is adequate?

The Cookie Factory



If we look at the cookie factory, we see that ABC currently has a high market share and low market growth. Therefore, they want to expand to Europe via online channels to rise to a star position. Without ensuring a safe online environment, where the portal is always available, the integrity of orders is guaranteed, and confidentiality of customer data and online transactions is to the highest standards, they won't be able to grow to the biggest online cookie seller. Why? Because when this is not guaranteed, customers will not likely buy cookies, adversaries can gain access to the portal, and ultimately, the brand image is harmed. In addition, market share can also decrease if the confidentiality and integrity of the cookie recipe is breached. This can happen both by stealing the recipe by the competitor or, by modifying the recipe or alterations to the production process resulting in less than delicious cookies.

The BCG growth-share matrix is primarily focused on the external environment. A model that focusses on the internal environment is the 7-S model of McKinsey.

7-S framework of McKinsey

Waterman, Peters, and Philips (1980) researched the relationship between structure, strategy, and organization. Their research resulted in the 7-S framework, presenting seven concepts related to organizational thought, as shown in Figure 13. Changing an organization is not just changing its structure. According to Waterman et al. (1980), “effective change is the relationship between structure, strategy, systems, style, skills, staff, and something we call superordinate goals”.

Structure is the way an organization is composed. Strategy deals with what goals a business wants to pursue and how. A system deals with all procedures necessary to run a business, especially financial procedures. Style is the way in which a business is run. In addition, staff is defined by the people and their skills are decisive for the organization’s competitive advantage. These components all refer to internal variables that are useful in reaching a strategic transformation. But the ultimate success will highly depend on the ability to derive strategy from shared values of the ones who implement it (Ward & Peppard, 2008).

The 7-S framework is based upon the ideas that multiple factors influence an organization’s ability to change, and interconnection between the components is inevitable. Failure to pay attention to the other S’s may cause the failure of the strategy, and there is no starting point, meaning that an organization can randomly start with an S.

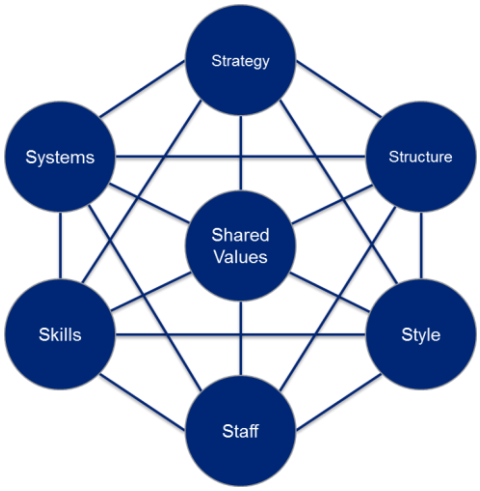


FIGURE 13: THE 7-S FRAMEWORK OF MCKINSEY

Cyber security application of the McKinsey 7-S model

As is clear from the description above, we think that the 7-S framework is useful to analyze the current status of the internal environment of an organization. Such an internal analysis of an organization’s cyber security capabilities is also important to do. We want to see how cyber security is positioned and structured within the organization. Who is responsible for what? In addition, a strategy in the field of cyber security should be imposed. Therefore, we also need the systems holding the cyber security resources together, namely the formal and informal procedures that are necessary for business continuity. Also, the style of the responsible persons for cyber security is an important influencing factor when changing the environment. Furthermore, the staff factor deals with the profiles and skills of the people responsible for cyber security. The skills factor considers what the organization excels at with regard to cyber security, e.g. what are their strengths? And lastly, the shared values is related to corporate culture regarding cyber security and the cyber security vision within the organization.

The Cookie Factory

We can explain this model by, again, using the cookie factory case. With the 7-S model of McKinsey we can assess the current situation of the internal cyber security organization in terms of organizational resources. First of all, at the cookie factory we see that there are not a lot of people involved in securing the organization and its products and services. In addition, the people who are now responsible for cyber security do not have specialized knowledge in security. Most projects are handled by people from the IT department and the responsibility for security lies with the CIO. There are currently little work procedures in place with regard to operationalizing cyber security. Also, due to the nature of the company (i.e. a family business), there is a natural resistance against organizational change. The main focus of the company is toward the business process, where a focus on cyber security lacks. As a consequence, the organizational skill factor in the area of cyber security is very low.

Porter's five forces

In 1979, Michael Porter described how competitive forces shape strategy. Porter identified five forces to review competition in the marketplace, necessary to adapt the corporate strategy to. Figure 14 shows the five forces that are relevant in assessing new and current industries or external environment an organization will be or is present in. The five competitive forces are threat of new entrants, bargaining power of buyers, bargaining power of suppliers, threat of substitute products or services, and rivalry amongst existing competitors.

Low entry barriers or weak competitive rivals may allow new competitors to enter the market. The threat of new entrants can be reduced by, amongst others, capital requirements, patents and specialist skills required, and differentiation and brand establishment/loyalty.

In addition, with more competition in an industry, potential buyers have more bargaining power. With little suppliers in an industry, suppliers have bargaining power. The bargaining power of buyers can be increased by, for example, low switching costs across suppliers and weak brand identities. Bargaining power of suppliers can be increased when there are few suppliers in the industry and when potential substitute suppliers or resources are not easily available.

Threat of substitute products always exists. However, this threat may be reduced by creating customer awareness for the need of the product and increasing loyalty of customers by using loyalty cards or promotions.

And finally, rivalry among existing competitors is often typified by vicious price wars or aggressive campaigns. This rivalry is usually increased when markets grow slowly, small number of similar sized competitors dominate the market, and there are many undifferentiated products by these competitors.

Cyber security application of Porter's five forces

The impact of the five forces on an organization and its competitive market can lead to a strategy. We can simply say that these five forces are 'external things in the competitive environment' an organization should assess in terms of impact. We think that, when applying this model to the field of cyber security, only threat of new entrants, threat of substitute products or services, and rivalry amongst existing competitors are relevant. The bargaining power of suppliers and the bargaining power of buyers is left out of scope because a lack of cyber security will not give any bargaining power for both suppliers and buyers. In our opinion, a lack of cyber security within an organization can lead to loss of confidentiality of important information which can provide a competitive advantage for competitors and new entrants.

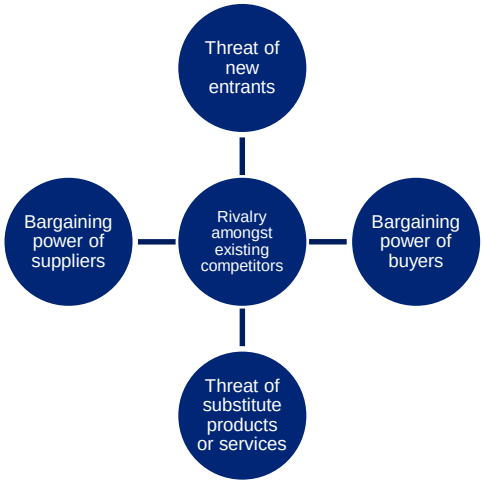


FIGURE 14: PORTER'S FIVE FORCES MODEL

These three forces can be used to assess different aspects of cyber security. For instance, assessing the threat of new entrants and substitute products or services is related to analyzing the threat landscape and the consequences of a security breach. In addition, rivalry amongst other companies can be seen as how other companies in the same industry have organized their cyber security.

To summarize, one can use Porter's five forces model to assess the external environment related to cyber security from a competitive perspective. By taking the threat landscape, the impact or consequences of a security breach, and the

level of security at competitors into account, it helps an organization to identify the current competitive environment of the industry in order to create a useful cyber security strategy.

The Cookie Factory

When we use these forces in relation to the cookie factory, we find some interesting results. For instance, looking at the threat landscape shows that everyone could shut down the factory by exploiting vulnerabilities, which has a high impact on the availability of the cookie factory. In addition, the integrity of the recipe can be affected by changing the recipe and the confidentiality can be affected when adversaries steal the recipe. These attacks are likely to be carried out by angry employees or jealous competitors. When an attack is successfully executed, this will harm the brand image and cause financial damage if, for instance, the production process is stopped or the recipe is modified. Furthermore, we know from an insider that the other cookie factories in the Netherlands, DEF and GHI, have better cyber security countermeasures than ABC. Therefore, ABC is more likely to be breached. It is thus necessary to get, at least, their cyber security at the same level as industry peers.

PEST(EL) Analysis

Another tool to analyze the external macro-environment is the PEST(EL) framework. PEST(EL) stands for political, economic, social, technological, environmental, and legal. Usually the environmental factor is discussed within the social factor, and legal is discussed within the political factor. According to Ward & Peppard (2008, p. 72), “carefully and continuously monitoring these factors can lead to significant business opportunities or identification of potential threats in time to take action to mitigate the effects”. There have been several studies that show two kinds of approach of the PEST(EL) analysis. First, it can be used to analyze the external environment. And second, it can be used to analyze the viability of a certain solution in the external environment (Peng & Nunes, 2007). Ultimately, this analysis tool is used to show which factors are of influence on the organization and its operations.

Cyber security application of the PEST(EL) analysis

We believe that the PEST(EL) factors can also be used to map both the external and the internal environment that influence the cyber security of an organization. According to us, political and legal factors can refer to laws and regulation that apply to the cyber security domain. Economic factors can influence the budgets available to implement cyber security measures. In addition, social and environmental factors can refer to, amongst other, awareness of people in the internal environment and social developments in the external environment. The technology factor can refer to technological developments in the external environment that call for new, extra, or advanced security.

The Cookie Factory

When we look at political and legal factors affecting the cookie factory, we see that in the Netherlands, since a cookie factory is not a governmental institution or bank, there are no obligations for the cookie factory to comply with special information security standards (e.g. ISO 27001 or CobiT). However, this may differ between countries and the cookie factory is obliged to follow the laws and regulations of the country where it is selling or producing cookies. What we also see is that it is economically more interesting to open an online channel than to open an offline store. In addition, we see a social development in the marketplace where people increasingly buy products online. And lastly, we think that it is technologically easy to set up an online channel as the technology has matured during recent years. Thus this affects the way security measures are imposed since there is a shift in how the business operates.

SWOT Analysis

In addition, the SWOT analysis is also a method to analyze an organization’s strategic position. SWOT stands for strengths, weaknesses, opportunities, and threats. According to Hill and Westbrook (1997), an organization must

have a good fit between the external environment, in terms of opportunities and threats, and the internal environment, in terms of its own strengths and weaknesses.

Cyber security application of the SWOT analysis

The four elements of the SWOT analysis can be directly used for the application in the cyber security domain in our opinion. For instance, the national information security strategy of Uganda lists their strengths, weaknesses, opportunities, and threats. One of the strengths is the "presence of Government political will in the area of national information security" (Uganda, 2011, p. 24). An internal weakness is, for example, "lack of information security awareness and persistent poor information security culture" (Uganda, 2011, p. 25). An opportunity identified by the government of Uganda is "actively participate in international co-operations on information security" (Uganda, 2011, p. 26). And lastly, an identified threat is "cybercrime, cyber warfare, and cyber terrorism" (Uganda, 2011, p. 27). As such, we think that every strength, weakness, opportunity, and threat gives direction to a strategy.

The Cookie Factory

The SWOT analysis can also be a helpful tool for the cookie factory to assess their internal and external environment. First of all, we see that ABC is using modern machines who are quite good protected against attacks from cyberspace. However, it seems that the employees of ABC are not aware about possible breaches and attacks. A recent test shows that 75% of the employees were fooled by a (fake) phishing mail where personal data was comprised and access to the system could be gained. Furthermore, we see that there are big opportunities in expanding the market of ABC online, through opening an online portal. However, by expanding the business online, we see several threats. Threats that may harm the availability of the portal, the integrity of orders, and the confidentiality of customer data and online transactions. This means that ABC should leverage the strengths and opportunities, and decrease or mitigate weaknesses and threats by making the employees more aware of security and protecting the online portal to the highest standards.

6.1.2Strategy elements from the military perspective

From the previous section we have learned that the organizational models are quite general and mostly focused on assessing the internal or the external environment. In this section we discuss strategy creation from the military domain. The military domain is well known for always strategically planning and structuring military missions. Their structured approach from deciding on a mission, to formulating the mission and the strategy, to actually deploying soldiers is useful input for the creation of other strategies.

In the military world, Helmuth Karl Bernhard von Moltke and John Boyd are, amongst others, well-known names with regard to strategy. Their approaches have proven its effectiveness and have been translated to the business domain. According to von Moltke, a German field marshal from 1819 until 1888, "strategy is not a lengthy action plan but rather the evolution of a central idea through continually changing circumstances" (Perky, 1991). Adjusting means to ends was one of the key ideas of von Moltke about strategy. In addition, von Moltke viewed strategy as a series of options. Von Moltke's work was influenced by Napoleon and Carl von Clausewitz, the last one being a Prussian general who wrote many military theories. One of them is related to strategy, where strategy was defined by him as "the use of engagements for the object of war" (Owens, 2007, p. 116). Von Clausewitz stressed that the unexpected developments in the environment call for direct action by leaders. Unexpected developments may appear under the 'fog of war', a term used to describe "the ability to process cognitive information and act quickly, effectively, and decisively on the battlefield, as well as the many external factors contributing to uncertainty and

indecision" (Lieberman et al., 2005). Like in fog, things tend to seem different than in reality and therefore rapid action is needed to overcome the sudden change in reality.

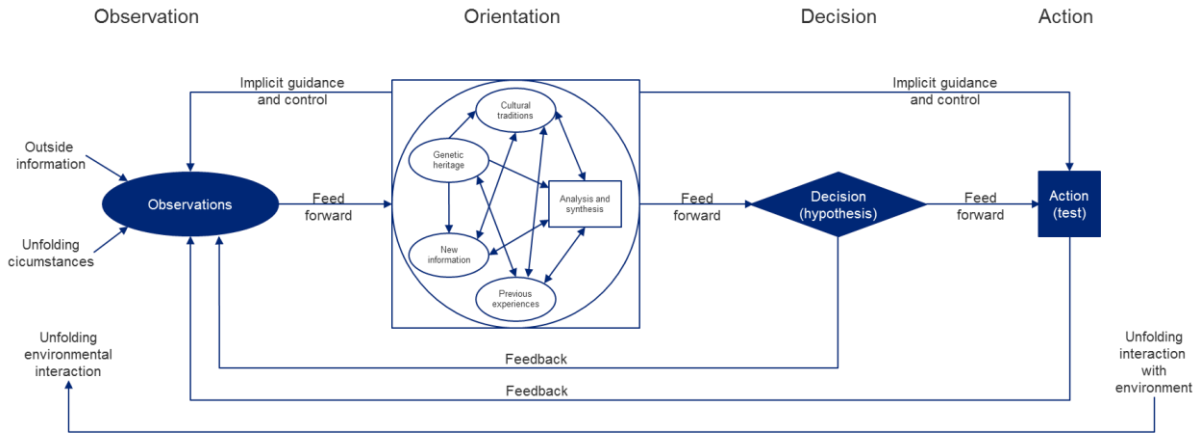


FIGURE 15: JOHN BOYD'S OODA LOOP

Another strategic thinker was John Boyd, a United States Air Force fighter pilot. According to Boyd, in order to understand the environment we must interact with it in different ways. And ultimately, strategy is "a game in which we must be able to diminish adversary's ability to communicate or interact with his environment while sustaining or improving ours" (Boyd, 1986, p. 34). In order to create strategy, Boyd developed the so-called OODA loop, which stands for Observe, Orient, Decide, and Act. It was used to help respond quicker and more appropriate to actions than the competitor. The best way to do so is by getting inside the OODA loop of the competitor, or simply put, to think ahead of what the competitor would do.

The first step in the OODA loop is observation. Observations are based on outside information, unfolding circumstances, implicit guidance and control from the orientation stage, and feedback from the decision and action stage. These observations are input for the orientation stage. The orientation stage is the most important stage of the model, and, amongst other things, filters the information on relevance from the previous stage. Important variables in the orientation stage that shape mental images, views or impressions of the world are cultural traditions, previous experiences, new information, and genetic heritage (Boyd, 1987a). It is said that "without cultural traditions and genetic heritage, the influence of new information and previous experiences increases"[9]. The analysis and synthesis element in the orientation stage is not so much a factor as it is an approach to analyze and synthesize the other factors by decomposing and recomposing them in a way that unrelated factors suddenly can become related. By emphasizing rather quickly made implicit relationships instead of more time-consuming explicit relationships, one can take an advantage above adversaries in terms of time and friction (Boyd, 1987a). The information from the orientation stage is fed forward to the decision stage where decisions are made about the strategy. The decision is the input for the actions that are needed to be taken in the action stage. Feedback from both the decision and action stage is fed back to the observations stage making the OODA loop continuous. The different stages of the OODA loop are shown in Figure 15.

Cyber security application of the OODA loop

What we have seen is that in the military field, strategy is created by looking at the opponents and their strategy. In addition, emphasis is on unexpected developments and observations that call for (immediate) action. Strategy is also seen as a series of options. And lastly, the OODA loop shows that feedback is very important before

[9] http://www.iohai.com/iohai-resources/certain-to-win-richards_files/frame.htm , consulted on 8-6-2015

continuing to the next stage. We will show how the OODA loop can be used to make a cyber security strategy. Since the model is generic in the terms it uses, and the military field is concerned with defense and attack strategies, we can use this model and its elements directly in the field of cyber security. The OODA loop is originally focused on situations in the battlefield, so very operationally focused. However, we are interested in using these steps to create a cyber security strategy where there is no immediate time pressure.

The Cookie Factory

First of all, within the observation phase outside information shows us that ABC is positioned very well in the marketplace with a low level of security and therefore a likely target for adversaries. Also, phishing and malware are dominating the cyber threat landscape and thus ABC too. This information is fed forward to the orientation stage where we analyze the information. From the analysis it shows that ABC is insufficiently protected against new forms of cyber-attacks. Previous experiences also supports the analysis because there were some incidents in the last 2 years. In order to be successful with the business, the decision is taken by the board of ABC to invest in implementing high standard cyber security measures. For instance, to ensure high availability of ABCs online portal, provide a safe online portal, and make the employees more aware of possible cyber threats. These actions are implemented over a time period of three years. Continuous guidance and control is needed and may imply the need for a new OODA cycle to respond to changes in the environment.

6.1.3 Strategy elements from the game theory perspective

In the previous section we discussed how strategy is created in the military domain. In this section we present how strategy is created in the game theory domain. When playing a game, one is continually defining goals one wishes to obtain. These can be, for instance, winning the game or obtaining the high score. In order to achieve this goal, a strategy is created by the player and steps are undertaken. It is a simple approach to strategy creation, however, valid. In this section we go into depth in this way of creating a strategy.

According to Johnson et al. (2008), game theory is about “the interrelationships between the competitive moves of a set of competitors”. Game theory is based upon two key assumptions: the rationality of competitors and the interdependent relationship between competitors. These can be translated into two ways in the process of creating a strategy. First, the strategist should get in the mind of the competitors and ask himself questions like “what would my competitor do?” Second, “decide strategy on the basis of understanding the outcomes of possible strategic moves of competitors” (Johnson et al., 2008, p. 280). This is also stressed by Brandenburger and Nalebuff (1995) who emphasize that the importance of game theory is in the focus on others instead of the own position. In addition, they add that a player can only take away from a game what he has put into it. This means that a strategist should look at the most value created player, and see how much value the remaining players create if this most value created player was not present. In addition, taking into account the steps that the attackers (the competitors) are likely to take can help find appropriate measures and justify those. In this way, a strategy is a continuous game in which steps are deliberated in advance and value is created and captured.

As a response to business game theory, Brandenburger and Nalebuff (1995) created a so-called ‘value net’ where players and their interactions are modelled. On the vertical axis, the customers and suppliers are modelled and the transaction-flow between them. On the horizontal axis, the substitutors (e.g. competitive products) and complementors (e.g. cooperation between companies) are located. The visualization of the value net is the first step in creating a game theory based strategy. The second step is to identify players, added values, rules, tactics, and scope (Brandenburger & Nalebuff, 1995). These variables are also appropriate and interesting to look at from a cyber security perspective.

Cyber security application of game theory

Game theory shows us that strategy can be created by focusing on others instead of the own position. This resembles, to some degree, how strategy is created in the military domain and therefore in the cyber security domain according to us. In addition, we saw that it is important to look at the most value created player and what value the remaining players create if the most value created player was not present. Let's say that security is a high value creator. If cyber security was taken away, can the other business services of the cookie factory still create value to the organization? Well, yes they can in our opinion. Security is not a high value creator in itself because security costs money and thus not directly contribute to the revenue of the cookie factory. A high value creator of the cookie factory is the recipe and in the future, will be the online portal. They can only stay a high value creator if the cyber security measures are up to the highest standards. Because if this is not the case, someone can steal the recipe or shut down the portal. Either way, it will take away the high value of the recipe or the online portal.

In addition, we should try to understand how the other players, the attackers, play. The cookie factory will most likely need to monitor the changing threat landscape and could implement a honeypot system to observe if an attacker breaches the security. This way the cookie factory can analyze the sophistication of the attacker.

The Cookie Factory

What we see is that the cookie factory will most likely be breached by an angry employee or jealous competitor. This means that their motivation is either revenge or espionage. The insider will probably use information that is easily available to him and might breach the system while being at work in the factory. The competitor will probably use highly sophisticated hackers to breach into the system. This can be done either by using the internet connection or by social engineering. This means that, for the internal employee, rights to the systems should be distributed carefully and the actions should be monitored. For the competitor, ABC could install a honey pot, for instance, and could train the employees to gain more awareness on possible threats.

6.1.4 Sub analysis

Analyzing the purpose of the models discussed above shows us different ways of looking at the area of creating a strategy. We took all elements from the models explained above. These elements are for instance market growth, strengths, weaknesses etcetera. We combined all these elements into three groups, namely: the social environment, the external environment, and the internal environment. These three groups are most applicable in the cyber security domain because, as we have explained in the introduction, attacks can be done by outsiders but also insiders. In addition, the humans (the social environment) are usually a weak link.

The social environment deals with, amongst others, humans, social relationships and culture within an organization (Barnett & Casper, 2001). The external environment deals with elements that exist outside the organization that are hard to control, but do influence the organization in different ways. For instance, a sudden rise in targeted phishing attacks may cause to focus a strategy more around being resilient towards this threat. The internal environment deals with all elements that exist within the organization. For instance, the business wants to go more digital and this thus results in having to have more and better protection of these digital services. The elements from the internal environment are, in comparison with the social environment, better measurable (e.g. comparable to hard skills).

Table 8 shows how the strategy elements from organizational, military and game theory models fit within the three groups. As such, we see how each model with associated elements relates to the three groups we classified. In our opinion, the results of analyzing the internal, external, and social environment can stress the need for a cyber security strategy, and determines the drivers. In addition, we use these three groups when we analyze the current situation during strategy creation because all models are used for this purpose.

The Cookie Factory

In the light of the cookie factory, the current social environment shows us that ABC is typified by a family business and its ways of working. This means that employees are resistant to change, but there is a lot of trust amongst the employees. The employees have a low awareness of possible cyber threats. The external environment of ABC shows that the amount of competitors will grow when ABC will enter the European market. Also, the competitors may be more aggressive and may be more knowledgeable in the area of cyber security. This may have a consequence that they could use this against a new entrant in their market as a protection measure of their own revenue. And finally, the internal environment shows us that the whole cookie factory is equipped with the newest machines. But their ICT landscape is not designed with cyber security in mind.

TABLE 8: COMMON ELEMENTS FOUND IN THE BUSINESS, GAME THEORY, AND MILITARY DOMAIN RELATED TO STRATEGY CREATION

Model	Element	Social environment	External environment	Internal environment
BCG Growth-share matrix	Market growth		X	
	Market share		X	
7-S model of McKinsey	Strategy			X
	Structure			X
	Style			X
	Staff			X
	Skills			X
	Shared values	X		
	Systems			X
Porter's five forces	Threats of new entrants		X	
	Bargaining power of buyers		X	
	Bargaining powers of suppliers		X	
	Threat of substitute products or services		X	
	Rivalry amongst competitors		X	
PEST(EL)	Political		X	
	Economic		X	
	Social	X		
	Technological		X	
SWOT	Strengths			X
	Weaknesses			X
	Opportunities		X	
	Threats		X	
OODA Loop	Cultural traditions	X		
	Outside information		X	
	Series of options			X
	Genetic heritage	X		
	Unfolding circumstances			X
	Unfolding environmental interaction		X	
	New information		X	X
	Previous experiences		X	X
Game theory	Added values			X
	Opponents		X	
	Players	X	X	
	Rules (Laws & regulations)		X	
	Tactics		X	

6.2 Strategy elements from the cyber security perspective

The classification found in the previous section shows that a common element in strategy formation is assessing the social, external, and internal environment. These environments are quite general, and as such, we want to get more insights into the specific cyber security strategy elements. Since there is nothing published on the creation of a cyber security strategy, we base our information on what we could extract from national cyber security strategy documents and interviews with experts in the field of cyber security. In addition, we show how these elements could be used when creating a cyber security strategy for ABC. However, this time we show the case application in the sub analysis for reasons discussed later on.

6.2.1 Cyber security strategy elements from a cross-border analysis of national cyber security strategies

Thirty-one national cyber security strategies across the world have been analyzed (see section 3.2.2) and elements for the creation of these strategy documents have been extracted. The analysis included both EU and non-EU countries where a cyber security strategy document was available.

During the analysis, elements were searched for in the national cyber security strategy documents. Since we found 48 unique elements, we classified the elements found in the national cyber security strategy documents in self-made groups as was done in the previous section, namely general elements and cyber specific elements.

Table 9 shows which elements fit within which category. These elements are used later on in the process of creating a cyber security strategy.

6.2.2 Cyber security strategy elements from the experts perspective

In addition to gathering which cyber security strategy elements in the public domain, we interviewed experts about their view on the creation of cyber security strategy (see section 3.2.3). During the interviews, we first asked how the interviewee developed a (cyber) security strategy and what process they followed. However, we noticed during the interviews that experts had trouble explicating the process they followed to create a (cyber) security strategy. Therefore, we show which elements they expressed instead of the process steps. Below we present a list of these important elements mentioned by the experts which they expressed as steps in the process to create a (cyber) security strategy, with the number of mentions behind each element.

- Threats (6)
- Current situation (6)
- Via a framework (6)
- Developments (5)
- Assets (4)
- Risk analysis (3)
- Link between the business strategy and the cyber security strategy (2)
- Scope (1)
- Gap analysis (1)
- Company landscape, both internal as external (1)
- Incidents (1)
- Evaluate before implementation (1)
- Stakeholders (1)

- Scenarios (1)
- Responsibilities (1)
- Baseline measurement (1)
- Vision of the future (1)

TABLE 9: THE CLASSIFICATION OF THE CYBER SECURITY ELEMENTS FOUND IN THE ANALYSIS OF NATIONAL CYBER SECURITY STRATEGIES

	General elements	Cyber specific elements
Drivers	X	
Economic impact	X	
Scope	X	
Definitions	X	
Relation with other strategic documents	X	
Relation with previous strategies	X	
Compliance with laws	X	
Stakeholders	X	
Threats		X
Risks		X
Challenges		X
Opportunities		X
Cyber trends		X
ICT trends		X
Maturity analysis	X	
Comparison with other countries	X	
Analysis of critical infrastructures	X	
Current situation	X	
Vision	X	
Mission	X	
Ambition	X	
Strategic objectives	X	
Strategy guidelines	X	
Key benefits	X	
Action	X	
Action timeframe	X	
Action stakeholders	X	
Action plan	X	
Action measure	X	
Important milestones and CSF	X	
Roles and responsibilities government and stakeholders	X	
Implementation plan	X	
Follow-up	X	
Assessment of effectiveness	X	
Expected effects	X	
Effectiveness of actions	X	
Effectiveness measures	X	
Consequences	X	
Organization	X	
Cooperation	X	
Financing	X	

Although we think these elements are very high-level, some experts discuss, for example, different kinds of developments. For instance, one can look at internal developments, technical developments, and social developments. These results show that the top five most mentioned process steps are analyzing the threats, analyzing the current situation, using a framework, analyzing development, and performing a risk analysis.

However, the list provided above lists both process steps and elements. Since we are only interested in the elements for this section, the process steps are excluded from the analysis. For instance 'using a framework', or 'performing a risk analysis' because they are not so much elements as they are detailed processes that can be followed. In addition, elements that are common to be found in a strategy document, like 'scope', are also excluded from the analysis.

Table 10 shows the results of the analysis where we divided the elements in two categories, namely: generic elements and cyber specific elements. These categories are the same as we used in the analysis of national cyber security strategy elements to support uniformity. The elements we found are used to create a cyber security strategy, which is explained later on.

TABLE 10: THE CLASSIFICATION OF THE CYBER SECURITY ELEMENTS EXPRESSED BY CYBER SECURITY EXPERTS

	General elements	Cyber specific elements
Threats		X
Current situation	X	
Developments	X	X
Assets	X	
Link between the business ambition and the cyber security ambition		X
Company landscape, both internal as external	X	
Incidents		X
Stakeholders	X	
Responsibilities	X	
Risks		X
Vision of the future	X	

6.2.3 Sub analysis

The elements presented in Table 9 and Table 10 show which cyber security specific elements are of importance in creating a strategy. We have seen that we could divide the elements found in the national cyber security strategies and interviews into two categories, general elements and cyber specific elements. We are most interested for this section in the cyber specific elements. If we look closely at both tables, we see that there is some overlap in elements. In both tables we see that threats and risks are important. In addition, trends and developments are also relevant elements. Because we think trends and developments are quite similar, we paired them together. Below we constructed a summary of the cyber security elements that are important to look at when creating a cyber security strategy:

- Link between the business ambition and cyber security ambition.
- Threats;
- Risks;
- Challenges;
- Opportunities;
- Trends & developments;
- Incidents;

The Cookie Factory

ABC wants to grow in the European market by exploring the online channel. This will obviously cause a need for a cyber security strategy and will result in an ambition that states that, amongst others, the online channels should be well protected. Threats the online portal of the cookie factory may face are, amongst others, the unavailability of the portal, the breach of the integrity of orders, and the breach of the confidentiality of customer data and online transactions. As such, this threat may lead to direct or indirect revenue loss, but chances are low this might happen. Therefore this is considered as a medium risk.

We also see some challenges that ABC may face. First of all, the cyber security measures should not be too expensive. Second, the social and the internal environment show several deficiencies that should be handled. However, we also see some opportunities, namely: to expand the business online via a web portal. A quick analysis of trends & developments shows that cyber security attacks are more and more targeted towards the employees and their mobile devices instead of targeting the ICT landscape directly. Furthermore, customer data has been breached in the past when a laptop was stolen and resulted in hundreds of email addresses and passwords being compromised.

6.3 Conclusion

In this chapter we saw that the military, game theory, and business strategy elements are applicable to the cyber security domain. This means that these models can be used for further analysis to create our own method. The complete analysis showed us that we must focus on the social, external and internal environment when determining the need for a cyber security, as well as assessing the current situation. During the assessment, both the cyber security defense capabilities and the cyber security threat landscape are topic of assessment.

The figure below (Figure 16) depicts the different angles to look for during the assessment phase. The entire assessment needs to focus on the following aspects to discover strengths and weaknesses (threats):

- The social environment:
  - Cyber security defense capabilities: e.g. awareness amongst personnel, a sensible level of trust, feeling responsible for the security of personal data, careful use of BYOD.
  - Cyber security threat landscape: e.g. more and more targeted towards employees, personal data and personal smart devices rather than attacks on the enterprise networks.
- The external environment:
  - Cyber security defense capabilities: e.g. information about possible adversaries, no lock-in to a single external company, regular knowledge gathering regarding cyber security from external experts, regular external audits performed at outsourcing partners.
  - Cyber security threat landscape: e.g. increase in zero-day exploits, more complicated attacks, better equipped and organized cyber security attackers.
- The internal environment:
  - Cyber security defense capabilities: e.g. good detection mechanisms, good response mechanisms, qualified security intelligence personnel, up-to-date with latest patches, regular vulnerability scans, regular penetration tests performed.
  - Cyber security threat landscape: e.g. internal IT complexity disguises potential weak spots, internet connectivity everywhere (wired and wireless).

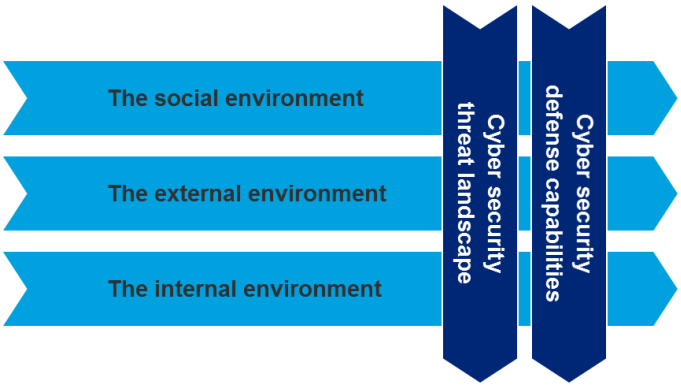


FIGURE 16: THE CYBER SECURITY SPECIFIC APPLICATION OF THE SOCIAL, EXTERNAL, AND INTERNAL ENVIRONMENT

As discussed before, the assessment of the social, external and internal environment can be used to establish the current situation of cyber security defense capabilities and the cyber security threat landscape and give input for the need for a cyber security strategy.

During the search for cyber security elements in the national cyber security strategies, we saw generic elements that are always in strategies but also cyber security related elements. Both groups had an overlap with what was said in the interviews. Because there is multiple support for these elements, we were confident to analyze them further. Looking at these elements once more, we saw an evident pattern across the elements.

As such, we tried to group these elements into logical process steps, which resulted in a deduced method to come to a cyber security strategy (illustrated in Figure 17):

1. Determine the strategic drivers and scope;
2. Analyze the cyber threat landscape;
3. Analyze the AS-IS situation;
4. Analyze the TO-BE situation;
5. Decide on the countermeasures;
6. Decide on implementation measures.

We made a detailed description of each method step, which can be found in the appendix (section 13.2). Since this is the only cyber security strategy method we have, it provides the basis together with some adaptations, for our conceptual method. More about this can be found in the next chapter.

		EU Countries																Non-EU Countries													
		AUT	BEL	CZE	EST	FIN	FRA	ITA	DEU	HUN	LVA	LTU	NLD	POL	SVK	ESP	GBR	AUS	CAN	JPN	KEN	MNE	NZL	NOR	SGP	CHE	TUR	UGA	USA	GEO	KOR	TTO
1. Strategic drivers & scope	drivers	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
	economic impact							X			X						X	X	X					X		X						
	scope																	X									X					
	definition cyber security	X	X			X		X		X			X					X	X					X				X				X
	glossary	X	X			X		X	X		X	X		X							X	X	X	X			X					
	relation with other strategic documents	X		X	X	X				X	X	X	X	X	X	X	X	X			X	X		X		X		X				X
	relation with previous strategies				X		X						X							X					X							
	compliance with laws		X						X					X	X	X		X			X	X						X				
	stakeholders			X	X					X			X	X			X		X	X	X	X	X			X						
2. Cyber threat landscape	threats	X					X	X	X	X			X			X	X	X	X	X	X	X	X	X	X	X		X				X
	risks	X														X				X		X				X	X	X				
	challenges				X			X						X							X	X		X					X			
	opportunities	X																														
	cyber trends		X		X				X				X				X			X	X											
	ICT trends		X		X								X					X		X					X			X				X
3. AS-IS situation	maturity analysis																				X							X				
	comparison with other countries														X													X				
	cyber security perspective EU														X																	
	SWOT analysis																											X				
	analysis of critical infrastructures																									X		X				
	analysis current situation				X					X	X				X							X				X		X				
4. TO-BE situation	vision				X	X				X							X								X			X				X
	mission																								X			X				
	ambition	X			X	X	X				X	X	X					X	X	X	X			X	X	X	X		X	X	X	
	- guiding principles	X		X	X	X					X					X	X	X		X						X	X	X	X		X
	strategic objectives	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X
	- strategic priorities														X		X	X					X	X					X			
	- strategic measures			X																												
	key benefits																				X											
5. Countermeasures	action	X	X				X	X		X	X	X	X	X	X	X	X	X	X	X		X		X		X	X	X	X	X	X	X
	action timeframe											X	X		X			X		X		X					X	X		X		
	action stakeholders											X	X									X					X	X		X		
	action plan											X	X				X					X		X			X	X		X		X
	action measures	X										X																				
	operational goals																															X
	important milestones and CSF																											X				
	roles and responsibilities government					X	X	X					X		X		X	X		X			X	X			X					X
	roles and responsibilities stakeholders		X			X	X	X	X				X		X		X	X		X		X		X			X	X		X		X
6. Implementation	implementation	X							X			X		X		X									X		X					
	follow-up	X									X				X			X		X							X					
	assessment of effectiveness													X				X														
	- expected effects													X																		
	- effectiveness of actions													X																		
	- effectiveness measures													X	X												X					
	consequences													X			X															
	organisation													X		X		X				X						X				X
	cooperation							X						X					X			X			X	X						
	financing													X	X			X										X				

FIGURE 17: GROUPING OF STRATEGY ELEMENTS FROM NATIONAL CYBER SECURITY STRATEGIES

7 Towards a conceptual method

We now have a clear idea which elements are important to incorporate in our method to create a cyber security strategy. This information provides, amongst others, input to answer the main research question 'How can a corporate organization develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition?' As mentioned in chapter 2, the goal of the research is to create a well-thought method for formulating a cyber security strategy, to answer the main research question. This chapter presents a conceptual method, based on the previous chapters, to formulate a cyber security strategy.

7.1 Input for the conceptual method

The previous chapter provided the basis for our conceptual method, namely the deduced method from the analysis of national cyber security strategies, consisting of the following steps:

1. Determine the strategic drivers and scope;
2. Analyze the cyber threat landscape;
3. Analyze the AS-IS situation;
4. Analyze the TO-BE situation;
5. Decide on the countermeasures;
6. Decide on implementation measures.

However, this method is only based on the national cyber security strategies. We want to take into account all information we gained in this research to create our method, and the elements found through this analysis were grouped on similarity, not on where it appeared in the national cyber security strategy documents. This means that the above given method needs to be adapted to meet our results from chapter 4, 5, and 6. These results are listed below:

- The drivers of a cyber security strategy (see section 5.4);
- The link between the cyber security ambition and the organization's ambition (see section 5.5);
- The company landscape (see section 6.1 and 6.2);
- The cyber threat landscape (see section 6.2);
- The general elements deduced from the cross-border analysis of national cyber security strategies (see section 6.2.1 and 13.2);
- The results from the interviews (see section 13.1).

We are now going to explain how we transformed the method steps listed above to the conceptual method we developed. First of all, in addition to the analysis of national cyber security strategies showing the importance of determining the strategic drivers, in the interviews it also became apparent that there must be a need for a cyber security strategy before actually creating one. It showed that there are different reasons for such strategies, and we can use these reasons to guide the strategist in the process of determining a need for a cyber security strategy. In the literature (section 5.4 and 6.1.4) we also described several reasons to create a cyber security strategy and showed how the assessment of the social, external, and internal environment can help determine this. As such, we also think it is important that the first step should be to determine the strategic drivers, or need for a cyber security strategy. In addition, in this first stadium of creating a cyber security strategy, we think it is important to already stress the cyber security ambition and strategic objectives which can later be communicated to stakeholders. Although the analysis of national cyber security showed that the ambition is related to the TO-BE situation phase, the actual documents show that the ambition and strategic objectives are usually already stated at the beginning of the document. Therefore, we think the first step should be 'Identify the need for a cyber security strategy and determine the ambition'. More detail about the sub activities in this step can be found in section 7.3.1.

With the first step we only focus on the 'determine the strategic drivers' part of the original step 'determine the strategic drivers and scope'. Since the first step was extended with determining the ambition and strategic

objectives, the second step goes into depth on the scope of the strategy and is named ‘define the cyber security strategy project setup’. Besides that the analysis of national cyber security strategies show the importance of defining the scope of the strategy, the experts also mention this. We therefore call the second step ‘define the cyber security strategy project setup’ where project specific matters, like scope, are identified. More detail about this step can be found in section 7.3.2.

The next step we found in the analysis of national cyber security strategies is to analyze the cyber threat landscape. As mentioned in section 6.2.3, we also think it is really important to analyze the cyber threat landscape separately. In addition, the experts also use cyber threat landscape analysis to base their cyber security strategy on (see section 13.1.1.5). As such, the third step in our conceptual model is ‘analyze the landscape’. More information on how one can analyze the landscape can be found in section 7.3.3.

The fourth step is based on analyzing the AS-IS and TO-BE situation as found in the analysis of national cyber security strategies. We combined these steps into one general step ‘perform a gap analysis’. A gap analysis has been named several times as an important step by experts and focuses on the difference between the AS-IS and TO-BE situation. We give multiple ways to perform such a gap analysis, based on the national cyber security strategies and expert opinions. More information about all sub activities can be found in section 7.3.4.

The following two steps are likewise to the ones found in the national cyber security strategies, ‘decide on the countermeasures’ and ‘decide on the implementation measures’. However, we have found evidence in the interviews of using scenarios. A short literature review showed that scenarios are a useful tool for management (e.g. Leemhuis, 1985) to develop multiple possible outcomes based on the current situation, in order to make decision making more easy. We think scenarios are a useful tool to determine different options of strategic measures to overcome the gaps found and to meet the set ambition and strategic objectives. Therefore, step five is ‘define multiple scenarios’ for possible countermeasures. More information can be found in section 7.3.5

Based on the scenarios from the previous step, the fifth step is: ‘elaborate on chosen scenario’. This step resembles the ‘decide on implementation measures’ step from the national cyber security strategies. As can be seen in section 7.3.6 the step ‘elaborate on chosen scenario’ is focused, amongst others, on the effects of the cyber security measures on the organization. More information about all sub activities can be found in section 7.3.6.

To summarize, Figure 18 shows the mapping of the method steps from the analysis of national cyber security strategies on the conceptual method as described above. In addition, a full table on the exact mapping between the literature, interview results, and analysis of national cyber security strategies can be found in appendix section 13.4.1.

As such, we have transformed the method deduced from the national cyber security strategies to the following method:

1. Identify the need for a cyber security strategy and determine the ambition;
2. Determine the scope and stakeholders;
3. Analyze the landscape;
4. Perform a gap analysis;
5. Define multiple scenarios;
6. Elaborate on chosen scenario.

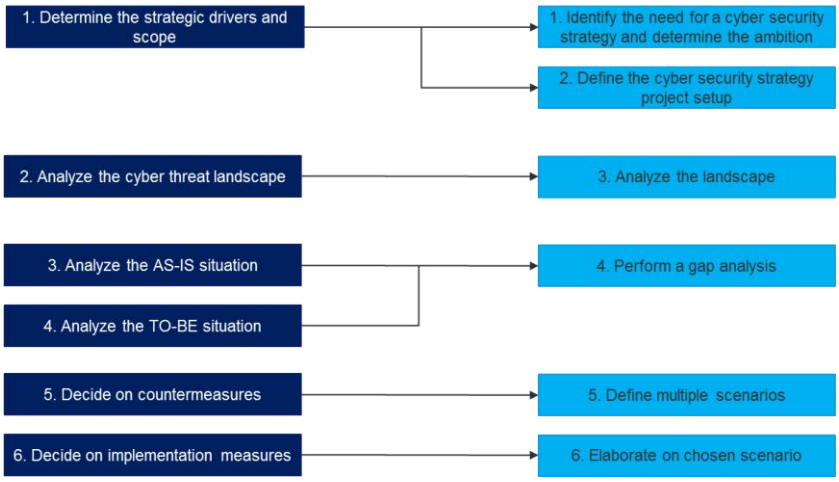


FIGURE 18: MAPPING OF THE METHOD STEPS FROM THE ANALYSIS OF NATIONAL CYBER SECURITY STRATEGIES (DARK BLUE) ON THE CONCEPTUAL METHOD (LIGHT BLUE)

7.2 Introduction to the conceptual method

The steps within the previous section give an outline of the high-level steps of our conceptual method. The conceptual method we created is based upon literature, interviews, and the analysis of national cyber security strategies, as described in the previous section. After validation, the conceptual method is updated to a final version.

As shown before, the method consists of six consecutive steps. Every step has sub activities, and related deliverables. In order to make the need to document decisions and evidence (of analyses) explicit, we have chosen to present the method using a process-deliverable diagram. A process-deliverable diagram is divided into two sections, which are linked to each other. On the left side, one can find the activities and on the right side, one can find the deliverables. Every output deliverable is automatically input for the next activities. More information about the syntax of this modelling method can be found in van de Weerd and Brinkkemper (2008).

Additionally to presenting our conceptual method, we have several side notes. During the interviews it became apparent that, in order to successfully create and implement a cyber security strategy, several conditions may apply. There should be buy-in from the management board and as such, they should propagate their support. In addition, the cyber security ambition and strategy should be deduced from the organization's ambition and/or strategy. Also, when creating the cyber security strategy, all stakeholders should be involved during the creation phase of the cyber security strategy. And lastly, this cyber security strategy should be evaluated every year (e.g. is the current cyber security strategy still relevant in the changing cyber threat landscape? Are project executed as planned? Is the driver still the same?), and renewed after a maximum of three years.

In addition, to execute the activities for creating the actual cyber security strategy, we acknowledge the following three roles:

- The management board;
- The responsible person(s) for group wide security management (with regard to ease of use, this is called the steering committee[10]);
- The stakeholders.

[10] Not every organization will create a project with a steering committee to establish a cyber security strategy. Therefore a responsible person or multiple persons for group wide security management is a more generic term. This person can be a CISO, or a CRO, or even security managers.

And finally, with every process deliverable diagram a table is constructed that explains all activities and concepts. These tables can be found in section 13.4 and thus provide additional information to the constructed method. It is advised to consult this information when developing a cyber security strategy, so that everyone is on the same page about what the activities constitute and the concepts mean.

The full conceptual method is explained in the next section.

7.3 The conceptual method

So far we have only introduced the six high level steps. In this section we describe every method step in depth, which also shows how this method is specifically to create a cyber security strategy. Several examples are given to explain the method steps in a more practical way. Firstly, our conceptual method is presented in a structured, process-deliverable diagram and can be found in Figure 19. A plain text version is present in appendix section 13.4

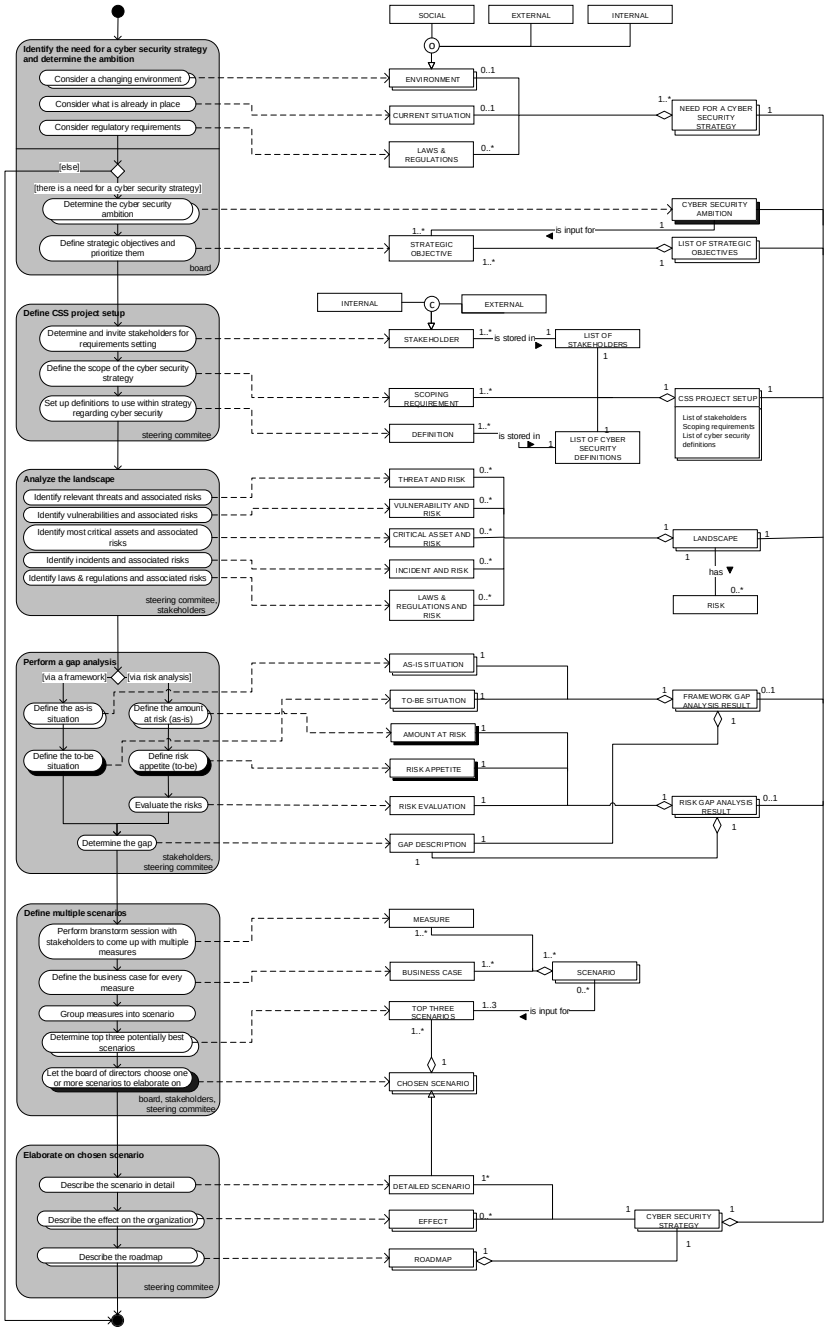


FIGURE 19: THE CONCEPTUAL CYBER SECURITY STRATEGY METHOD

7.3.1 Step 1: Identify the need for a cyber security strategy and determine the ambition

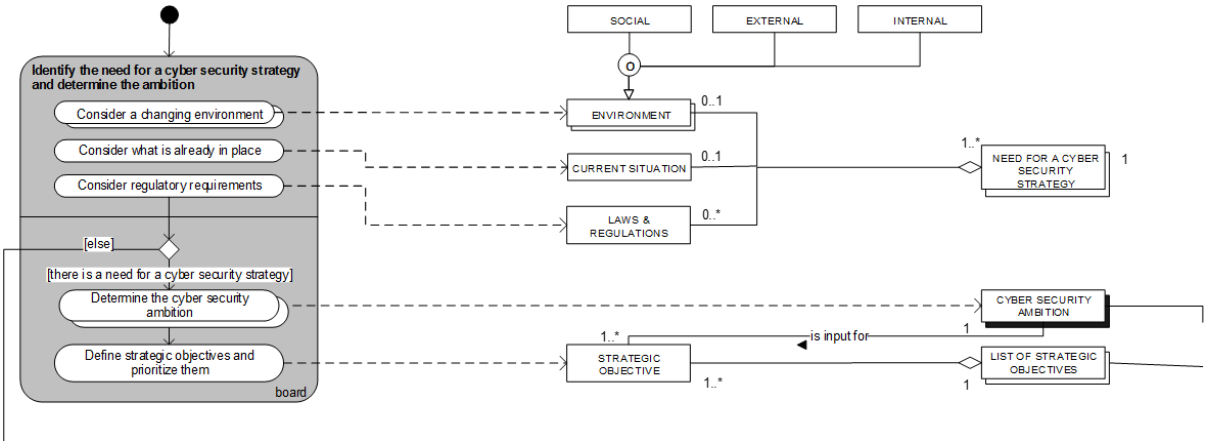


FIGURE 20: PDD STEP 1 IDENTIFY THE NEED FOR A CYBER SECURITY STRATEGY AND DETERMINE THE AMBITION

The first step is to decide on the need for a cyber security strategy (Figure 20). Without a proper driver, succeeding at establishing and implementing a cyber security strategy is harder. The management board should deliberately ask themselves why they want a cyber security strategy. This can be done by considering a changing environment, by looking high-level into the cyber threat landscape, the position of the organization in the marketplace, the value of information stored and the risks involved when this information gets exposed, or the developments in the field and the consequence of de-perimeterization [11] (Figure 21). In addition, the management board should consider the current situation regarding the cyber security strategy and controls in place. Also, the board should look into laws and regulations that might oblige them to have a certain cyber security strategy. For instance, the 'Nederlandse Bank' insists that all Dutch banks and insurance companies comply with the CobiT standard. In section 5.4 we saw that often the cyber security strategy is initiated by external regulators to comply with laws and regulation. When the need for a cyber security strategy is identified, the management board should document all their decisions.

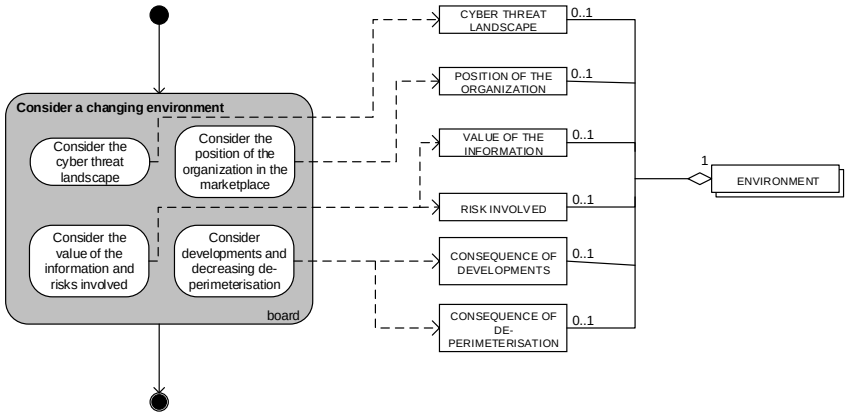


FIGURE 21: PDD STEP 1.1 CONSIDER A CHANGING ENVIRONMENT

Once the need for a cyber security strategy is established, the management board should determine an ambition. This ambition should state their high-level aspirations with cyber security. To establish the cyber security ambition, the management board should identify the organization's ambition and link this to the cyber security ambition (Figure 22). Cyber security should inherently support the organization's operations and therefore the organization's

[11] De-perimeterization concerns the fading of the technological boundaries between organizations and the external environment. So, information from the organization and its systems are not bound to physical location anymore and therefore more vulnerable.

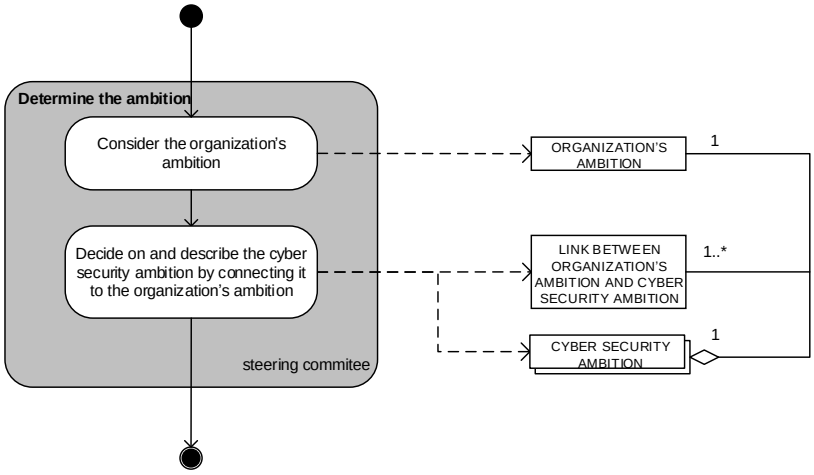


FIGURE 22: PDD STEP 1.4 DETERMINE THE CYBER SECURITY AMBITION

ambitions. Once this is done, the management board should make the cyber security ambition more practical and conveyable to the public by making it coherent, powerful, and realistic or by incorporating an ambition level.

For instance, we suggest that one could think of industry-standard, industry-leading, and overall leading. Industry standard means that the company wants to do is what is recognized as standard in the industry and what most competitors have implemented. Industry-leading means that the company wants to excel in their industry with regard to cyber security. The company wants to have the best cyber security compared to industry competitors. And lastly, overall leading means that the company want to have the best cyber security outside of their own industry. They want to be leading, innovative, and of cyber security.

When the cyber security ambition is determined, strategic objectives can be defined and prioritized. Strategic objectives are high-level objectives based on the ambition, necessary for the successfulness of the strategy and should be SMART (specific, measurable, achievable, relevant, time-bound). These decisions and results should be documented, both for the cyber security ambition and the associated strategic objectives.

An example of an ambition with associated strategic objectives is from the Dutch cyber security strategy 2.0 (the Netherlands, 2013, p. 8-9):

> *The Netherlands is a leader in cyber security:*
>
> - Dutch society knows how to make safe, optimal use of the advantages of digitization;
> - Dutch businesses and the research community are pioneers in 'security by design' and 'privacy by design';
> - Together with its international partners, the Netherlands is part of a progressive coalition that seeks to protect fundamental rights and values in the digital domain.
>
> The following strategic objectives are presented that align with the cyber security ambition:
>
> - The Netherlands is resilient to cyber-attacks and protects its vital interests in the digital domain;
> - The Netherlands tackles cybercrime;
> - The Netherlands invests in secure ICT products and services that protect privacy;
> - The Netherlands builds coalitions for freedom, security, and peace in the digital domain;
> - The Netherlands has sufficient cyber security knowledge and skills and invests in ICT innovation to attain cyber security objectives.

If the management board cannot identify a need for a cyber security strategy, we advise them not to continue formulating a cyber security strategy until there is a legitimate driver.

7.3.2 Step 2: Determine the cyber security project setup

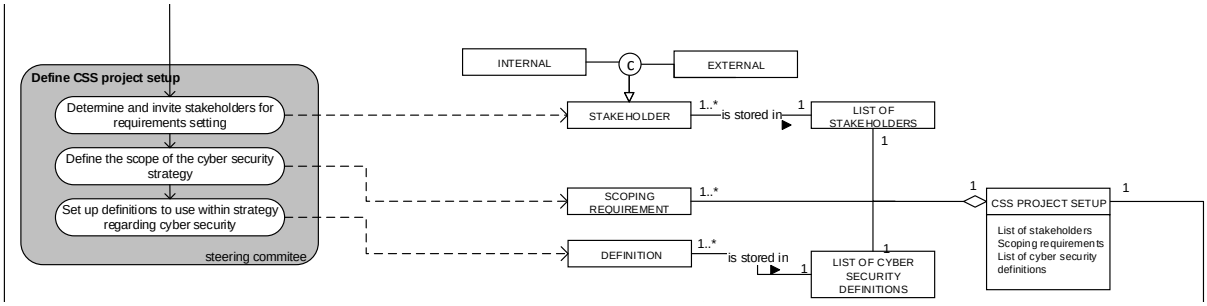


FIGURE 23: PDD STEP 2 DETERMINE THE SCOPE AND STAKEHOLDERS

Once there is a need for a cyber security strategy established and decided upon a cyber security ambition, the next step is to determine the scope and stakeholders (Figure 23). First, the steering committee should determine stakeholders and what their stake is in the cyber security strategy, and invite them for requirements setting. One could distinguish different stakeholders with certain priorities based on their stakes in the cyber security strategy. We suggest the following distinction:

- Business leaders (priority 1): to learn the needs from the business;
- IT (priority 2): to understand the current state of IT security;
- Privacy and Security (priority 3): to learn privacy and information security requirements;
- Risk Management (priority 4): to learn the current state of cyber security risk management practices.

The next step is to define the scope of the cyber security strategy. What falls within the cyber security domain and what does not? And finally, the steering committee should set up definitions to use within the cyber security strategy. For instance, what does cyber security mean to the organization?

The steering committee should document all decisions regarding the stakeholders, scope, and definitions in a so-called project setup document.

7.3.3 Step 3: Analyze the landscape

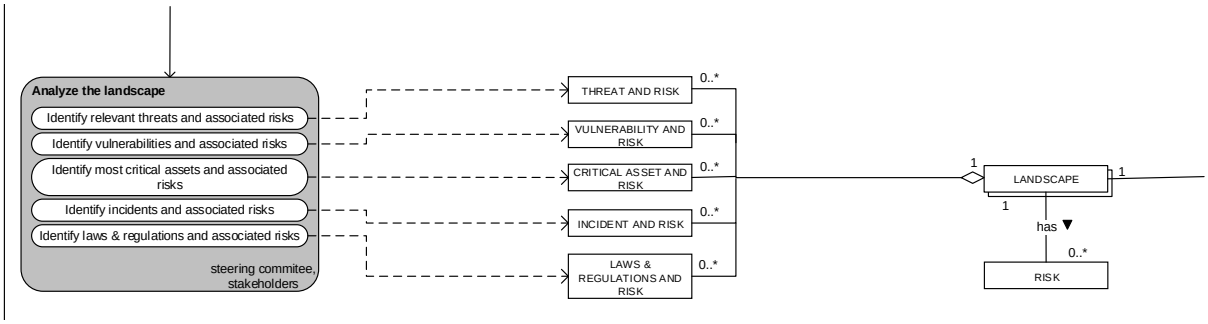


FIGURE 24: PDD STEP 3 ANALYZE THE LANDSCAPE

Now that the project setup has been determined, the steering committee, together with the stakeholder, can analyze the landscape in depth (Figure 24). With the landscape we mean the aspects of the cyberspace influencing the organization of interest, both internally and externally. This means that one should identify the critical assets of the organizations and the risks associated when something happens to the confidentiality, integrity, or availability of this asset. In addition relevant threats to the organization and their critical assets, and their associated risks. But also identify vulnerabilities and their associated risks. Furthermore, one should consider the incidents from previous

weeks or months, and what risks were associated with these incidents and what risks exist when this incident is happening again. And finally, laws & regulations should be identified and what risks are associated when one does not oblige to the regulation. The risks should be given a rating based on the probability times the impact formula. The results of the landscape analysis and the risks associated are registered in a document.

An example of considering threats to the critical assets of an organization:

Bank X has a number of customer accounts that store money. As such, one of their critical assets is the customer accounts, and another critical asset is money. A threat to these critical assets is that someone hacks into the system and steals customer data and/or money from the customers. If this happens, it results in reputation and financial damage for the bank.

7.3.4 Step 4: Perform a gap analysis

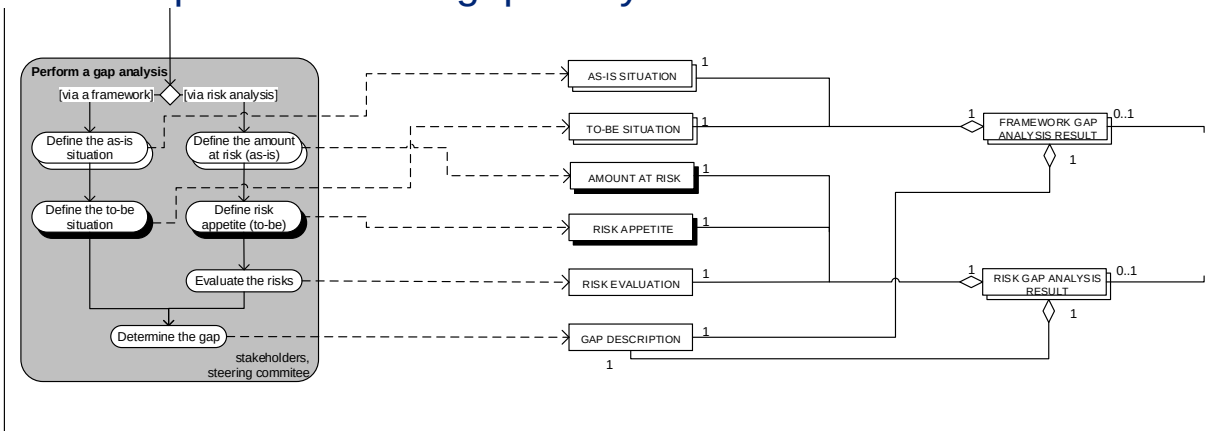


FIGURE 25: PDD STEP 4 PERFORM A GAP ANALYSIS

Once the landscape has been analyzed, a gap analysis must be performed by the steering committee (Figure 25). To determine the gap, one could choose between two approaches, performing a risk analysis or using a framework. A framework is usually used as a baseline and consists of a basic set of measures. These measures are so generic that they can be used for every organization. A risk analysis is, however, performed specifically for the organization of interest. We suggest that this approach should therefore only be used when the organization is mature enough. Performing a risk analysis is complex, labor-intensive, and requires a lot of knowledge on conducting it, while using a framework is, simply said, checking a list. Below we present all activities associated with using a framework to determine the gap and all activities associated with performing a risk analysis.

- *Using a framework.*
  A common approach for determining a strategy is by using a framework (Figure 26). With a framework we mean standards (e.g. ISO2700x), frameworks (e.g. CobiT), and maturity models (e.g. NIST). These can be used as a checklist to see what is already in place, and to see what should be implemented to, for instance, comply with standards, or to gain a higher maturity. The first step is to define the as-is situation with a framework chosen by the steering committee and optionally, benchmark these results against results from peers in the industry (Figure 26). The second step is to use the framework to define the to-be situation (see Figure 25 again). The difference between these situations results in zero or more gaps.

An example of a commonly used framework is the NIST maturity model. It is developed by the Government of the United States of America, and specifically made for organization's that manage critical infrastructures. There is a clear link in the model between the business drivers and the cyber security activities that should be undertaken. In addition, a clear link is made with risks, and according to the government of the USA it provides "a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risks for those processes, information, and systems directly involved in the delivery of critical infrastructure services" (NIST, 2014, p. 3). According to several experts, the NIST model is primarily practical in use and easy to communicate to the board.

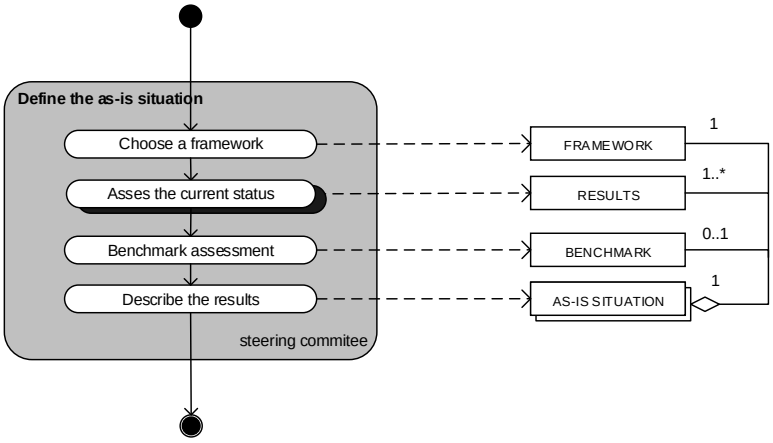


FIGURE 26: PDD STEP 4.1A DEFINE THE AS-IS SITUATION

- *Performing a risk analysis.*

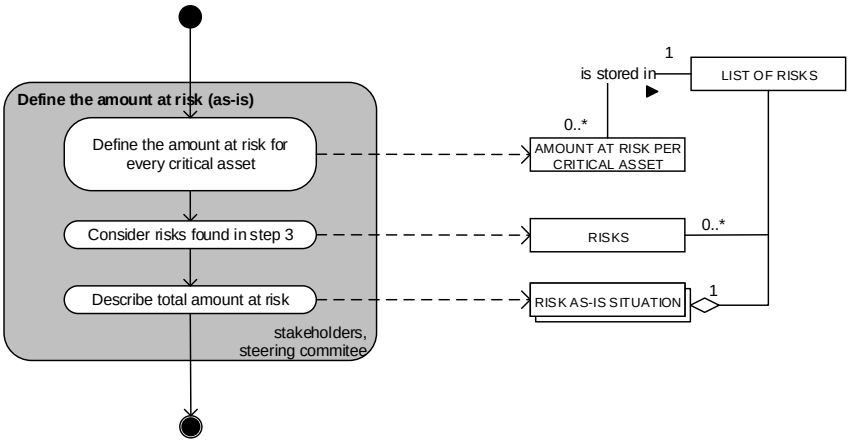


FIGURE 27: PDD STEP 4.1B DEFINE THE AMOUNT AT RISK (AS-IS)

A risk analysis is performed by, first, defining the as-is situation (Figure 27). This is done by defining the amount at risk for every critical asset and considering the risks found in the previous step. The amount at risk can be determined by assessing the degree to which the confidentiality, integrity, and availability of every critical asset is affected. Second, the to-be situation is assessed in the form of a risk appetite. The risks appetite is the amount of risk the management board is willing to take. Next, the risks are evaluated, meaning that the significance of a risk is determined. And finally, the gap between the risk appetite (the to-be situation) and the amount at risk (the as-is situation).

The results of the gap analysis should be elaborated in a document, and communicated to the stakeholders.

7.3.5 Step 5: Define multiple scenarios

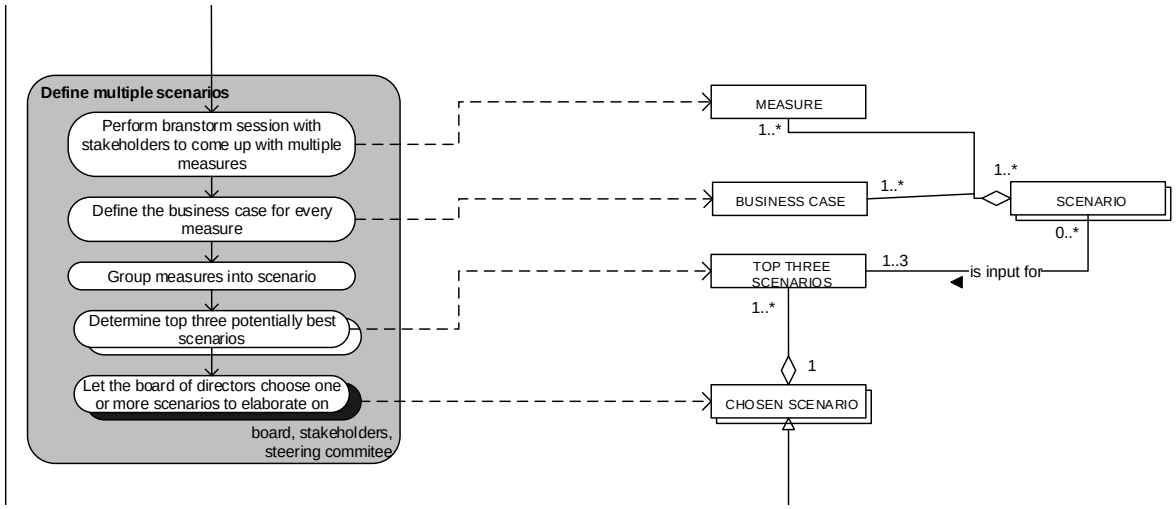


FIGURE 28: PDD STEP 5 DEFINE MULTIPLE SCENARIOS

The next step is to define multiple scenarios that contain packages of measures to close the gaps and adhere to the strategic objectives (Figure 28). In order to do so, it is first necessary to perform a brainstorm session with stakeholders to come up with multiple measures. After this is done, the steering committee considers the implicit and explicit cost and benefits for every measure. Next, the steering committee should group the measures in scenarios.

This grouping process can be based on, for example, time necessary, resources necessary, money necessary or risk mitigation. For instance, the first scenario is the cheapest to implement and covers only the basic gaps, the second scenario is the most expensive to implement, but covers all gaps. The third scenario is not cheap nor expensive, and covers all gaps but on a basic level.

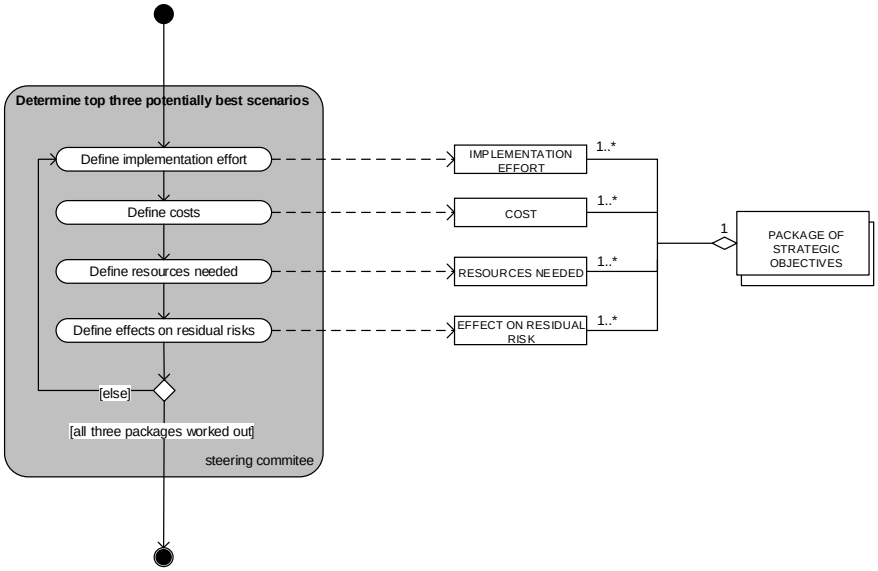


FIGURE 29: PDD STEP 5.4 DETERMINE TOP THREE POTENTIALLY BEST SCENARIOS

Once scenarios are identified, a top three should be determined on to make the choice of a scenario easier for the management board (Figure 31). For all three scenarios, the steering committee should define the implementation effort, involved costs, resources needed, and the residual risk. The last activity is that the management board decides on one or more scenarios to implement. This decision is documented.

7.3.6 Step 6: Elaborate on chosen scenario

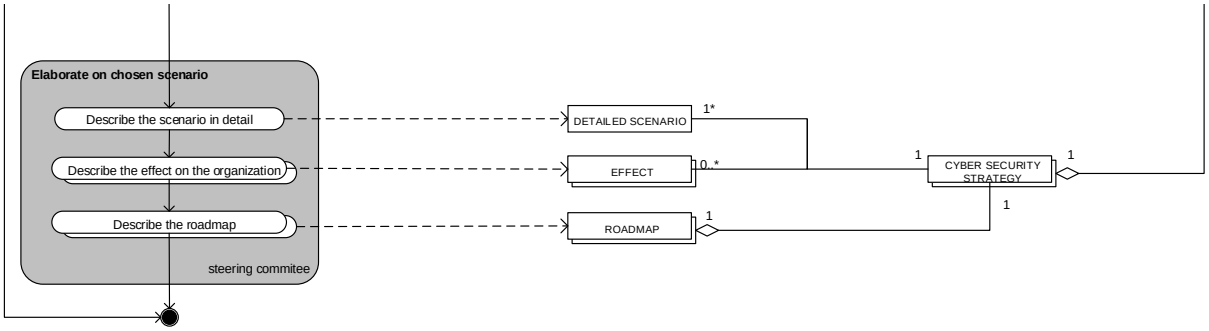


FIGURE 30: PDD STEP 6 ELABORATE ON CHOSEN SCENARIO

In this step, the chosen scenario from the previous step by the management board is elaborated on (Figure 30). The chosen scenario is first described in detail. Next, the effect on the organization from implementing the chosen scenario is described. The steering committee should determine the effect on the staff, their skills and knowledge. In addition, the effect on the business processes should be considered, as well as on the technologies used, the culture of the organization and the consequences for the roles and responsibilities related to cyber security controls in place. This last one can be explicated by using a RACI matrix. RACI stands for Responsible, Accountable, Consulted, and Informed, and is used to map responsibilities to persons.

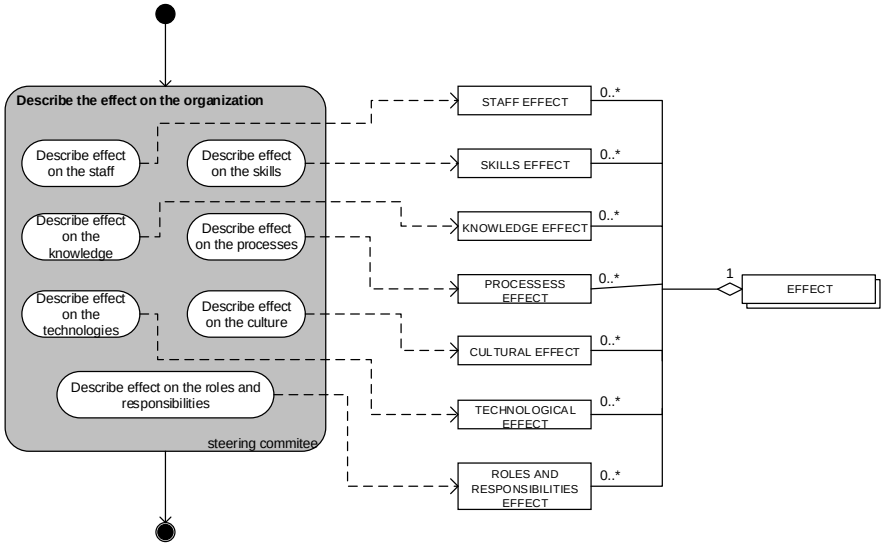


FIGURE 31: PDD STEP 6.2 DESCRIBE THE EFFECT ON THE ORGANIZATION

And finally, the roadmap is defined (Figure 32). To define the roadmap, the steering committee should define milestones, deadlines, resources, and collaboration needed to implement the strategy. In addition, they should decide on what quality is acceptable for the implementation of the strategy that could be used in assessing the effectiveness afterwards. Besides, other effectiveness measures should be defined as well. An example of an implementation plan for a strategic objective is presented in Table 11.

.

These decisions are documented and the roadmap is communicated to the stakeholders and the staff responsible for implementing the strategy.

A cyber security strategy document can then be created based on the documents containing the need for a cyber security strategy, the cyber security ambition, the project setup, the landscape analysis, the gap analysis result, the detailed scenario, and the roadmap.

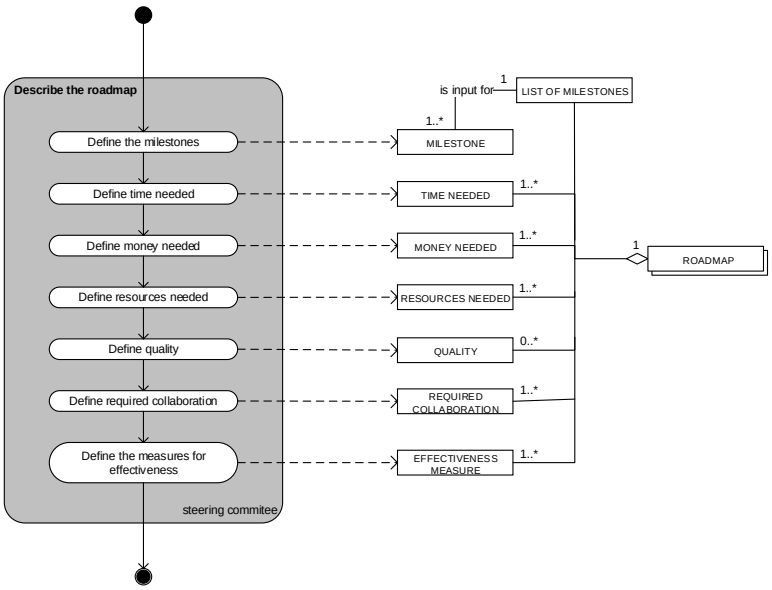


FIGURE 32: PDD STEP 6.3 DESCRIBE THE ROADMAP

TABLE 11: IMPLEMENTATION PLAN EXAMPLE

Objective	Measure	Responsible	Costs	Resources	Effectiveness measure	Deadline	Completed after 1 year	Completed after 2 years	Completed after 3 years
Objective #1	Measure #1								
	Measure #2								

8 Validation

The conceptual method presented in the previous chapter should be validated in order to prove its accuracy and validity. This is done via two ways which correspond to the evaluation techniques we described via the research framework of Hevner et al. (2004, guideline 4) . First, we validated our method with experts in a workshop session. Second, we validated our method by testing it against a real case. Evaluating our conceptual method twice provides research rigor (see section 3.2).

8.1 Workshop session validation

The workshop session was held with 17 experts, as indicated in the research approach section. During the workshop session feedback was given about the conceptual method.

The feedback from the workshop session primarily showed us that names for activities were confusing and incorrect. For instance, it was mentioned that the term 'project' in the step 'define the cyber security strategy project setup' was confusing since the creation of a cyber security strategy should not necessarily be carried out in project form. Also, several groups mentioned that the cyber security strategy should be part of the overall business strategy. By just considering the organization's ambition, you will not do this. Literature also strongly pointed out that a cyber security ambition cannot be seen separately from the organization's ambition. Furthermore, there was a misunderstanding between the different activities that were mentioned in the first step and the same activities mentioned in step three or four. Therefore, we should make it more explicit that the first step focuses on the external landscape and the, current, third step 'analyze the landscape' is more focused on the internal landscape. And finally, the last major comment was that there are multiple granularity levels within the method. For instance, one group mentioned that the first three steps were actually focused on creating a strategy, whereas the other three steps were focused on creating a plan to implement the strategy. This meant that we should adjust the method to show one level of granularity, the level that is focused on merely creating a cyber security strategy.

The workshop session validation also shows that it is good to review every step and the previous steps after completion. Also, it is shown that the first step (i.e. 'identify the need for a cyber security strategy and determine the cyber security ambition') is the most important and difficult step. But also that steps one, two, and three provide the basis for the following steps. Therefore, these must be devised thoroughly before continuing to the next steps. Also, getting management buy-in is a crucial issue in the process of creating a cyber security strategy. This buy-in should be given when a need for a cyber security strategy is established. And finally, it is said that performing a gap analysis is the most time-consuming step to carry out in practice, due to the need to conduct interviews, benchmark results, and use and understand frameworks.

8.2 Case study validation

Furthermore, the conceptual method was tested by comparing it to a real cyber security strategy document. The only disadvantage is that a cyber security strategy document only partly reveals the followed method. Therefore, we held an interview with a member of the project responsible for creating this cyber security strategy.

What we mainly saw from the analysis is that the drivers and the ambition are well formulated. The drivers show us that they thought about the changing environment, the threat landscape, the position in the marketplace, and regulatory requirements. However, they did not consider the value of the information and risks involved but indicate that this is important to consider. In addition, a cyber security ambition was stated. Also, visions per important domain are established. The cyber security ambition is also linked to the organization's ambition. Furthermore, the cyber security strategy case also made use of stating guiding principles for the creation of the strategy. This is considered useful to set expectations up front according to the project member. The same accounts for having

multiple visions when different categories to which the strategy applies are mentioned or when frameworks are used.

Within the cyber security strategy project setup, stakeholders were determined and invited for requirements setting according to the project member. And although we did not see in the document that the scope of the cyber security strategy was determined, it was in fact determined but not written down. Furthermore, definitions to use within the strategy regarding cyber security were not set. The project member values this step as very important and mentioned that it should have been added to the cyber security strategy of the case organization.

Furthermore, relevant threats, incidents, and laws & regulations are analyzed as part of the landscape analysis. Vulnerabilities and critical assets were not analyzed, but are considered to be useful and to add value to the analysis when added. The project member added that threats should be communicated and discussed with stakeholders. Also, laws and regulations may also be interesting to look at from an internal perspective. The project member added that is useful to evaluate the landscape analysis results with stakeholders and adjust the results if necessary.

The fourth step, perform a gap analysis, is done elaborately in the case. The NIST model is used as a framework to assess the current and target situation. A separate excel sheet gives a detailed overview of the framework analysis. The only thing we saw in the case was that only partly a benchmark assessment was conducted. This was, according to the project member, partly performed but not document. The case study shows us that they also looked at which projects are currently running related to cyber security. This is seen as a relevant step by the project member, so that current activities can be mapped and compared to what should be done. In addition, the project member added again that it is very useful to evaluate the analysis results with stakeholders and adjust the results if necessary.

Next, the cyber security strategy case did not make use of scenarios. Business cases for every measure were also not defined. However, they did perform multiple sessions with stakeholders to come up with multiple measures. The project member mentioned that scenarios were not used, but they did have multiple options for certain measures with regard to costs. Having multiple options and present these to the decision makers is considered very useful by the project member.

And finally, a target operating model and a roadmap are used to elaborate on the chosen scenario, or in this case the chosen strategy. The target operating model is a deliverable of the strategy, but describes the effect on the organization in detail. The roadmap also elaborates on milestones, time needed, money needed, resources needed, and the collaboration needed. The cyber security strategy case, however, does not elaborate on the effect on the technologies and culture whereas both are considered important to consider in the process of creating a cyber security strategy. Furthermore, quality and measures for effectiveness are not describes as part of the roadmap. Quality is not as important to define, but measures for effectiveness in the form of key performance indicators are, according to the project member.

In addition, the cyber security strategy case also defines next steps. The project member mentions that this is very useful, but should be incorporated as a precondition to formalize the process of executing the roadmap. These results are used to change the conceptual method.

8.3 Changes to the conceptual method

Based on the two validations, several changes had to be made. First of all, we went from a method that has six underlying steps to a method that has four underlying steps to create a cyber security strategy. Step three and four (i.e. ‘analyze the landscape’ and ‘performing a gap analysis’ respectively) in the conceptual method were merged into step three ‘analyze the landscape’. The same accounts for step five and six in the conceptual method (i.e.

‘define multiple scenarios’ and ‘elaborate on chosen scenario’ respectively), who merged into step four, ‘describe multiple strategic objectives and associated tasks’.

We applied the general comments given in the case study and the workshop session to all steps. This means that in the first step (i.e. ‘identify the need for a cyber security strategy’) we modified, inserted, and deleted several activities. We chose to have the scope identified after the driver has been established, because it is necessary to know the scope of the strategy before determining on a cyber security ambition. Optionally, one should determine cyber security visions per domain the cyber security ambition applies to, as was found in the case study. Furthermore, we think that the organization’s ambition should be identified instead of considered, and should be made part of the organization’s strategy besides merely describing the connection. And finally, the guiding principles and desired outcomes of the cyber security strategy should be defined, according to the experts in the workshop session and the case study. This gives more guidance through the rest of the steps to create boundaries and constraints for the creation of the cyber security strategy.

The second step, now known as ‘define the cyber security strategy operating setup’ deals not only with determining and inviting stakeholders for requirements setting, and setting up definitions to use within the cyber security strategy regarding cyber security. One should also define the governance of the cyber security strategy, to show who is responsible, accountable, consulted, and informed during the creation of the cyber security strategy and when it is created. In addition, strategy dependencies should be mapped. For instance, on which strategies is the cyber security strategy based? And finally, experts find it useful to describe the desired interactions with key stakeholders at the start of the creation of the cyber security strategy, so that these stakeholders know what is expected of them during the process and afterwards. As such, we added this activity to our conceptual method.

The third step (i.e. ‘Analyze the landscape’) groups the conceptual step three and four together (i.e. ‘Analyze the landscape’ and ‘perform a gap analysis’), and focuses on analyzing the social, external, and internal landscape to identify relevant threats, critical assets, vulnerabilities, and incidents the organization faces. Based on the results from the case study, we also added that requirements (i.e. internal and external laws & regulations) should be identified, running activities related to cyber security as well as identifying the internal culture. In addition, we suggest that the results from the landscape analysis should be evaluated with stakeholders and adjusted if necessary. Also, we added the gap analysis to this step but follows the same structure as in the conceptual method. During the framework approach, one can also optionally determine cyber security visions per framework domain the cyber security ambition applies to. In addition to defining and prioritizing the gaps, the gap analysis should be evaluated with stakeholders and adjusted if needed. Furthermore, problem areas should be defined based on the landscape and gap assessment as a logical consequence of adding the above described change. This is input for deciding on the strategic objectives in the next step, ‘describe multiple strategic objectives and associated tasks’.

Step four (‘Describe multiple strategic objectives and associated activities’) has been composed from step five and six in the conceptual method (i.e. ‘define multiple scenarios’ and ‘elaborate on chosen scenario’). This step is now focused on defining and describing strategic objectives instead of measures. In our opinion, this eliminates the different levels that were present in the conceptual method as indicated in the workshop session. In addition, since we do not focus anymore on specific measures, it eliminates the need for defining multiple scenarios for measure implementations. In the context of high-level activities we define options. Moreover, a brainstorm session with stakeholders is used to communicate problem areas and decide on multiple strategic objectives related to the cyber security ambition. These results should be evaluated, according to several experts, and adjusted if necessary. In addition, we suggest that the remaining strategic objectives should be prioritized with the stakeholders. Instead of determining measures, we now focus on high-level activities that can be conducted to close the gap. Furthermore, besides defining the milestones, time needed, money needed, resources needed and measures for effectiveness,

we also focus on defining the collaboration needed, responsibilities, and intermediary goals to elaborate on the high-level activities. After the management board chose the ultimate course of action, the effect of the strategy on the organization is discussed instead of as part of the roadmap.

To summarize, Figure 33 shows how we changed the six method steps from the conceptual method to the four method steps of the final method. We also listed all changes in section 13.3.3. Based on the changes proposed above, we created a new process-deliverable diagram and which serves as the final method, i.e. the building blocks for a cyber security strategy.

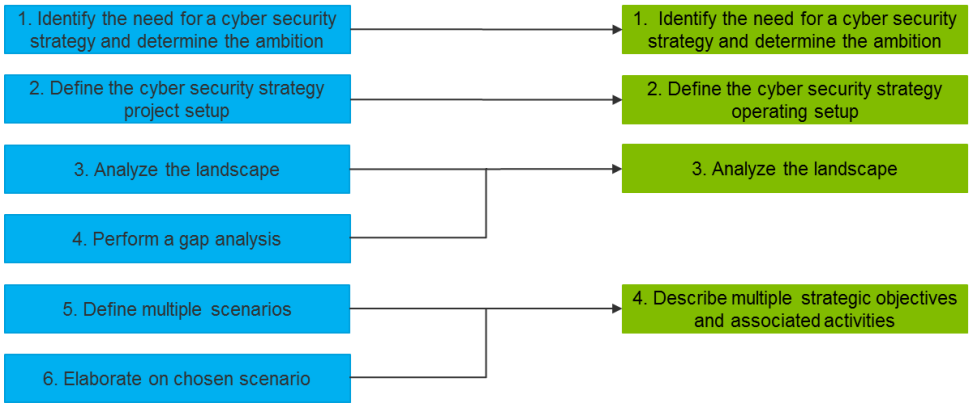


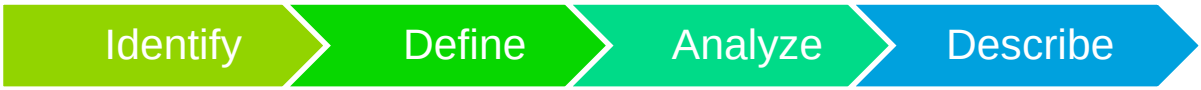
FIGURE 33: MAPPING OF HIGH LEVEL ADAPTATION OF THE CONCEPTUAL METHOD (LIGHT BLUE) TO THE FINAL METHOD (GREEN)

9 The building blocks for a cyber security strategy

In this chapter the final method is discussed to give insight in how corporate organizations can develop a cyber security strategy based on a cyber security ambition that supports the organization's ambition.

9.1 The final method

Based on the validation results described above, we have derived a final method which we elaborate on in this section. Four building blocks underlie the creation of a cyber security strategy.



But before creating such a strategy, one should take note of the following constraints:

- Without buy-in from the management board, one should not create a strategy. Their support is important for the implementation phase of the strategy. Most 'projects' fail without proper support from the management board;
- The cyber security strategy should be part of, aligned with, and support the business strategy. No exceptions;
- The cyber security strategy should be evaluated yearly (or more frequently) and renewed every three years;
- Stakeholders should be involved early in the process of creating a cyber security strategy. Besides the management board, stakeholders are the basis for getting information and afterwards, implementing and propagating the strategy;
- The outcomes of every step and the previous steps should be reviewed after the completion of this step;
- After completion of creating a cyber security strategy, the process of executing the roadmap should be formalized (e.g. in the form of indicating next steps).

The first step is to identify the need for a cyber security strategy and determine the ambition. This means that one should consider the changing environment by looking at, for instance, the emerging external cyber threat landscape, the position of the organization in the market, the value of the information and risks involved, and the developments and decreasing de-perimeterization. In addition, the management board should consider what strategy and controls are already in place and regulatory requirements. Once the need for a cyber security strategy is identified, the scope should be defined. Next, the cyber security ambition can be determined by identifying and connecting the organization's ambition to the cyber security ambition. And finally, guiding principles (i.e. what do we have to hold into account) and the desired outcomes of the cyber security strategy (i.e. what do we expect to achieve).

The second step is to define the cyber security strategy operating setup. This is done by determining and inviting stakeholders for the requirements setting in the following steps. Also, definitions to use within the cyber security strategy regarding cyber security should be set up. For instance by answering the questions: what does cyber security mean to us? When is a threat relevant? What is critical? In addition, governance structures should be defined by using, for example, a RACI matrix. Furthermore strategy dependencies should be defined to see what influence the strategy has on business units, people, and etcetera. And finally, by inviting stakeholders to help in

the process of creating a cyber security strategy, it is important to describe the interaction one desires with these key stakeholders.

Once the need, ambition, and operation setup is determined, it is important to analyze the landscape to base further strategic directions on. First, the social, external and internal landscape is analyzed by, for instance, examining relevant threats, most critical assets, vulnerabilities, and incidents, by performing interviews and quantitative analysis. Other ways of examining these landscapes can be done using one of the models described in chapter 6. Next, a gap analysis is performed by using a framework or performing a risk analysis. When using a framework, the as-is situation is decided upon by assessing the current status with the framework of choice and optionally, benchmarking the results against industry peers. After that, the to-be situation is decided upon. For instance, if the framework or maturity model shows that an organization has a maturity of level 1, then the to-be situation could be that they wish to move to a maturity level of 3. When following a risk analysis approach, the as-is situation is determined by defining the amount at risk for every critical assets. The to-be situation is the risk appetite. The identified risks should then be evaluated and prioritized. When the as-is and the to-be situation are defined, the gaps can be determined and described by comparing the as-is situation with the to-be situation. Finally, based on the assessment of the internal and social landscape and the gap analysis, problem areas are defined and described. These problem areas are fed forward to the final step.

The final step is to describe multiple strategic objectives and associated tasks. A brainstorm session is performed with stakeholders to communicate problem areas and decide on multiple strategic objectives. These strategic objectives should be SMART. The results from the brainstorm session should be evaluated and adjusted if needed. In addition, high-level activities is determined for every strategic objectives. A list of evaluated strategic objectives is used to define a business case for every strategic objective. Next, the strategic objectives need to be elaborated on by defining milestones, time needed, money needed, resources needed, collaboration needed, responsibilities, the measures for effectiveness, and intermediary goals. Next, together with the stakeholders, one should prioritize the strategic objectives. This can be done, for example, by using the MoSCoW method. After the prioritization, the management board should choose the ultimate course of action.

On the next page, a full process-deliverable diagram is presented. The associated activity and concept diagrams are given in section 13.5, as well as an evidence table showing on what sources a step is based on.

9.2 The process-deliverable diagram

The process-deliverable diagram below depicts the final method to construct a well-thought cyber security strategy. The sub process-deliverable diagrams associated to the open activities can be found in the appendix section 13.5.4 as well as a plain text variant of our method.

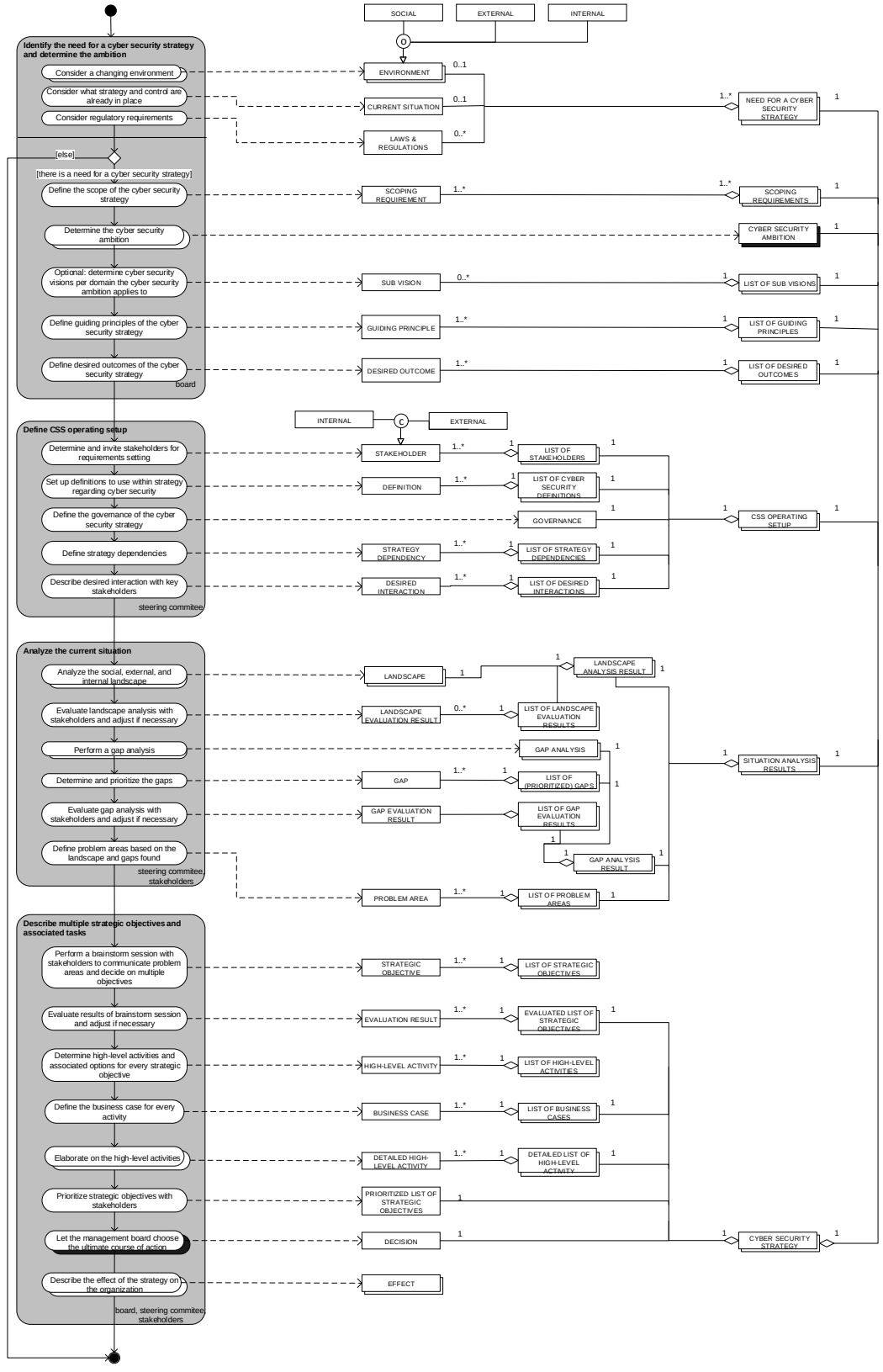


FIGURE 34: THE FINAL BUILDING BLOCKS OF A CYBER SECURITY STRATEGY

9.3 A practical example: The Cookie Factory

In the previous chapters we have already shed a light on the cookie factory to apply the theory in a practical way. We now use the cookie factory to explain our final method to construct a cyber security strategy. For the convenience of the reader, we will repeat the general description of the cookie factory and continue with the application of the final method.

But first, we must note that actually creating a cyber security strategy may take up to months to create. Therefore, in this case, we will only touch upon these subjects high-level. This means that we sometimes group several steps in one outcome and we do not elaborate why certain outcomes were chosen. In a normal setting this should of course be done.

ABC, founded in 1901, is a family business with specialties in baking all sorts of cookies. During all these years, ABC has developed itself into a very modern company with access to the best materials to bake the cookies. The cookie recipe is stored in the machine and therefore, drives and controls the machine. All processes in the factory happen autonomous and the machines can be managed remotely after working hours. In addition, cookies can nowadays be ordered online by direct customers or retailers. This year, the cookie factory had a revenue of 15 million euros in the Netherlands.

The cookie factory has a very modern IT landscape to support both the administrative environment as the factory environment. The Administrative systems are all linked together and hold information about the clients, payments, overall finances and the recipe (both current in use as new recipes is development). The factory machines are controlled by factory systems that are also linked to the internal network and operate fully automated.

9.3.1 Step 1: Identify the need for a cyber security strategy and determine the ambition

The board of ABC has decided that, in the current threat landscape, even their cookie factory should be more secured. They base this on an analysis where they primarily looked at the emerging cyber threat landscape. Simply said, they discovered that everyone could shut down the factory by exploiting vulnerabilities, which has a high impact on the availability of the cookie factory. In addition, the integrity of the recipe can be affected by changing the recipe and the confidentiality can be affected when adversaries steal the recipe. Based on these threats, and the fact that they have a high position and image in the marketplace, a cyber security strategy is needed. There was currently no cyber security strategy in place and there are no regulation that will affect the need for a strategy and the strategy itself. As such, there is a definite need for a cyber security strategy that will encompass the entire IT environment of ABC.

The cyber security ambition of ABC is stated as follows: “ABC wants to have an above industry average secure online and offline environment”. This ambition supports the organization’s ambition: to be the biggest online cookie seller in Europe. To achieve this ambition, the following guiding principles are defined:

- Conform to worldwide cyber security standards;
- Close alignment with the organization’s goals;
- Close engagement with employees to create awareness about cyber security threats;
- Prefer proactive activities above reactive activities.

In addition, the following outcomes are desired:

- Aware employees;
- Little to no security incidents: no successful cyber-attacks.

9.3.2 Step 2: Define the cyber security strategy operating setup

Before executing step two, it is important that a responsible person(s) for group wide security management is identified. If desired, a steering committee is formed. They will be responsible for executing step two to step four. ABC has formed a steering committee.

To determine the requirements for ABC, the steering committee invites the management board, business leaders, and the IT manager to brainstorm about the specific requirements for the operating setup. The steering committee, together with the stakeholders, set up definitions to use within the cyber security strategy regarding cyber security. They decided that, amongst others, cyber security is defined as: “Cyber security deals with protecting all information and non-information based assets which are processed, stored, and transported via the internet”. In addition, they determine that the Chief Financial Officer will be in charge over governing the cyber security strategy once it is created. The Chief Financial Officer is put forward as he can best balance different interests in cyber security and take the business perspective into mind.

The steering committee identifies that the cyber security strategy is dependent on the organization’s strategy. In addition, there is also an IT strategy to use cloud solutions where possible. The cyber security strategy should take these strategies into mind.

And finally, the following interaction is desired from the key stakeholders:

- The steering committee will gather every four weeks;
- The management board is available to join one or more brainstorm sessions and to provide feedback if requested;
- Some key employees are appointed to this initiative and expected to communicate open and honest.

Taking all this information into account, a RACI best explains the different roles of all stakeholders (Figure 35).

	Responsible	Accountable	Consulted	Informed
Management board		X		
Business leaders			X	
IT manager			X	
Chief Financial Officer	X			
Key employees			X	
All ABC employees				X

FIGURE 35: RACI ABC OPERATING SETUP

9.3.3 Step 3: Analyze the landscape

The steering committee, together with the stakeholders, analyzed the social, external, and internal landscape on relevant threats, most critical assets, vulnerabilities, incidents, requirements, running activities, and internal culture. The following outcome is obtained through interviewing the stakeholders as identified in the previous step:

Threats

- The availability of the portal is breached;
- The integrity of orders is breached;
- The confidentiality of customer data, online transactions, and the secret cookie recipe is harmed.

Most critical assets

- Recipe;
- Customer data;
- Financial data;
- Production process.

Vulnerabilities

- Low awareness of employees due to ABC being a family business with high internal trust;

- Low internal knowledge about cyber security;
- The factory machines are linked to the internal network and possibly reachable through the internet.

Incidents

- Customer data has been breached in the past when a laptop was stolen and resulted in hundreds of email addresses and passwords being compromised.

Requirements

- So far there are no internal laws and regulations that ABC as a cookie factory should be taken into account;
- The privacy act should be taken into account when dealing with and processing customer data.

Running activities

- There are no running activities in the area of cyber security as this is a rather new field for ABC to handle;
- ABC is currently developing an online portal to be used to expand their business.

Internal culture

- ABC is a family business where trust is high;
- The employees of ABC are not used to think about threats coming from the outside world;
- The employees of ABC show some resistance against organizational change.

These results are evaluated with the stakeholders and found to be correct.

Next, a gap analysis is performed by using a framework because a risk analysis is too costly and time consuming. In addition, it is already found that ABC does not have a high maturity in their cyber security capabilities. Therefore, a framework analysis will suffice. Because ABC specifically wants a cyber security strategy, the steering committee chose to use the NIST maturity model which is specifically oriented towards cyber security capabilities. The NIST maturity model used five categories with different sub categories which a scored against a four tier scale.

The current and desired situation assessed (Table 12) according to the NIST maturity model shows the following results:

TABLE 12: CURRENT VERSUS DESIRED STATE VIA NIST MODEL

	Identify	Protect	Detect	Respond	Recover
Current	1	2	1	1	1
Desired	3	3	3	2	2

As stated in the guiding principles, ABC prefers proactive measurements before reactive measurements. Hence, the difference in the desired maturity differences in the identify/protect/detect versus respond and recover. The steering committee decided that focus should lie on the biggest gaps, which are in the areas of identify and detect. Next will be protect, followed by respond and recover. The stakeholders agree with the found gaps and prioritization.

The in-depth framework analysis, which is not shown here, reveals several specific problem areas in all five phases. In addition, problem areas were found in the landscape analysis. This main problem were the unaware employees of ABC and the lack of separation between the administrative network and the factory network.

9.3.4 Step 4: Describe multiple strategic objectives and associated activities

The problem areas that were found in the next step are communicated to the stakeholders who were identified in the second step. The stakeholders brainstormed on strategic objectives and ultimately the steering committee decided on the following strategic objectives:

- ABC is resilient to cyber-attacks;
- ABC handles customer data with care for privacy;
- ABC builds secure-by-design applications and a web portal;
- Employees of ABC have sufficient cyber security knowledge.

The stakeholders agree with the chosen strategic objectives. Business cases are defined for each of the strategic objectives, and the overall business case is presented here. To reach the strategic objectives, ABC needs to implement a certain amount of countermeasures valued at a total implementation cost available of €350.000 during the next two years. After the implementation of these measures, ABC expects no loss of data or unavailability of the online portal. Any 24 hour outage of the online portal is estimated at a loss of €45.000. There is an industry-average of 3.5 days outage of the online portal per year, resulting in an annual loss of €157.500. In this calculation the financial loss of reputational damage is not calculated as this is difficult to estimate in a real value. In addition, the countermeasures must mitigate the risk of a breach of confidentiality or integrity of customer data. Assuming an average of one breach every five years where 1000 records are disclosed with a value of €150 per record, the estimated loss is €150.000 in five years. Therefore, resulting in an annual loss of €30.000. The total annual loss is €187.500. This results in an ROI of less than two years.

Next, the following high-level activities per strategic objective are defined:

- ABC is resilient to cyber-attacks;
  - Implement extensive detection and response measures
    - Milestone: 2 years
    - Time needed: 350 days
    - Money needed: €150.000
    - Resources needed: 3FTE
    - Collaboration needed: IT department and one external consultant
    - Responsibilities: IT is leading
    - Measures for effectiveness: no undetected breaches, response within 1 hour
  - Implement a back-up online portal to be used in case of unavailability
    - Milestone: 3 months
    - Time needed: 50 days
    - Money needed: €10.000
    - Resources needed: 0.5FTE
    - Collaboration needed: IT department
    - Responsibilities: IT is leading
    - Measures for effectiveness: back-up available and tested twice a year
  - Disentanglement of the factory network from the administrative network
    - Milestone: 6 months
    - Time needed: 100 days
    - Money needed: €20.000
    - Resources needed: 1FTE
    - Collaboration needed: IT department and factory manager
    - Responsibilities: IT is leading
    - Measures for effectiveness: the administrative network is not accessible through the factory network and vice versa

    - Optionally: implement high standard and expensive encryption software to protect the cookie recipe
        - Milestone: 1 year
        - Time needed: 50 days
        - Money needed: €50.000
        - Resources needed: 0.5FTE
        - Collaboration needed: IT department and external software company
        - Responsibilities: IT is leading
        - Measures for effectiveness: all data is encrypted, encryption algorithm key length must protect the information to at least the year 2020
    - Optionally: implement a honey pot system
        - Milestone: 3 months
        - Time needed: 20 days
        - Money needed: €20.000
        - Resources needed: 0.5FTE
        - Collaboration needed: external vendor
        - Responsibilities: IT is leading
        - Measures for effectiveness: two detected cyber-attack attempts per year
- ABC handles customer data with care for privacy;
    - Implement countermeasures as defined by the Dutch privacy act
        - Milestone: 1 year
        - Time needed: 100 days
        - Money needed: €25.000
        - Resources needed: 1FTE
        - Collaboration needed: IT department and one external consultant
        - Responsibilities: IT is leading
        - Measures for effectiveness: successful compliance check per year
- ABC builds secure-by-design applications and a web portal;
    - Educate software developers in designing secure code
        - Milestone: 2 years
        - Time needed: 350 days
        - Money needed: €50.000
        - Resources needed: 4FTE
        - Collaboration needed: IT department and external educational firm
        - Responsibilities: IT is leading
        - Measures for effectiveness: secure code, less than five vulnerabilities detected by penetration tests
    - Obtain a contract to have a periodically penetration test to be performed
        - Milestone: 1 month
        - Time needed: 20 days
        - Money needed: €30.000
        - Resources needed: 1FTE
        - Collaboration needed: external penetration firm
        - Responsibilities: IT is leading
        - Measures for effectiveness: penetration test performed 4 times per year

    - Optionally: have an external party develop and maintain secure-by design applications and a web portal
        - Milestone: 2 years
        - Time needed: 350 days
        - Money needed: €150.000
        - Resources needed: 3FTE
        - Collaboration needed: external firm
        - Responsibilities: IT is leading
        - Measures for effectiveness: secure applications and web portal, less than five vulnerabilities detected by penetration tests
    - Optionally: have all internal software developers certified for creating secure code
        - Milestone: 3 months
        - Time needed: 50 days
        - Money needed: €40.000
        - Resources needed: 4FTE
        - Collaboration needed: external educational firm
        - Responsibilities: IT is leading
        - Measures for effectiveness: all internal software developers certified
- Employees of ABC have sufficient cyber security knowledge.
    - Educate all employees with the basics of information and cyber security awareness
        - Milestone: 6 months
        - Time needed: 50 days
        - Money needed: €35.000
        - Resources needed: 1.5FTE
        - Collaboration needed: HR and external educational firm
        - Responsibilities: HR is leading
        - Measures for effectiveness: all employees received awareness training

Based on the information given above, the following prioritization is defined by the stakeholders:

1. Employees of ABC have sufficient cyber security knowledge;
2. ABC is resilient to cyber-attacks;
3. ABC builds secure-by-design applications and a web portal;
4. ABC handles customer data with care for privacy;

The management board agrees with the chosen strategic objectives and high-level activities without choosing the options. This will result in: ABC has to hire one additional FTE specialized in the field of cyber security. The entire population of employees have better understanding and awareness of the risks involved with the online portal and the value of the intellectual property, like the cookie recipe. Additionally processes are implemented to ensure secure-by-design coding and regularly performing penetration tests. ABC has to implement quite some technological solutions to adhere to have above average cyber security countermeasures. And finally, every employee has a set of extra responsibilities in their job description regarding the awareness and prevention of cyber security attacks.

10 Discussion

The main research question that served as a guidance for this research was: *How can corporate organizations develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition?*

Literature regarding strategy creation models, interviews with experts, and the analysis of national cyber security strategy documents enabled us to get a grip on how strategy is created, and specifically in the cyber security domain. This research answered the main research question. However, despite that a cyber security strategy method was deduced from the information that was gathered, the method steps are still quite generic and high-level. This was due to the fact that we experienced that interviewees find it hard to explicate the process in detail and the scientific literature being was not going into depth.

Currently, data is one of the most valuable assets of an organization and should therefore be protected from threats coming from cyberspace. Experts indicated that, especially, when data is processed within the organization a cyber security strategy is needed, and therefore corroborates the previous statement. In addition, it was said that a cyber security strategy can be useful to decrease or eliminate threats, vulnerabilities and consequences to minimize the probability and impact of a cyber-attack. Our research showed why it is important to focus on assessing the internal, external, social, and cyber threat environment when creating a cyber security strategy to reduce the aforementioned threats, vulnerabilities, and consequences. Our research either confirms or extends the findings presented in the introduction.

In addition, our research focused on describing a way that helps corporate organizations develop a cyber security strategy. A structured method was deduced. Though, experts consulted during the validation phase mentioned that they would use this method, probably, as a tool to guide them through the process of creating a cyber security strategy instead of following it precisely. The question raised in literature (e.g. Mintzberg) and by experts is whether a method, as we have presented, is too structured for something as organic as strategy creation. And this remains an unresolved question.

Furthermore, we experienced that the research approach that we used was effective to gain the desired results, since we did get to extract a method from it. However, it would have been more helpful if experts had a more clear idea of the exact method they used, if there was more literature available showing concrete steps to be taken to create a (cyber security) strategy, and if there was more information available about the national cyber security strategies. First, we experienced during the interviews that experts had trouble explicating a process they followed. Perhaps a focus group where experts think together of a method would have gotten extra results that would give us more grip on how a cyber security strategy is created, for instance on the order of certain activities. Second, we noticed during the analysis of literature that most strategic models were quite generic and high level, resulting in a conclusion with high-level strategy elements. Although the literature results were helpful and we now know how strategy is created in different field, more fields could have been explored to help get more interesting results. And finally, we think that the analysis of national cyber security strategies was the most effective research method, because it gave a more complete, and bigger picture of how a cyber security strategy is created which provided the basis for constructing our conceptual method. However, it would have been better if we would have known the exact process countries followed to create their cyber security strategy and maybe also whether this strategy was successful. The method we now deduced from the national cyber security strategies is now subject to a researcher bias. Given these limitations of the research method, we could have missed important elements which could results in presenting a less than complete method.

Nevertheless, the method presented in this research shows scientifically and practically grounded building blocks to create a cyber security strategy. The six building blocks, and associated sub steps, focus on identifying the need

for a cyber security strategy and determining a cyber security ambition, defining the cyber security strategy operating setup, analyzing the current situation, and describing strategic objectives together with associated activities. The found method extends the body of knowledge about strategy creation and specifically in the field of cyber security. By following this method to create a well-thought cyber security strategy, it also helps organizations to be more resilient to an emerging threat landscape. Furthermore, the validation showed that it is considered a useful tool to use in practice.

Despite the fact that a method to create a well-thought cyber security strategy was presented, it remained quite high-level and several steps could use more discussion. Future research could go more into depth for every step. For instance by answering the question: how do you identify threats? Or when do you use the framework approach and when the risk analysis approach? Furthermore, the method should be tested in practice by creating a real cyber security strategy for a corporate organization by following the method steps. More about this can be found in section 11.1.

10.1 Reflection on threats to validity

Every research is susceptible to threats that may decrease the validity of the research. Therefore we reflect on the threats to construct validity, internal validity, external validity, and reliability (Wohlin et al., 2012). First of all, construct validity deals with whether research subjects were on the same page on different definitions that guide the research. This threat has been mitigated during the interviews by asking every expert whether they agreed with the presented definition about an ambition and a strategy. During the workshop session this was unfortunately not done. This is a disadvantage of our research. In addition, internal validity refers to the threat that a causal relationship between two variables may be influenced by another variable. During our research, we assumed and investigated that there is a causal relationship between a cyber security strategy and the organization's strategy. Literature showed this relationship was indeed present and that there is no reason to assume that other variables may interrupt or influence this causal relationship. The interview results also show that the security department is usually placed directly under the management board as a staff function and therefore there is not much direct influence from, for instance, the IT department. Next, external validity is concerned with whether the research results are relevant for other domains and to what extent these are generalizable. Although we only interviewed experts from the information and cyber security domain, we did investigate strategy creation from other perspectives besides information and cyber security. This shows us that our strategy creation method can be applied in domains were they are dealing with fast changes, internal and external threats, and preferably to defend against moves from competitors. And finally, reliability. The research approach is explicated in chapter 3 and other researchers therefore should be able to replicate the research and find the same results.

11 Conclusion

This chapter gives an overview of the answers to the sub questions and the main research question.

SQ1: What drives a cyber security strategy for corporate organizations?

Literature and expert interviews showed that the following drivers are most common to initiate a cyber security strategy:

- Corporate governance: corporate codes often imply the need for a strategy for effective risk management;
- Legal: some industry-related laws have requirements for a cyber security strategy;
- Regulatory: regulations may have requirements for an information security strategy;
- Audit: audit reports may require a strategy as part of overall good governance;
- Management: executive management may require a cyber security strategy as part of an overall strategic cascade;
- Peer and media pressure: peer organizations and oversight bodies may create pressure to adopt a strategy. In addition, media attention to security breaches may drive a strategy;
- Incidents: cyber security incidents may call for immediate action and the creation or the update of a (new) strategy;
- Risks or the risk appetite: the degree to which an organization is at risk or the amount of risk that an organization is willing to accept may require a strategy;
- Threats to the critical assets of the organization: threat to the critical assets of the organization may call for a strategy;
- The inadequacy of the former cyber security strategy: the inadequacy of the former cyber security strategy can require a new strategy to adequately address threats.

The drivers mentioned above provide a basis to what 'things' could be considered when identifying the need for a strategy. However, in practice there may be other drivers to initiate the creation of a cyber security strategy.

SQ2: How and to what extent are an organization's ambition and a cyber security ambition related?

Although there are different opinions in whether there should exist a separate cyber security ambition, it is clear to us however, that this cyber security ambition cannot be seen separately of the organization's ambition. Based on what we found in the literature and the interviews, we can conclude that the cyber security ambition should always directly support the organization's ambition or the cyber security ambition is derived from the organization's ambition. Furthermore, the cyber security ambition is translated to a cyber security strategy. This strategy should take in mind the organization's strategy, as concluded from the literature. In the organization's strategy specific strategic objectives and projects are listed. When an organization wants to include cyber security in these projects, then a link is made between the organization strategy and the cyber security strategy. This means that in creating a cyber security strategy, one should identify and incorporate the organization's ambition in the cyber security ambition.

SQ3: Which elements are included in a strategy?

Analyzing the literature showed us that most information about strategy creation was available in the business, game theory, and military domain. The models and theories related to these domains showed that there are three main focal points of strategy creation, namely: focusing on the external environment, the internal environment, the social environment, or a combination of these three.

The social environment deals with, amongst other, humans, social relationships and culture within an organization. The external environment deals with elements that exist outside the boundaries of the organization and the internal environment deals with all elements that exist within the organization.

The analysis of common elements present in strategy creation processes and models show the focus on the environment as an important factor to consider. In our opinion, the results of analyzing the internal, external, and social environment can stress the need for a cyber security strategy, and determines the drivers. In addition, we use these three groups when we analyze the current situation during strategy creation because all models are used for this purpose. This implies that an environment analysis is an important part in establishing a cyber security strategy, and therefore should be incorporated in the process of creating a cyber security strategy.

SQ4: Which cyber security elements are of importance for a cyber security strategy (to be successful)?

Interviews with cyber security experts and the analysis of national cyber security strategy documents showed that one should specifically assess the cyber threat landscape when creating a cyber security strategy. For instance, by identifying threats, risks, incidents, and cyber trends. The following elements are of importance for a cyber security strategy, which we typify as the cyber security threat landscape:

- Link between the business ambition and cyber security ambition.
- Threats;
- Risks;
- Challenges;
- Opportunities;
- Trends & developments;
- Incidents;

During the literature review, we also tried to assess whether the business, game theory, and military elements are applicable in the cyber security domain. This assessment showed that all elements were applicable to the cyber security domain and therefore the elements identified in the previous sub question are also important cyber security elements to include in the process of creating a cyber security strategy. What we noticed is that the cyber landscape, in addition to focusing on the cyber threat landscape, encompasses the social, external, and internal environment. This means that we ought to assess an organization's social, external, and internal environment both in terms of their current cyber security defense capabilities and the influence of the cyber threat landscape on the social, external, and internal environment. To summarize, the entire assessment needs to focus on the following aspects to discover strengths and weaknesses (threats):

- The social environment:
    - Cyber security defense capabilities: e.g. awareness amongst personnel, a sensible level of trust, feeling responsible for the security of personal data, careful use of BYOD.
    - Cyber security threat landscape: e.g. more and more targeted towards employees, personal data and personal smart devices rather than attacks on the enterprise networks.
- The external environment:
    - Cyber security defense capabilities: e.g. information about possible adversaries, no lock-in to a single external company, regular knowledge gathering regarding cyber security from external experts, regular external audits performed at outsourcing partners.
    - Cyber security threat landscape: e.g. increase in zero-day exploits, more complicated attacks, better equipped and organized cyber security attackers.
- The internal environment:
    - Cyber security defense capabilities: e.g. good detection mechanisms, good response mechanisms, qualified security intelligence personnel, up-to-date with latest patches, regular vulnerability scans, regular penetration tests performed.

- Cyber security threat landscape: e.g. internal IT complexity disguises potential weak spots, internet connectivity everywhere (wired and wireless).

This assessment can be used to establish the current situation of cyber security defense capabilities and the cyber security threat landscape and give input for the need for a cyber security strategy.

RQ: How can a corporate organization develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition?

Based on the research done to answer the sub questions and the actual answers to the sub question, we can answer the main research question. A corporate organization can develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition by following these high-level steps:

1. Identify the need for a cyber security strategy and determine the cyber security ambition;
2. Define the cyber security strategy operating setup;
3. Analyze the current situation;
4. Describe the strategic objectives and associated activities.

Chapter 9 elaborates on these four building blocks. However, in order to successfully create and implement a cyber security strategy, several conditions apply. Buy-in from senior management is of utmost importance. Without their support, the strategy is likely to fail. In addition, the cyber security strategy should be part of, aligned with, and support the business strategy, as mentioned in section 5.5. Furthermore, the cyber security strategy should be evaluated yearly and renewed every three years. During the creation of the cyber security strategy, stakeholder should be identified and involved early in the process. And finally, the outcomes of every step and previous steps need to be reviewed after completion of this step. Every step is an important building block for the next step and without proper consideration and evaluation, the chance is higher that decision are made on incorrect information.

11.1 Future work

Based on what we found in this research, we identified several directions for future work. First of all, one could validate the method in practice by walking through all steps. This way, we could really validate the order and applicability of the steps in the field. In addition, one could research strategy creation from more perspectives, for instance from a marketing perspective. Furthermore, it would be interesting to look at more popular methods in the field, rather than scientific methods. For instance, the cyber security framework of NIST also shows steps to follow to improve cyber security programs at organization. One can also perform more research about every single step, to research what possible ambitions, project setups, strategic objectives, and strategies are in the field of cyber security. In addition, it is interesting to research which tools can be used to perform the found method steps. Moreover, one could research different methods to model traceability between the outcomes of different method steps (e.g. i*, tree diagrams). And finally, research into the successfulness of the method and the cyber security strategy would be very important and interesting. We would like to get answers to questions like when is a (cyber security) strategy considered successful? How do the steps used to come to a cyber security strategy relate to the successfulness of the strategy? How can you measure when a step in the method has been successfully executed? Our research raised all these questions and we are curious to the answers.

12 References

Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2008). Making Sense of Technology Trends in the Information Technology Landscape: A Design Science Approach. *MIS Quarterly*, *32*(4), 779–809.

Austria. (2013). Austrian Cyber Security Strategy.

Baetz, M. C., & Bart, C. K. (1996). Developing Mission Statements Which Work. *Long Range Planning*, *29*(4), 526–533. doi:10.1016/0024-6301(96)00044-1

Barnett, E., & Casper, M. (2001). A definition of "social environment". *American Journal of Public Health*, *91*(3), 465. doi:10.2105/AJPH.91.3.465a

Bevir, M. (2012). *Governance: a short introduction*. Oxford University Press.

Boyd, J. (1987a). Organic Design for Command and Control.

Boyd, J. (1987b). The Strategic Game of ? and ?

Brandenburger, A. M., & Nalebuff, B. j. (1995). The Right Game: Use Game Theory to Shape Strategy. *Long Range Planning*, *28*(5), 128. doi:10.1016/0024-6301(95)90326-7

Byres, E., & Lowe, J. (2004). The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. In *Proceedings of the VDE Kongress* (pp. 1–6).

CEB. (2013). Is Your Company Taking Risk Reduction Too Far? Retrieved from http://news.executiveboard.com/2013-04-15-Is-Your-Company-Taking-Risk-Reduction-Too-Far

Chabinsky, S. R. (2010). Cybersecurity Strategy : A Primer for Policy Makers and Those on the Front Line. *Journal of National Security Law & Policy*, *4*(27), 27–39.

Choo, K.-K. R. (2011a). The cyber threat landscape: Challenges and future research directions. *Computers & Security*, *30*(8), 719–731. doi:10.1016/j.cose.2011.08.004

Choo, K.-K. R. (2011b). Trends & issues financial and insurance industry. *Trends and Issues in Crime and Criminal Justice*, *408*(1), 1–6.

Cisco. (2011). *The Internet of Things How the Next Evolution of the Internet The Internet of Things How the Next Evolution of the Internet Is Changing Everything*.

Cohen, F. (2001). The New Cyber Gang — A Real Threat Profile. *Network Security*, *2001*(5), 15–17. doi:10.1016/S1353-4858(01)00517-7

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

Contreras, J. L., Denardis, L., & Teplinsky, M. (2013). Mapping Today ' s Cybersecurity Landscape Mapping Today ' s Cybersecurity Landscape, *62*(5), 1113–1130.

Czech Republic. (2015). Cyber Security Strategy of the Czech Republic.

David, F. R. (1989). How companies define their mission. *Long Range Planning*, *22*(1), 90–97. doi:10.1016/0024-6301(89)90055-1

Deloitte. (2011). *Raising the Bar 2011 TMT Global Security Study – Key Findings*.

Deloitte. (2013). *Blurring the lines 2013 TMT Global Security Study*.

Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. *Journal of Information Technology Management*, *XVII*(2), 13–22.

Eden, C., & Ackermann, F. (1998). *Making Strategy: The Journey of Strategic Management*. Londen: Sage Publications.

El Aoufi, S. (2009). *Economic Evaluation of Information Security*. Amsterdam: VU University Amsterdam.

ENISA. (2014). *Threat Landscape and Good Practices for the Internet Infrastructure*.

Estonia. (2014). Cyber Security Strategy Estionia.

Finland. (2013). Finland´s Cyber security Strategy.

Flick, U. (2009). *An Introduction to Qualitative Research*.

Gemalto. (2015). *Breach Level Index Annual Report 2014*.

George, A. L., & Bennett, A. (2004). *Case Studies and Theory Development in the Social Sciences*.

Gorschek, T., Wohlin, C., Garre, P., & Larsson, S. (2006). A Model for Technology Transfer in Practice. *IEEE*, *23*(6), 88–95.

Gragido, W. (2011). Beyond zero: analysing threat trends. *Network Security*, *2011*(7), 7–9. doi:10.1016/S1353-4858(11)70074-5

Grant, R. M. (1991). The resource-based theory of competitive advantage Implications for strategy formulation. *Strategic Management Journal*, *17*(S2), 109–122.

Grant Thornton. (2011). *Cybercrime*. doi:10.1007/SpringerReference_11517

Greitzer, F. L., Moore, A. P., Cappeli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the Insider Cyber Threat. *Security & Privacy, IEEE*, *6*(1), 61–64.

Hedley, B. (1977). Strategy and the “business portfolio.” *Long Range Planning*, *10*(1), 9–15. doi:10.1016/0024-6301(77)90042-5

Henderson, J. C., & Venkatraman, N. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *32*(1), 472–484.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Hill, T., & Westbrook, R. (1997). SWOT analysis: It’s time for a product recall. *Long Range Planning*, *30*(1), 46–52. doi:10.1016/S0024-6301(96)00095-7

Huijboom, N., & Broek, T. Van Den. (2011). Open data: an international comparison of strategies. *European Journal of ePractice*, (April), 1–13.

Hungary. (2013). National Cyber Security Strategy.

Ireland, R. D., & Hirc, M. a. (1992). Mission statements: Importance, challenge, and recommendations for development. *Business Horizons*, *35*(June), 34–42. doi:10.1016/0007-6813(92)90067-J

ISACA. (2014). Glossary. Retrieved from http://www.isaca.org/Pages/Glossary.aspx?tid=2077&char=C

ISF. (2007). *Strategy Project team Review and quality assurance*.

ISO. (2013). *ISO 27001:2013*.

IT Governance Institute. (2007). *CobiT 4.1*.

Johnson, G., Scholes, K., & Whittington, R. (2008). *Exploring Corporate Strategy.* doi:10.1016/0142-694X(85)90029-8

Kellerman, T. (2010). Cyber-Threat Proliferation. *Security & Privacy, IEEE*, *8*(3), 70–73.

Kenya. (2014). National Cybersecurity Strategy.

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering*.

KPMG. (2014). *Cyber Security : from threat to opportunity*.

Leemhuis, J. P. (1985). Using scenarios to develop strategies. *Long Range Planning*, *18*(2), 30–37. doi:10.1016/0024-6301(85)90020-2

Lieberman, H. R., Bathalon, G. P., Falco, C. M., Morgan, C. a., Niro, P. J., & Tharion, W. J. (2005). The fog of war: Decrements in cognitive performance and mood associated with combat-like stress. *Aviation Space and Environmental Medicine*, *76*(7 II), 7–14.

Lipson, H. F. (2002). Tracking and Tracing Cyber-Attacks Technical Challenges and Global Policy Issues.pdf.

Lithuania. (2012). The programme for the Development of Electronic Information Security (Cyber-Security) for 2011-201.

McFadzean, E., Ezingeard, J., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. *Online Information Review*, *31*(5), 622–660. doi:10.1108/14684520710832333

Mehari. (2010). Mehari: Information risk analysis and management methodology. Retrieved from https://www.clusif.asso.fr/en/production/mehari/

Mintzberg, H. (1978). Patterns in Strategy Formation, *24*(9), 934–948.

Mintzberg, H., Ahlstrand, B., & Lampel, J. (1998). *Strategy safari: a guided tour through the wilds of strategic management*. *Free Press*. New York, NY, USA: The Free Press. Retrieved from http://www.amazon.co.uk/dp/0273656368

Montenegro. (2013). National Cyber Security Strategy for Montenegro.

Mueller, M., & Kuehn, A. (2013). Einstein on the Breach : Surveillance Technology , Cybersecurity and Organizational Change 1 Introduction. In *12th Workshop on the Economics of Information Security (WEIS 2013)* (pp. 1–26). Georgetown University, Washington.

National Audit Office. (2013). *The UK cyber security strategy : Landscape review*.

the Netherlands. (2013). Nationale Cybersecurity Strategie 2.

New Zealand. (2011). New Zealand's Cyber Security Strategy.

NIST. (2012). *Guide for Conducting Risk Assessments*. USA.

NIST. (2014). *Framework for Improving Critical Infrastructure Cybersecurity*.

Orman, H. (2003). The Morris Worm: A Fifteen-Year Perspective. *IEEE Security & Privacy*, *1*(5), 35–43.

OWASP. (2014). OWASP Risk Rating Methodology. Retrieved from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Owens, M. T. (2007). Strategy and The Strategic Way of Thinking. *Naval War College Review*, *60*(4), 15.

Peng, G. C. A., & Nunes, M. B. (2007). Using PEST Analysis as a Tool for Refining and Focusing Contexts for Information Systems Research. In *6th European Conference on Research Methodology for Business and Management Studies* (pp. 229–236). Lisbon, Portugal.

Perky, L. T. (1991). Strategic improvising: How to formulate and implement competitive strategies in concert. *Organizational Dynamics*, *19*(4), 51–64. doi:10.1016/0090-2616(91)90053-C

Poland. (2013). Cyperspace Protection Policy of the Republic of Poland.

Ponemon. (2013). *2013 Cost of Data Breach Study : Global Analysis*.

Ponemon. (2015). *Cost of data breach study: Global Analysis 2015*.

Porter, M. E. (1979). How competitive forces shape stategy. *Harvard Business Review*, 137–141.

Potts, M. (2012). The state of information security. *Network Security*, *2012*(7), 9–11. doi:10.1016/S1353-4858(12)70064-8

PwC. (2014). *US cybercrime : Rising Key findings from the 2014 US State of Cybercrime Survey*.

Sarkar, R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report*, *15*(3), 112–133. doi:10.1016/j.istr.2010.11.002

Shimeall, T. J., & Spring, J. M. (2014). *Introduction to Information Security: A Strategy-based Approach*. Waltham, USA: Elsevier B.V.

Silvius, A. J. G. (2007). Exploring Differences in the Perception of Business & IT Alignment. *Communications of the IIMA*, *7*(2), 21–32.

Singapore. (2013). National Cyber Security Masterplan.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford, UK: Oxford University Press.

Skrt, B., & Antoncic, B. (2004). Strategic planning and small firm growth: An empirical examination. *Managing Global Transitions*, *2*(2), 107–122. doi:10.1007/s10464-011-9453-y

Slovakia. (2008). National Strategy for Information Security in the Slovak Republic.

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications*, *5*, 147–158.

Uganda. (2011). National Information Security Strategy Uganda.

Van de Weerd, I., & Brinkkemper, S. (2008). Meta-Modeling for Situational Analysis and Design Methods. *Handbook of Research on Modern Systems Analysis and Design Technologies and Applications*, 35–54. doi:10.4018/978-1-59904-887-1

Verizon. (2014). *2014 Data Breach Investigations Report*.

Victoria, S., & Florin, B. (2012). Emerging IT Technologies - Advantages and Risks, *2012*(5), 181–188.

Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. doi:10.1016/j.cose.2013.04.004

Wall, D. S. (2010). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*(2), 107–124. doi:10.1057/sj.2012.1

Ward, J., & Peppard, J. (2008). *Strategic Planning for Information Systems*. Chichester, West Sussex, England: John Wiley Sons, Ltd.

Waterman, R. H., Peters, T. J., & Phillips, J. R. (1980). Structure is not organization. *Business Horizons*, *23*(3), 14–26.

Whittington, R. (2001). *What is strategy and does it matter?* Cengage Learning EMEA.

Wilson, I. (1992). Realizing the power of strategic vision. *Long Range Planning*, *25*(5), 18–28. doi:10.1016/0024-6301(92)90271-3

Withers, P. (2011). Information Security Threat Vectors.

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in Software Engineering*. Heidelberg: Springer.

Woollacott, P. (2007). Cybercrime comes of age. *Itnow*, *49*(2), 6–7. doi:10.1093/combul/bwl110

Zimski, P. (2011). Navigating the new threat landscape. *Computer Fraud & Security*, *2011*(5), 5–8. doi:10.1016/S1361-3723(11)70049-5

13 Appendix

13.1 Analysis of expert views on the topic of cyber security strategy

In the sub sections below we will present a summary of the answers given to the questions posed in the interviews. First the answers given to the questions about a cyber security ambition are discussed. Next, the answers give to the questions about a cyber security strategy are discussed.

13.1.1 Ambition

13.1.1.1 Why was a certain ambition chosen?

There are many possible drivers for creating a cyber security strategy. It may be driven by a person, department, organization or by the government or it may be driven by incidents, reputation, the business or risks. A consultant explained how a cyber security strategy is driven by an organization's risk appetite:

> *"It is driven by the willingness of an organization to take risks. What if the webportal of a cookie factory is not available and this is really bad for the organization, then the security strategy is driven by the fact that you would want to invest a lot of money to improve the availability of the webportal. But if it not bad at all, then it won't be a problem in my opinion. The question is: how important is something at the moment it is not available anymore? That is actually a risk analysis. What risk is acceptable? Is it acceptable to be offline for 2 days? Or for a month? On the basis of that, your risk appetite, you will determine what your strategy should be" – Expert 4*

Another example is that many cyber security strategies are driven by external regulators. The 'De Nederlandse Bank' requires that Dutch financial institutions comply with certain laws.

> *"In practice, it [the cyber security strategy] is often initiated because regulators want it. This is what I see in most organizations. Whether it is a regulator or a government, that is how it usually starts. When people are working on this strategy and are thinking about it, only then a naturally intrinsic motivation will occur." – Expert 6*

During the interviews, sixteen unique drivers were presented. These are the following:

- The IT department (1)
- The inadequacy of the former cyber security strategy (1)
- The organization itself (2)
- The government (2)
- The willingness to be compliant (2)
- Media attention (2)
- To promote arrangements with regard to cyber security (2)
- Threats to the critical assets of the organization (2)
- To retain a good reputation (3)
- For the usefulness and necessity of a cyber security strategy (4)
- The security department (4)
- The management board (5)
- The business operations or the business goals (5)

- Risks or the risk appetite (5)
- Incidents (8)
- The law or external regulators (8)

The lists shows that most cyber security strategies are driven by the law or external regulators, incidents, and risks.

13.1.1.2 How did you substantiate the cyber security ambitions? Which methods or means are used to formulate the cyber security ambition?

The interviewees were then asked how they would substantiate a cyber security ambition and what methods were used to formulate this ambition. Input for the cyber security ambition are, amongst others, developments (1), a government baseline (1), and the business ambition (7). One of the interviewees explained how the business ambition is input for the cyber security ambition, using the same example as with the previous question.

> *"You should first determine what exactly the ambition of the organization itself is, what the goal is. Once you know that, you must think about what is really important in that process. Suppose we talk about that cookie bakery. Where lies the key value? The formula of the cookies is very important, raw materials must be good, or everyone should always be able to order cookies online. If one of these is the business goal, then you have to make sure it becomes a key element [to the organization]. That way, you try to define a number of assets which you have to protect." – Expert 4*

In addition, according to the interviewees a cyber security ambition statement should give answer to the question 'why' (2), and contain an ambition level that an organization wants to achieve (5).

> *"An ambition statement should contain an ambition level that you wish to achieve, why you want to achieve that level, and which conditions apply. How you will do this will be your strategy." – Expert 10*

Besides that the cyber security ambition is mostly based on the business ambition and it should answer the 'why' question and contain an ambition level, it should be presented in a storytelling way with which employees can relate. However, the ambition statement should still be specific, measurable, acceptable, realistic, and time-oriented (SMART).

13.1.1.3 To what extent was this cyber security ambition connected to the (broader) ambition of the organization? How do you process an organization ambition in a cyber security ambition?

The answers to the previous question already showed that half (7) of the employees mentioned that the business ambition is direct input for the cyber security ambition. When asking the question directly to the interviewees, ten out of twelve stated that the cyber security ambition cannot be seen inseparably of the organization ambition.

> *"The ambition should, at least, contain a translation of the company's goals" – Expert 2*

> *"That is a good question. One of the subjects is always 'business alignment', so how do you align your security strategy with your business strategy. What we do try, of course, is to define the common ground to, at least, translate this to 'why is security important in the context of the business strategy or philosophy?' " – Expert 11*

One interviewee stated that at his organization the cyber security ambition was not driven by and linked to the organization ambition. Two interviewees stated that they did not have a separate cyber security ambition. They always try to support the organization ambition with their security department.

> *"I do not think that you need that kind of a vision for information security. That is your business vision. My idea is that your security strategy is actually meant to secure your company's vision and business strategy. You try to accomplish your business strategy, however, there are many threats, amongst others, from the cyber security field. These are a threat to your business goals." – Expert 6*

In addition, two interviewees state that it is not surprising if companies do not have a separate cyber security ambition or strategy. It is often the case that these are mentioned in a subsection of a high-level strategy document of the organization.

Although there are different opinions in whether there should exist a separate cyber security ambition, it is clear however, that this cyber security ambition cannot be seen inextricably of the organization's ambition.

13.1.1.4 What is the independent role of security within an organization? What is the playing field of IT, security and business?

Another important question posed during the interview was 'what is the independent role of security within an organization?' This is important to know because the position of security within an organization can affect the choices being made regarding the cyber security ambition, strategy, and the exact measures taken.

Eleven out of twelve interviewees stated that security should be seen separate from IT, because:

> *.. it should be initiated by the business processes. – Expert 1*
>
> *.. IT only deals with ICT projects, while most problems should be dealt with on the process side. – Expert 3*
>
> *.. security also deals with matters that fall outside the scope of IT. – Expert 4*
>
> *.. IT is an enabler, they must implement measures. – Expert 5*
>
> *.. the actual management of cyber security risks is not something that belongs to the IT department. They can only facilitate and arrange measure to make it easier. – Expert 7*
>
> *.. security should be an integral part – Expert 9*
>
> *.. you have people, process, and technology. Technology is of course a substantial part. But when I, as an ignorant user, put a USB stick in my computer or I click on the wrong email or link, then on the back side it is still technique, but it is the human that makes the mistake. – Expert 12*

Several interviewees (6) stated that the security department should be or is positioned at the risk department, while others (2) state that security should be a staff function because it is an integral part of all departments within the organization. Besides the hierarchical positioning of security, the interviewees (6) proclaim that security should be controlled by a member of the executive board, e.g. a Chief Risk Officer.

In addition, security should be an advisor (5) so that value can be created. One interviewee said the following about the constructive, advising role of the security department:

"By saying 'if that is what you want, what can I [from the security department] do to make sure it is possible in a safe way' instead of saying 'no, you are not allowed to do that because it is unsafe!' That is really just hitting the brakes without looking at the purpose. Because that unsafe thing, is that even relevant for this organization and in this phase? Maybe not. Maybe it is indeed unsafe, but if you [from the security department] do something extra or something in a slightly different way, it could be possible to allow it within the constraints. Then you say 'well okay, if you do it this way and limit it in that way, then you can do it'. That is a very different message than just saying 'No don't do it, because it is unsafe!" – Expert 2

In addition, two interviewees also state that the other role of security is to be the supervising party. For example, to independently monitor whether everybody carries out their processes and whether they perform well.

It seems that there are different views on the role and position of security, but it is evident that it should always be seen and positioned separate from the IT department.

13.1.1.5 Strategy

13.1.1.5.1 What elements were of importance to develop the (cyber) security strategy? What process was followed?

After questions about cyber security ambition, it was then important to make the connection to the 'how' side of the ambition by asking questions about the cyber security strategy. First it was asked how the interviewee developed a (cyber) security strategy and what process they followed.

Examples of processes mentioned by the interviewees are:

- 1. Perform a risk and threat analysis; 2. Have a dialogue with the stakeholders; 3. Discuss the current situation; 4. Link results of step 1, 2 and 3 with the ambition by formulating strategic objectives; 5. Evaluate strategy before implementation; 6. Implement the strategy (Expert 7)
- 1. Asses current situation versus the ambition and decide on gap; 2. Create a roadmap; 3. Define scope; 4. Implement the strategy (Expert 11)
- 1. Assess developments; 2. Assess threats; 3. Assess critical assets; 4. Define risks; 5. Decide on what you want to achieve; 6. Create a roadmap; 7. Implement the strategy (Expert 12)

However, it was noticeable during the interviews that interviewees had trouble explicating the process they followed to create a (cyber) security strategy. Below is a list of important elements mentioned by the interviewees which they expressed as steps in the process to create a (cyber) security strategy.

- Threats (6)
- Current situation (6)
- Via a framework (6)
- Developments (5)
- Assets (4)
- Risk analysis (3)
- Link between the business strategy and the cyber security strategy (2)
- Scope (1)
- Gap analysis (1)
- Company landscape, both internal as external (1)
- Incidents (1)
- Evaluate before implementation (1)

- Stakeholders (1)
- Scenarios (1)
- Responsibilities (1)
- Baseline measurement (1)
- Vision of the future (1)

Although these elements are very high-level, some interviewees discuss, for example, different kinds of developments. For instance, one can look at internal developments, technical developments, and social developments.

These results show that the top 5 most mentioned process steps are analyzing the threats, analyzing the current situation, using a framework, analyzing development, and performing a risk analysis.

13.1.1.5.2 Is there a direct link between the cyber security strategy and cyber security risks?

The literature (see chapter 4) suggests that cyber security is closely related to risk management. Therefore interviewees were asked if there is a direct link between the cyber security strategy and cyber security risks. Four interviewees state that there is an obvious link between these concepts. One of the interviewees responded to this question with:

> *"Yes. We have a risk management process which has previously been defined. It starts with an information owner who determines a so-called code, then a risk analysis will be performed which results in certain measures. Accepting residual risks as part of the rest effect is part of identifying measures. Finally these measures are actually implemented and managed". – Expert 3*

Others (2) respond that there is a link between the cyber security strategy and cyber security risks, but these are not made explicit. Three interviewees also state that the link between risks and the strategy is made by doing a threat landscape analysis. However, not everyone agrees that a risk analysis is necessary to be performed (2) during the creation of a cyber security strategy.

It seems that the majority of the interviewees agree with the literature by confirming that there is a direct link between the cyber security strategy and cyber security risks. This link may either be made explicit or not, this depends on what is common in the company of interest.

13.1.1.5.3 Do you take into account current threats? And future threats?

In addition, the literature also suggests that the threat landscape is of importance in formulating a strategy. The interview results show that all interviewees think it is important to take into account current threats in formulating the cyber security strategy. However, taking into account future threats is not as easy as taking into account current threats.

> *"It is very important. The only problem is that as far as you know the threats of today, the ones of tomorrow you certainly don't know. So in your strategy, and that is that adaptive element you want, you will need to invent something how you will deal with receiving new knowledge and how you will process this in operational guidelines, standards, etcetera." – Expert 2*

Two other interviewees agreed. One interviewee added to this that it would be more interesting to look at what threats will become relevant in the future if the ambition is pursued.

> *"I think that the future threats are much more linked to the business model objectives for the coming years." – Expert 5*

These results show that there is a consensus in taking current threats into account. But it is more difficult to take future threats into account as they are very difficult to foresee.

13.1.1.5.4 Are stakeholders, and their roles and responsibilities, used in formulating the strategy? How?

Next, interviewees were asked whether it is necessary to involve stakeholders in the process of formulating the strategy, and making their roles and responsibilities clear. All interviewees (12) answered 'yes' to this question.

> *"Yes, we did this very clearly at company Y. A RACI table was drawn. This is how it should look like. This has to be done [involving stakeholders] because you have to get approval acceptance of your strategy. If I make up a strategy where you have a very important role, but you were not included in the process, then it will take a while before I have you motivated to execute the strategy." – Expert 5*

Four other interviewees mentioned the use of a RACI matrix to set and assign roles and responsibilities in a structured manner.

It is noticeable that is very important to involve stakeholders, either internal or external, in the creation of the cyber security strategy. Failing to do so may result in a lack of buy-in[12] by stakeholders according to interviewees.

13.1.1.5.5 Who 'guards' the construction / realization of the strategy?

In the process of creating a strategy it is important that this process is guided by a specific person, a so-called guardian. Six interviewees said the guard of the strategy is the security department or, more specifically, the CISO. Others (3) mention that the steering committee should guard the strategy. A more high-level answer was that the owner of the strategy, whoever that may be, should be the guardian (2). Besides the previously mentioned guards, the management board (2) was stated as a suitable guard or an external party (2), for instance, a consultant in control of the project.

> *"The steering committee. It cannot be the case that someone writes the strategy in isolation. The one that does that can better quit his job." – Expert 10*

> *"It often happens in two ways. If all is well, someone is eventually the owner of the strategy. This can be the CISO for example, that it is his strategy. But it might also be possible that, for example, the head of IT the owner of the strategy is, or someone else. The second thing is that the strategy is often translated into a number of projects or programs in which is embedded that strategic objectives are met." – Expert 11*

It has become clear that the construction and realization of the strategy should be guarded by the owner of the strategy, whether this is the security department, the CISO, or someone else.

13.1.1.5.6 In order to substantiate / realize the strategy, did you make use of frameworks / capabilities? Based on what criteria do you choose a framework?

And lastly, interviewees were asked whether they made use of frameworks or standards to substantiate the strategy, and if so, based on what criteria they choose such a framework. All interviewees (12) mention the use of frameworks as a tool to substantiate a strategy. Criteria for choosing a specific framework are:

- Practicality (2)
- What the external party uses (2)

[12] Supporting, disseminating, and ultimately implementing the cyber security strategy

- What is best for the company (2)
- The type of company (2)
- What the client uses (1)
- Based on the threats (1)
- Whether the industry considers it as a standard (1)
- What government defines as mandatory (1)

Frameworks are frequently used according to the interviewees. There are many frameworks available in the cyber security domain, for instance ISO 27001, NIST, and the government Baseline (BIR). Choosing a specific framework as a tool to substantiate the cyber security strategy may be of diverse reasons.

13.1.1.6 Other beliefs

In addition to the responses given above, interviewees mentioned other important information related to the process of formulating a cyber security strategy. Several interviews mention that a cyber security ambition and strategy is usually composed to last a maximum of three years. Every year the strategy should be evaluated on the projects followed and their results. Furthermore, several interviewees said that the commitment from the management board is crucial for the successful implementation of the cyber security strategy. Another interviewee said that he thought a cyber security strategy is only important for organizations who process data. In addition, two interviewees mentions that it is also a good idea to compose different scenarios of measures to be chosen. And lastly, sometimes an organization builds forward upon a previous strategy, if this one is usable.

13.1.2 Conclusion

The analysis of the interviews with cyber security experts shows that the cyber security ambition is mostly based on the business ambition and it should answer the ‘why’ question and contain an ambition level, it should be presented in a storytelling way with which employees can relate. However, the ambition statement should still be specific, measurable, acceptable, realistic, and time-oriented (SMART). Although there are different opinions in whether there should exist a separate cyber security ambition, it is clear however, that this cyber security ambition cannot be seen inextricably of the organization’s ambition.

The analysis also shows that most cyber security strategies are driven by the law or external regulators, incidents, and risks. Moreover, the three most important elements mentioned by the interviewees to substantiate a cyber security strategy are the threats, the current situation, and developments. In addition, the process followed to substantiate the strategy can either be by using a framework or by performing a risk analysis. Frameworks are frequently used according to the interviewees. There are many frameworks available in the cyber security domain, for instance ISO 27001, NIST, and the government Baseline (BIR). Choosing a specific framework as a tool to substantiate the cyber security strategy may be of diverse reasons. Risk analysis is usually done by using the IRAM technique or SPRINT forms.

The results also show that it seems that the majority of the interviewees agree with the literature by confirming that there is a direct link between the cyber security strategy and cyber security risks. This link may either be made explicit or not, this depends on what is common in the company of interest. In addition, there is a consensus in taking current threats into account. But it is more difficult to take future threats into account as they are very difficult to foresee. Also, it is noticeable that it is very important to involve stakeholders, either internal or external, in the creation of the cyber security strategy. Failing to do so may result in a lack of buy-in by stakeholders according to interviewee. The construction and realization of the strategy should be guarded by the owner of the strategy, whether this is the security department, the CISO, or someone else.

And lastly, it seems that there are different views on the role and position of security, but it is evident that it should always be seen and positioned separate from the IT department.

These results will provide input for creating the method and help to answer the sub questions, discussed in the nest section.

13.2 A cross-border analysis of national cyber security strategies

From the previous section we saw that strategy creation methods are mostly available in other domains than in the cyber security domain. In addition, no cyber security strategies from corporate organizations could be found online. These documents could give indirect insights in the method they used for creating that document. However, due to the transparent nature of public organizations, and their social responsibility towards citizens, it is not surprising that in the public domain cyber security strategies are generally published. Besides, citizens are one of the most important stakeholders in governmental cyber security strategies. Therefore these published strategies are a good basis for the understanding of a cyber security strategy. This understanding can create a basis for discussion about cyber security strategy in corporate organizations. By analyzing the strategy documents on content, and identifying what is generally described (e.g. strategic objectives, cyber threat landscape for a specific country), one can externalize the critical factors taken into account when constructing a security strategy and what steps were followed.

13.2.1 Step 1: Determine the strategic drivers and the scope

The determination of the strategic drivers and scope step resembles the introduction section of most national cyber security strategy documents. Here the drivers for having a strategy are discussed. For example, there could be more cyber-attacks in the last months or the economic impact resulting from a breach is very high for all stakeholders. In addition, the strategy is scoped according to what is held into account and what is not. This might include the definition of cyber security, to have everybody on the same page. For example, the following definitions for cyber security were used:

> *"The term 'cyber security' stands for the security of infrastructures in cyber space, of the data exchanged in cyber space and above all of the people using cyber space"* (Austria, 2013)
>
> *"Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured"* (Finland, 2013)
>
> *"Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in that transforms cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace"* (Hungary, 2013)

Although they are not similar to the one described by ENISA in the introduction, they do emphasize the cyber space as the environment where actions are performed and the environment which needs to be secured.

In addition, there is usually a link made to other strategic documents, like the national security strategy, and to previous cyber security strategies. For example, the Estonian Cyber Security Strategy (2014) already states in their introduction that "the Cyber Security Strategy 2014-2017 is the basic document for planning Estonia's cyber security and a part of Estonia's broader security strategy" and that "this strategy continues the implementation of many of the goals found in the Cyber Security Strategy 2008-2013; however, new threats and needs which were not covered by the previous strategy have also been added". In addition, compliance with law and the identification of stakeholders are also discussed and related to the strategic drivers and scope of the strategy.

FIGURE 36: A CROSS-BORDER ANALYSIS OF NATIONAL CYBER SECURITY STRATEGY DOCUMENTS

		EU Countries																Non-EU Countries													
		AUT	BEL	CZE	EST	FIN	FRA	ITA	DEU	HUN	LVA	LTU	NLD	POL	SVK	ESP	GBR	AUS	CAN	JPN	KEN	MNE	NZL	NOR	SGP	CHE	TUR	UGA	USA	GEO	KOR	TTO
1. Strategic drivers & scope	drivers	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
	economic impact							X			X						X	X	X					X		X						
	scope																	X									X					
	definition cyber security	X	X			X		X		X			X					X	X					X				X				X
	glossary	X	X			X		X	X		X	X		X							X	X	X	X			X					
	relation with other strategic documents	X		X	X	X				X	X	X	X	X	X	X	X	X			X	X		X		X		X				X
	relation with previous strategies				X		X						X							X						X							
	compliance with laws		X						X					X	X	X		X			X	X					X		X				
	stakeholders			X	X					X			X	X			X		X	X	X	X	X				X						
2. Cyberthreat landscape	threats	X					X	X	X	X			X			X	X	X	X	X	X	X	X	X	X	X	X		X				X
	risks	X														X				X		X					X	X	X				
	challenges				X			X						X							X	X		X						X			
	opportunities	X																															
	cyber trends		X		X				X				X				X			X	X												
	ICT trends		X		X								X					X		X					X			X					X
3. AS-IS situation	maturity analysis																				X							X					
	comparison with other countries														X													X					
	cyber security perspective EU														X																		
	SWOT analysis																											X					
	analysis of critical infrastructures																									X		X					
	analysis current situation				X					X	X				X							X				X		X					
4. TO-BE situation	vision				X	X				X							X								X			X				X
	mission																								X			X					
	ambition	X			X	X	X				X	X	X					X	X	X	X			X	X	X	X		X	X	X		
	- *guiding principles*	X		X	X	X					X					X	X	X		X						X	X	X	X	X		X
	strategic objectives	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X
	- *strategic priorities*														X		X	X					X	X					X				
	- *strategic measures*			X																													
	key benefits																				X												
5. Countermeasures	action	X	X				X	X		X	X	X	X	X	X	X	X	X	X	X		X		X		X	X	X	X	X	X	X	X
	action timeframe											X	X		X			X		X		X					X	X		X			
	action stakeholders											X	X									X					X	X		X			
	action plan											X	X				X					X		X			X	X		X			X
	action measures	X										X																					
	operational goals																																X
	important milestones and CSF																											X					
	roles and responsibilities government					X	X	X					X		X		X	X		X			X	X			X						X
	roles and responsibilities stakeholders		X			X	X	X	X				X		X		X	X		X		X		X			X	X		X		X
6. Implementation	implementation	X							X			X		X		X								X		X						
	follow-up	X									X				X			X		X							X						
	assessment of effectiveness													X				X															
	- *expected effects*													X																			
	- *effectiveness of actions*													X																			
	- *effectiveness measures*													X	X											X							
	consequences													X			X																
	organisation													X		X		X				X						X					X
	cooperation							X						X					X			X			X	X							
	financing													X	X			X										X					

13.2.2 Step 2: Analyze the cyber threat landscape

An important step within all national cyber security strategies is the assessment of the current and future cyber threat landscape, also as a way to illustrate the importance of having a cyber security strategy and to serve as a basis for the strategy. Here, threats, risks, attacks, challenges, opportunities, and trends are discussed in order to shape the threat environment the country is dealing with. A good example is Austria, who made a matrix (Figure 37) by comparing different threats against the probability of occurring and the consequence.

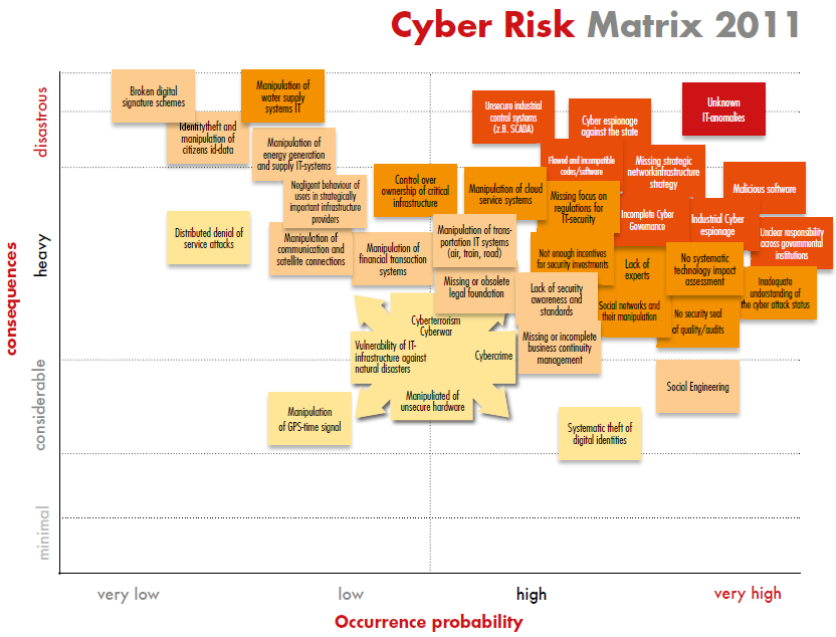


FIGURE 37: CYBER RISK MATRIX 2011 (Austria, 2013)

Another way of illustrating recent cyber-attacks is by showing a timeline, like Singapore (2013) did. In addition, some countries also identified challenges to cyber security. An example of a challenge to cyber security is the fact that the internet is more and more used for criminal activity and therefore gives cyberspace a rather negative image (Montenegro, 2013).

13.2.3 Step 3: Analyze the AS-IS situation

In the previous step, the focus was on the cyber threat landscape, i.e. the external landscape of the public agencies. Another important step is to analyze the AS-IS situation, or at least to identify what is already in place. The national cyber security strategies have shown that this could be assessed in different ways. One way is by doing a maturity analysis. Although this is a rather extensively used method in organizations, it seems that public organizations are not using these to assess current situations and base their strategic objectives on the identified gap (i.e. only Kenya and Uganda use this method); or not disclosing them. Other initiatives are an analysis of the current situation, what is already in place concerning cyber security. Less used methods are a SWOT analysis, comparison with other countries, comparison with the EU perspective, analysis of IS soft controls, analysis of critical infrastructures, and the analysis of social growth. For example, the Slovakia states that “the tasks defined for the forthcoming period are based on the current state of play in information security in Slovakia compared to the situation in other EU Member States and other advanced countries of the world” (Slovakia, 2008). ENISA published a good practice guide to national cyber security strategies, and one of their main points is to identify critical information infrastructures. However, not many strategy documents, except for Switzerland and Uganda, describe what a country’s critical information infrastructures are.

13.2.4 Step 4: Determine the TO-BE situation

The strategic drivers and the external and internal analysis of the country's environment will lead to the whole of strategic goals or the so-called desired TO-BE situation. Within this step, we distinguish the components listed in Figure 38, from high level to low level that constitute the strategy, based on their common occurrences in the national cyber security strategies.

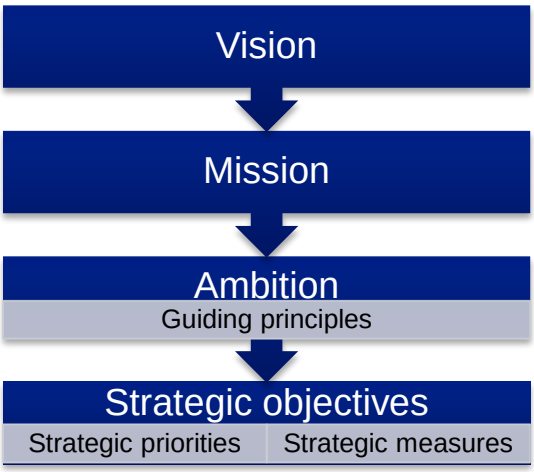


FIGURE 38: STRATEGY COMPONENTS DISTILLED FROM NATIONAL CYBER SECURITY STRATEGIES

An example of a vision is "Estonia is able to ensure national security and support the functioning of an open, inclusive and safe society" (Estonia, 2014). A mission is only mentioned twice, by Singapore and Uganda, where Singapore states that "the NCSM2018's mission is to enhance Singapore's cyber security capabilities in four focal areas – Government, Critical Infocomm Infrastructure (CII), Businesses and Individuals".

In addition, an example of an ambition is "the Netherlands is leading in the field of cybersecurity" (the Netherlands, 2013, p. 8). This ambition is supported by guiding principles, like "the Dutch society successfully makes optimal and safe use of the benefits of digitization" (the Netherlands, 2013, p. 8). Examples of strategic objectives, priorities or measures can be, amongst others, found in the strategy of the Czech Republic, Slovakia, and New Zealand. New Zealand's first priority is to create an increasing awareness and online security. The key initiative to this objective is "to partner with industry and non-government organizations, to centralize cyber security information and resources for ease of access, and deliver a coordinated cyber safety awareness-raising programme" (New Zealand, 2011).

Besides the above described strategy components, some countries also describe strategy guidelines (e.g. to which measures the strategy should satisfy) and key benefits of the strategy.

13.2.5 Step 5: Decide on the countermeasures to be taken

Building forward from the previous step, strategic goals, action plans and specific actions are discussed that need to be taken to implement the strategy. These usually consist of clear-cut actions that need to be undertaken by specific stakeholders, within a certain time, within a certain budget. The strategy of Lithuania does this elaborately in an action plan, illustrated in Figure 39. The strategy of Uganda also discusses important milestones that need to be achieved and critical success factors for the implementation of the strategy. Uganda is the only country that elaborates on these two topics. However, what is more commonly discussed is the roles and responsibilities of the government and stakeholders. There are special tasks for the government itself, which it should carry out. In addition, stakeholders involved in some way in the strategy. The government can also be the stakeholder, as the strategy could affect them as well. Therefore the distinction is made between roles and responsibilities of the government (the sender) and of stakeholders (the receiver).

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
1.	*1. To ensure the security of national information resources*		Level of compliance of national information resources with security requirements, (%)	–	95	98	All the institutions specified in items 3 to 29 of this Annex, according to their competences
2.		1.1. to improve the coordination and monitoring of electronic information security (cyber security);	Level of resources (%), security of which is monitored by an institution designated by the law on the basic requirements related to ensuring electronic information security (cyber security)	–	70	100	All the institutions specified in items 3 to 10 of this Annex, according to their competences
3.			Percentage of entities in defining and implementing national policy in the area of electronic information security (cyber security) that belong to the national system of coordination of electronic information security (cyber security), (%) Permanent collegial consultative council of electronic information security (cyber security) established	– –	80 yes	100 yes	Ministry of the Interior, Ministry of National Defence, Ministry of Transport and Communications, State Data Protection Inspectorate
4.			Number of evaluation studies of existing capabilities in the area of electronic information security (cyber security) and their potential	–	1	2	Ministry of the Interior

FIGURE 39: SCREENSHOT OF ACTION PLAN OF THE CYBER SECURITY STRATEGY OF LITHUANIA FOR 2011-2019 (Lithuania, 2012)

13.2.6 Step 6: Decide on implementation measures

After directed actions are discussed, some countries also roughly discuss how they are going to implement the strategy; the follow-up. For example, a follow-up could how the country will assess the effectiveness of the strategy every year after the implementation. To give meaning to the 'effectiveness of the strategy', some countries propose a measure, and elaborate on the expected effects. In addition, the effectiveness of specific actions was also discussed by Poland. Poland is one of the only country that discusses the topic of effectiveness elaborately, and dedicate a separate chapter to this topic. For example, an effectiveness measure is "the number of closed incidents in relation to the total number of categorized incidents" (Poland, 2013). In addition, they expect, amongst others that the strategy will result in a higher level of security and resistance against attacks (Poland, 2013). Also, they dedicate a section to the consequences of not achieving the desired effects.

Other more often used concepts regarding implementation are the governmental organization needed, collaboration with other both public and private institutions, and the financial resources necessary to implement the cyber security strategy.

13.2.7 Conclusion

The analysis of national cyber security strategies resulted in the following deduced method:

1. Determine the strategic drivers and the scope;
2. Analyze the cyber threat landscape;
3. Analyze the AS-IS situation;
4. Determine the TO-BE situation;
5. Decide on the countermeasures to be taken;
6. Decide on the implementation measures.

This method will be used later on in the process of creating an own method. This input will also be combined with the results from in-depth interviews with experts in the field of cyber security, discussed in the next chapter.

13.3 Workshop session and case study validation results

13.3.1 Workshop session validation of the conceptual method

13.3.1.1 Completeness

13.3.1.1.1 Which steps that you usually take to come to a cyber security strategy are missing in this method?

- The cyber strategy should be part of the overall business strategy. Just 'consider the organization's ambition' is not enough.
- Alignment business strategy.
- Key stakeholders.
- Governance and interactive key stakeholders.
- Within step 1, the link between the business strategy and the security strategy is not apparent.
- Step 3 could be considered together with step 1.
- Under step 4, consider adding prioritization step (for risks).
- Important to have senior management buy-in for the strategy (step 1).
- Cut in results brainstorm session (step 5.x).
- Brainstorm → interviews, workshops.
- Gantt chart/project planning (step 2.x).
- Project risks and dependencies (step 2.x).
- Define deliverables/outcomes (step 1.x)
- As-is situation should be more extensive
- None.

13.3.1.1.2 Which steps in this method do you consider redundant?

- 3. Analyze the landscape: this is also partly covered in step 1 (identify the need) and partly in step 4 (gap analysis - B). As a separate step it is not logical.
- Step 1.1 and 4.1 – identify the as-is.
- Step 1.1 and 3 – analyze the landscape.
- There is overlap/redundancy with step 1 and 3.
- 3.1 vs 1.1.1
- 3.2 too low-level
- 1.3 vs 3.5
- 6. Review if strategy fits risk.

13.3.1.2 Correctness

13.3.1.2.1 Do you think the order of the steps is right? Or do you use a different order in practice? If so, what order do you use?

- It begins with a cyber security strategy, but the steps later on are primarily the cyber security plan (the implementation of the strategy).
- Define the scope of the cyber security strategy should already be done in step 1.
- Correct.
- Step 2 could be the starting point (scope/stakeholders), rest is in logical order.
- Ok.
- Business should be involved at an earlier stage.
- Define desired outcome.
- Step 6 could be incorporated in another point.
- We miss a step which reviews all previous steps.

13.3.1.2.2 Which steps are the most important ones?

- Aligning with the business strategy.
- 1.1, 1.4, 4.1.
- 1, 2, and 3. Because if these are not done or incorrectly, the following steps will be based on possibly wrong assumptions.

- 1.5 and 5.1 deserve more emphasis.
- Business involvement.
- 1. Without the need and commitment the strategy will not be implemented.

13.3.1.2.3 Which steps are the least important ones?

- Elaborate on the strategy. This is not really relevant for the strategy, but it is for the implementation of the strategy.
- 3.2, 3.4, 3.5.
- Steps 5 and 6 seem to have overlap in several steps. Could perhaps be made more efficient.
- n/a.
- Project setup.
- 6. This could be incorporated in step 5.

13.3.1.2.4 Which steps are the most difficult ones to execute in practice?

- Defining the scope of the cyber security strategy.
- 6.3.6, 1.4.
- Step 1 and 2.
- 5.1.
- Determine the business value of the strategy.
- 1. Because you need to convince and engage people.

13.3.1.2.5 Which steps are the most time-consuming to carry out in practice?

- Complete gap analysis.
- 3.3, 4, 5.2.
- Step 4, due to interviews, benchmarking, and frameworks.
- 5.2.
- Determine the ambition.
- Stakeholder alignment.
- Scenario choosing.
- 1. People don't want to change and have their own idea about things. To convince them is the hardest part.

13.3.1.2.6 Which steps are unclear to you? Which ambiguities are currently in the method?

- Where 'strategy' is listed, it is not always clear if this is the security strategy or the overall strategy.
- 3: Link between threat analysis and as-is analysis is unclear. Partly in step 1, and partly in step 4.
- The 'optional' steps in 1 are more detailed in steps 3 and 4. So not really optional? Consider removing under step 1.
- n/a, we expect that every step has its own explanation.
- I would require definitions: when is a threat relevant? What is critical? Etc.
- 6.

13.3.1.3 Acceptability

13.3.1.3.1 Would you find it useful to use this method to construct a cyber security strategy for a corporate organization?

- Only if you continue with a security plan to close the gap. Just for the strategy, you can make the method shorter.
- Yes.
- Yes, it provides structure in the process.
- As a sanity check(list).
- This provides an outline which can be used to structure the process at the start.
- Recap/fallback for the project.
- Yes, it could be useful because it is a structured approach.
- Refined boundaries and constraints.
- It could possibly help to establish buy-in.

13.3.1.3.2 Would you actually use this model? If not, what has to be changed?

- Models are rarely used 'as-is', but are always useful as a basis to use for a specific project.
- Would use it.
- Yes it is useful, perhaps some steps could change order.

- Yes, if developed into user-friendly support package.
- Yes, what could be added are the outcomes of the steps. Right now it is much subject to interpretation.
- It could guidance and function as a supplement but not as the main driver.

13.3.1.4 Discussion

13.3.1.4.1 When do you use the risk analysis approach and when do you use the framework approach (in step 4)?

- Framework: you use this almost always, whether explicit (when asked for an ISO27001 implementation) or implicit (in order to ensure completeness of the subjects)
- Framework: maturity assessment. Risk: quantitative assessment.
- In our opinion, method B always needs to be used to determine risks and priorities. Method A is optional but does provide structure and benchmarking.
- They interlock. The risks analysis approach can fit in a framework; framework is optional, risk analysis is not.
- Inside out ('we want world-class'→ current risk do not matter/are not the driver) or outside in (we see these risks and will define a strategy to mitigate).
- Do not really understand the difference.

13.3.2 Case study validation of the conceptual method

13.3.2.1 Step 1: Identify the need for a cyber security strategy and determine the cyber security ambition

TABLE 13: CASE STUDY VALIDATION STEP 1

Sub activity	Present?	Sub sub activity	Present?
Consider a changing environment	Yes; within the drivers section it is noticable that a changing environment is considered and present as a driver.	**Consider the cyber threat landscape**	Yes; the cyber threat landscape is seen as a driver, therefore, must be considered.
		Consider the position of the organization in the marketplace	Yes; a comparison is made against industry companies and this result is a driver for a cyber security strategy.
		Consider the value of the information and risks involved	No. (but should be done)
		Consider developments and decreasing de-perimeterization	Yes, is considered for the need for a cyber security strategy.
Consider what is already in place	Yes; within the drivers section it is noticable that a changing environment is considered and present as a driver.		
Consider regulatory requirements	Yes; regulations are considered and is one of the drivers.		
Determine the cyber security ambition	Yes; a vision is determined. Also, visions per important domain are established.	**Identify the organization's ambition**	Yes; the business context is discussed.
		Decide on and describe the cyber security ambition by connecting it to the organization's ambition	Yes; a translation is made from the business goals to how cyber should support that business goal. The direct translation is present in another document.
Define strategic objectives and prioritize them	Yes; but these are only mentioned in the summary and in the TOM slides. No traceabilty and rationale behind these strategic objectives.		

13.3.2.2 Step 2: Define the cyber security strategy project setup

TABLE 14: CASE STUDY VALIDATION STEP 2

Sub activity	Present?	Sub sub activity	Present?
Determine and invite stakeholders for requirements setting	Yes; this is done but not written down in the CS strategy document.		
Define the scope of the cyber security strategy	Yes; but not documented.		
Set up definitions to use within strategy regarding cyber security	No. (But is considered to be very important to do)		

13.3.2.3 Step 3: Analyze the landscape

TABLE 15: CASE STUDY VALIDATION STEP 3

Sub activity	Present?	Sub sub activity	Present?
Identify relevant threats and associated risks	Yes; the threat context is identified.		
Identify vulnerabilities and associated risks	No. (but is considered to be important)		
Identify most critical assets and associated risks	No. (but is considered to be important)		
Identify incidents and associated risks	Yes; this is done.		
Identify laws & regulations and associated risks	Yes; this is done and (therefore) part of a strategic objective.		

13.3.2.4 Step 4: Perform a gap analysis

TABLE 16: CASE STUDY VALIDATION STEP 4

Sub activity	Present?	Sub sub activity	Present?
Define the as-is situation (via a framework)	Yes; a current maturity is presented.	**Choose a framework**	Yes; however why (because it is easy to communicate to the board) they chose the framework is not given.
		Assess the current status	Yes; this is done using the NIST model.
		Benchmark assessment	Partly; one of the drivers is that the maturity is below industry peers. A benchmark is performed, but not documented.

		Describe the results	Yes; the results are described in a separate excel sheet and summarized in a table in the slides.
Define the to-be situation (via a framework)	Yes; a target maturity is defined for every area.		
Define the amount at risk (via risk analysis)	-	**Define the amount at risk for every critical asset**	-
		Consider risks found in the previous step	-
		Describe the total amount at risk	-
Define the risk appetite (via risk analysis)	Yes; a very high-level risk appetite is described.		
Evaluate the risks (via risk analysis)	-		
Determine the gap	Yes, the gaps are described		

13.3.2.5 Step 5: Define multiple scenarios

TABLE 17: CASE STUDY VALIDATION STEP 5

Sub activity	Present?	Sub sub activity	Present?
Perform multiple sessions with stakeholders to come up with multiple measures	Yes; multiple measures in term of projects with associated activities are presented and these were devised by the stakeholders.		
Define the business case for every measure	No. Only costs are identified.		
Group measures into scenario	No.		
Determine top three potentially best scenarios	No.	**Define implementation effort**	No; not for a scenario.
		Define costs	No; not for a scenario.
		Define resources needed	No; not for a scenario.
		Define residual risk	No; not for a scenario.
Let the management board choose one or more scenarios to elaborate on	No.		

13.3.2.6 Step 6: Elaborate on chosen scenario

TABLE 18: CASE STUDY VALIDATION STEP 6

Sub activity	Present?	Sub sub activity	Present?
Describe the scenario in detail	Yes; the chosen solution is elaborated in detail.		
Describe the effect on the organization	Yes; this is described using a target operating model, amongst others.	**Describe effect on the staff**	Yes; this is described in the TOM.
		Describe effect on the skills	Yes; this is described in the TOM.
		Describe effect on the knowledge	Sort of; indirectly one can deduce this from the target state measures as described in the TOM slides.
		Describe effect on the processes	Yes; the target state measures in the TOM slides describe this.
		Describe effect on the technologies	No. (but is considered important)
		Describe effect on the culture	No. (but is considered important to take into account, but shouldn't be described)
		Describe effect on the roles and responsibilities	Yes; within the organizational overview of the current state assessment & target state of the TOM slides, roles and responsibilities are presented.
Describe the roadmap	Yes; the roadmap is described in detail. A seperate excel sheet details all activities related to achieving the vision from the current situation.	**Define the milestones**	Yes; the deadlines for the projects are presented.
		Define the time needed	Yes; the time needed to execute the projects are presented.
		Define the money needed	Yes; the total FTE cost, license / toolin cost, and deadline cost are given.
		Define the resources needed	Yes; the number of FTE, the costs associated, total FTE, and effort is given.
		Define the collaboration needed	Yes; dependencies are presented.
		Define the quality	No.
		Define the measures for effectiveness	No.

13.3.2.7 Additional notes

The business goals are also considered as driver for a CS strategy. Guiding principles for the creation of the strategy are given. There are three threat categories identified. For every threat category, an actor, method, motivation, and targets are given. Also, attack sophistication is discussed. A graph is presented with attacks, based on their risk and sophistication. With the assessment of the current and target maturity, a conclusion and summary is given. As well as which running projects are linked to the areas of interest. Although implementation effort, costs, and resources needed are not discussed in the context of scenarios, they are discussed in the roadmap. Scenarios have been developed for a proposed organizational structure in the TOM slides. A target operating model is used to present how the organization will have to change to successfully implement the roadmap and achieve the vision. In addition, the roadmap shows which new and/or existing fit with the newly suggested projects. Also, for every domain in the roadmap a specific vision is given.

13.3.3 Changes based on validation

TABLE 19: CHANGES IN CONCEPTUAL METHOD BASED ON VALIDATION

	From	In	To	In	Evidence
Modify	Define the cyber security strategy project setup		Define the cyber security strategy operating setup		Workshop session
Modify	- Analyze the landscape - Perform a gap analysis (by using a framework or performing a risk analysis)		Analyze the landscape		Workshop session
Modify	- Define multiple scenarios - Elaborate on chosen scenario		Describe multiple strategic objectives and associated tasks		Workshop session
Modify	Consider what is already in place	Identify the need for a cyber security strategy and determine the ambition: consider a changing environment	Consider what strategy and controls are already in place	Identify the need for a cyber security strategy and determine the ambition: consider a changing environment	Workshop session
Modify	Define the scope of the cyber security strategy	Define the cyber security strategy project setup	Define the scope of the cyber security strategy	Identify the need for a cyber security strategy and determine the cyber security ambition	Workshop session
Modify	Consider the organization's ambition	Identify the need for a cyber security strategy : determine the cyber security ambition	Identify the organization's ambition	Identify the need for a cyber security strategy : determine the cyber security ambition	Workshop session

	From	In	To	In	Evidence
Modify	Decide on and describe the cyber security ambition by connecting it to the organization's ambition	Identify the need for a cyber security strategy : determine the cyber security ambition	Decide on and describe the cyber security ambition by connecting it to and making it part of the organization's strategy	Identify the need for a cyber security strategy : determine the cyber security ambition	Workshop session
Insert			Optional: determine cyber security visions per domain the cyber security ambition applies to	Identify the need for a cyber security strategy	Case study
Modify	Define strategic objectives and prioritize them	Identify the need for a cyber security strategy	5. Perform a brainstorm session with stakeholders to communicate problem areas and decide on multiple strategic objectives (directions) 6. Prioritize strategic objectives with stakeholders	Describe multiple strategic objectives and associated tasks	Workshop session
Insert			Define guiding principles of the cyber security strategy	Identify the need for a cyber security strategy and determine the ambition	Workshop session
Insert			Define desired outcomes of the cyber security strategy	Identify the need for a cyber security strategy and determine the ambition	Workshop session
Modify	Set up definitions to use within strategy regarding cyber security	Define the cyber security strategy project setup	Set up definitions to use within the cyber security strategy regarding cyber security	Define the cyber security strategy operating setup	Workshop session

	From	In	To	In	Evidence
Insert			Define the governance of the cyber security strategy	Define the cyber security strategy operating setup	Workshop session
Insert			Define strategy dependencies	Define the cyber security strategy operating setup	Workshop session
Insert			Describe desired interaction with key stakeholder	Define the cyber security strategy operating setup	Workshop session
Modify	- Identify relevant threats and associated risks - Identify vulnerabilities and associated risks - Identify most critical assets and associated risks - Identify incidents and associated risks - Identify laws & regulations	Analyze the landscape	- Identify relevant threats and associated risks - Identify vulnerabilities and associated risks - Identify most critical assets and associated risks - Identify incidents and associated risks - Identify requirements (external and internal laws and regulations)	Analyze the current situation: analyze the internal and social landscape	Workshop session, case study
Insert			- Identify running activities related to cyber security - Identify the internal culture	Analyze the current situation: analyze the internal and social landscape	Case study
Insert			Evaluate landscape analysis with stakeholders and adjust if necessary	Analyze the current situation	Case study

	From	In	To	In	Evidence
Modify	- Determine the gap - Determine the gap	Perform a gap analysis: via a framework and via a risk analysis	Determine and prioritize the gaps	Analyze the current situation	Workshop session
Insert			Evaluate gap analysis with stakeholders and adjust if necessary	Analyze the current situation	Case study
Insert			Define problem areas based on the landscape and gaps found	Analyze the current situation	Logic
Insert			Evaluate results of brainstorm session and adjust if necessary	Describe multiple strategic objectives and associated tasks	Workshop session
Modify	Define the business case for every measure	Define multiple scenarios	Define the business case for every strategic objective	Describe multiple strategic objectives and associated tasks	Logic
Delete	Group measures into scenario	Define multiple scenarios			Workshop session
Delete	- Determine the top three potentially best scenarios - Define implementation effort - Define costs - Define resources needed - Define effects on residual risks	Define multiple scenarios			Workshop session
Insert			Determine high-level activities and associated options for every strategic objective	Describe multiple strategic objectives and associated tasks	Logic, case study
Modify	Describe the roadmap	Elaborate on chosen scenario	Elaborate on the high-level activities	Describe multiple strategic objectives and associated tasks	Logic
Modify	- Define the milestones	Elaborate on chosen scenario:	- Define the milestones	Describe multiple strategic objectives and	Workshop session

	From	In	To	In	Evidence
	- Define the time needed - Define the money needed - Define resources needed - Define the measures for effectiveness	describe the roadmap	- Define the time needed - Define the money needed - Define resources needed - Define the measures for effectiveness and intermediary goas	associated tasks: elaborate on the high-level activities	
Delete	- Define quality	Elaborate on chosen scenario: describe the roadmap			Case study
Insert			- Define the collaboration needed - Define the responsibilities	Describe multiple strategic objectives and associated tasks: elaborate on the high-level tasks	Workshop session
Delete	Describe the scenario in detail	Elaborate on chosen scenario			Logic
Modify	- Describe the effect on the organization - Describe effect on the staff - Describe effect on the skills - Describe effect on the knowledge - Describe effect on the processes - Describe effect on the technologies - Describe effect on the culture - Describe effect on the	Elaborate on chosen scenario	- Describe the effect on the organization - Describe effect on the staff - Describe effect on the skills - Describe effect on the knowledge - Describe effect on the processes - Describe effect on the technologies - Describe effect on the roles and responsibilities	Describe multiple strategic objectives and associated activities: describe the effect on the strategy of the organization.	Case study, logic

	From	In	To	In	Evidence
	roles and responsibilities				

13.4 Additional resources from the conceptual method

13.4.1 Evidence

TABLE 20: EVIDENCE TABLE CONCEPTUAL METHOD

Nr	Activity	Reference
1.	Identify the need for a cyber security strategy and determine the ambition	• Literature: 5.2, 5.4 • Interviews: all (14) • NCSS: 13.2.1, 13.2.4 (1. Strategic drivers & scope: drivers, 4. To-be situation: vision, ambition)
1.1	Consider a changing environment	• Literature: 1.1, 1.2, 4.1, 4.3, 5.1 • Interviews: 1, 7, 8, 9, 12 • NCSS: 13.2.2 (2. Analyze the cyber threat landscape: cyber trends, ICT trends)
1.1.1	Consider the cyber threat landscape	• Literature: 4.2.6, 4.3 • Interviews: 1, 9, 10 • NCSS: -
1.1.2	Consider the position of the organization in the marketplace	• Literature: 6.1.1, 6.1.2, 6.1.3 • Interviews: - • NCSS: -
1.1.3	Consider the value of the information and risks involved	• Literature: • Interviews: 4, 5, 6, 7, 8 • NCSS: 13.2.2 (2. Analyze the cyber threat landscape: risks)
1.1.4	Consider developments and decreasing de-perimeterisation	• Literature: 4.1, 4.3 • Interviews: 1, 7, 8, 9, 12 • NCSS: -
1.2	Consider what is already in place	• Literature: - • Interviews: 3, 4, 7, 8, 9, 10, 11 • NCSS: 13.2.3 (3. As-is situation: analysis current situation)
1.3	Consider regulatory requirements	• Literature: - • Interviews: 2, 3, 4, 6, 7, 8, 9, 12 • NCSS: 13.2.1 (1. Strategic drivers & scope: compliance with laws)
1.4	Determine the cyber security ambition	• Literature: 2.1, 5.2 • Interviews: 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12 • NCSS: 13.2.4 (4. To-be situation: vision, ambition)
1.4.1	Consider the organization's ambition	• Literature: 5.5 • Interviews: 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12 • NCSS: 13.2.1 (1. Strategic driver & scope: relation with other strategic documents)
1.4.2	Decide on and describe the cyber security ambition by connecting it to the organization's ambition	• Literature: 5.5 • Interviews: 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12 • NCSS: 13.2.1 (1. Strategic driver & scope: relation with other strategic documents)
1.5	Define strategic objectives and prioritize them	• Literature: 5 • Interviews: - • NCSS: 13.2.4 (4. To-be situation: strategic objectives, strategic priorities)
2.	Define CSS project setup	• Literature: - • Interviews: - • NCSS: 13.2.1 (1. Strategic drivers & scope)
2.1	Determine and invite stakeholders for requirements setting	• Literature: - • Interviews: All (14)

		• NCSS: 13.2.1 (1. Strategic drivers & scope: stakeholders)
2.2	Define the scope of the cyber security strategy	• Literature: 6.1.3 • Interviews: 11 • NCSS: 13.2.1 (1. Strategic drivers & scope: scope)
2.3	Set up definitions to use within strategy regarding cyber security	• Literature: - • Interviews: - • NCSS: 13.2.1 (1. Strategic drivers & scope: definition cyber security, glossary)
3.	Analyze the landscape	• Literature: 6.1, 6.2, 6.3 • Interviews: 9 • NCSS: 13.2.2 (2. Analyze cyber threat landscape)
3.1	Identify relevant threats	• Literature: 4.2.6, 6.1.1.5 • Interviews: all (14) • NCSS: 13.2.2 (2. Analyze cyber threat landscape: threats)
3.2	Identify vulnerabilities and associated risks	• Literature: 4.2.4 • Interviews: 4, 10, 11, 12 • NCSS: -
3.3	Identify most critical assets and associated risks	• Literature: 4.2.2 • Interviews: 4, 10, 11, 12 • NCSS: 13.2.3 (3. As-is situation)
3.4	Identify incidents and associated risks	• Literature: - • Interviews: 2, 3, 4, 5, 7, 8, 10, 12 • NCSS: -
3.5	Identify laws & regulations and associated risks	• Literature: 6.1.1.4, 6.1.3 • Interviews: 2, 3, 4, 6, 7, 8, 9, 12 • NCSS: 13.2.1 (1. Strategic drivers & scope: compliance with laws)
4.	Perform a gap analysis	• Literature: - • Interviews: 6, 7, 11, 12 • NCSS: 13.2.3 (3. To-be situation)
4.1A	Define the as-is situation	• Literature: - • Interviews: 3, 4, 7, 8, 9, 11 • NCSS: 13.2.3 (3. To-be situation: maturity analysis, SWOT analysis, analysis current situation)
4.1.1A	Choose a framework	• Literature: - • Interviews: 1, 2, 4, 5, 6, 7, 8, 9, 10, 11 • NCSS: -
4.1.2A	Assess the current status	• Literature: - • Interviews:1, 2, 4, 5, 6, 7, 8, 9, 10, 11 • NCSS: 13.2.3 (3. To-be situation: maturity analysis, SWOT analysis, analysis current situation)
4.1.3A	Benchmark assessment	• Literature: - • Interviews: 14 • NCSS: 13.2.3 (3. As-is situation: comparison with other countries)
4.1.4A	Describe the results	• Literature: - • Interviews: - • NCSS: - (+ logic)
4.2A	Define the to-be situation	• Literature: • Interviews: • NCSS: 13.2.4 (4. To-be situation)
4.1B	Define the amount at risk (as-is)	• Literature: 4.2.5 • Interviews: 1, 2, 3, 4, 6, 7, 8, 10, 11, 12 • NCSS: -
4.1.1B	Define the amount at risk for every critical asset	• Literature: - • Interviews: 6 • NCSS: -
4.1.2B	Consider risks found in step 3	• Literature: - • Interviews: - • NCSS: - (+ logic)
4.1.3B	Describe total amount at risk	• Literature: -

		• Interviews: - • NCSS: - (+ logic)
4.2B	Define risk appetite (to-be)	• Literature: 4.2.5? • Interviews: 1, 2, 3, 4, 6, 7, 8 • NCSS: -
4.3B	Evaluate the risks	• Literature: - • Interviews: - • NCSS: - (+ logic)
4.4	Determine the gap	• Literature: • Interviews: 6, 7, 11, 12 • NCSS: -
5.	Define multiple scenarios	• Literature: - • Interviews: 9 • NCSS: -
5.1	Perform a brainstorm session with stakeholders to come up with multiple measures	• Literature: - • Interviews: 7 • NCSS: 13.2.5 (5. Countermeasures: action)
5.2	Define the business case for every measure	• Literature: - • Interviews: 1, 9, 14 • NCSS: -
5.3	Group measures into scenario	• Literature: - • Interviews: 9 • NCSS: -
5.4	Determine top three potentially best scenarios	• Literature: - • Interviews: - • NCSS: - (+ logic)
5.4.1	Define implementation effort	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action plan)
5.4.2	Define costs	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action plan)
5.4.3	Define resources needed	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action plan)
5.4.4	Define effects on residual risk	• Literature: - • Interviews: - • NCSS: - (+ logic)
5.5	Let the board of directors choose one or more scenarios to elaborate on	• Literature: - • Interviews: - • NCSS: - (+ logic)
6.	Elaborate on chosen scenario	• Literature: - • Interviews: - • NCSS: - (+ logic)
6.1	Describe the scenario in detail	• Literature: - • Interviews: - • NCSS: - (+ logic)
6.2	Describe the effect on the organization	• Literature: - • Interviews: - • NCSS: 13.2.6 (6. Implementation: consequences, organization)
6.2.1	Describe the effect on the staff	• Literature: 6.1.1.2 • Interviews: - • NCSS: 13.2.6 (6. Implementation: consequences, organization)
6.2.2	Describe the effect on the skills	• Literature: 6.1.1.2 • Interviews: - • NCSS: 13.2.6 (6. Implementation: consequences, organization)
6.2.3	Describe the effect on the knowledge	• Literature: • Interviews: -

		• NCSS: 13.2.6 (6. Implementation: consequences, organization)
6.2.4	Describe the effect on the processes	• Literature: 6.1.1.2 • Interviews: 10, 14 • NCSS: -
6.2.5	Describe the effect on the technologies	• Literature: 6.1.1.4 • Interviews: 10, 14 • NCSS: -
6.2.6	Describe effect on the culture	• Literature: 6.1.1.2, 6.1.2, 6.1.3 • Interviews: 13, 14 • NCSS: -
6.2.7	Describe effect on the roles and responsibilities	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action stakeholders, roles and responsibilities government, roles and responsibilities stakeholders)
6.3	Describe the roadmap	• Literature: - • Interviews: 4, 6, 7, 9, 11, 12 • NCSS: 13.2.5 (5. Countermeasures: action plan)
6.3.1	Define the milestones	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: important milestones and CSF)
6.3.2	Define time needed	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action timeframe)
6.3.3	Define money needed	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action plan)
6.3.4	Define resources needed	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action plan)
6.3.5	Define quality	• Literature: - • Interviews: - • NCSS: - (+ logic)
6.3.6	Define required collaboration	• Literature: - • Interviews: - • NCSS: 13.2.5 (6. Implementation: cooperation)
6.3.7	Define the measures for effectiveness	• Literature: - • Interviews: - • NCSS: 13.2.6 (6. Implementation: assessment of effectiveness, expected effects, effectiveness of actions, effectiveness measures)

13.4.2 Activity tables

TABLE 21: ACTIVITY TABLE CONCEPTUAL METHOD

Activity	Sub activity	Description	Role
Identify the need for a cyber security strategy and determine the ambition	Consider a changing environment	The management board considers the ENVIRONMENT on a high-level, which might be part of the NEED FOR A CYBER SECURITY STRATEGY. The elements to be assessed in the ENVIRONMENT can be SOCIAL, EXTERNAL, and/or INTERNAL (see section **Error! Reference ource not found.**)	Management board
	Consider what is already in place	The management board considers the CURRENT SITUATION on a high-level, which might be part of the NEED FOR A CYBER SECURITY STRATEGY.	Management board

Activity	Sub activity	Description	Role
	Consider regulatory requirements	The management board considers the LAWS & REGULATIONS on a high-level, which might be part of the NEED FOR A CYBER SECURITY STRATEGY.	Management board
	Determine the cyber security ambition	If there is a NEED FOR A CYBER SECURITY STRATEGY, the management board will need to determine a CYBER SECURITY AMBITION.	Management board
	Define strategic objectives and prioritize them	Based on the CYBER SECURITY AMBITION, the management board defines one or more STRATEGIC OBJECTIVES. Every STRATEGIC OBJECTIVE is stored in a LIST OF STRATEGIC OBJECTIVES.	Management board
Determine the scope and stakeholders / Define CSS project setup	Determine and invite stakeholders for requirements setting	The steering committee will determine and invite every STAKEHOLDER, INTERNAL or EXTERNAL, for the upcoming activities. A STAKEHOLDER is stored in a LIST OF STAKEHOLDERS which can be used later on.	Steering committee
	Define the scope of the cyber security strategy	The steering committee will decide on the SCOPE for the CYBER SECURITY STRATEGY by determining SCOPING REQUIREMENTS.	Steering committee
	Set up definitions to use within strategy regarding cyber security	The steering committee will set up DEFINITIONS to use within the CYBER SECURITY STRATEGY. Every DEFINITION is stored in a LIST OF CYBER SECURITY DEFINITIONS.	Steering committee
Analyze the landscape	Identify relevant threats and associated risks	The steering committee, together with the stakeholders, identifies relevant THREATS and associated RISKS facing the organization. Zero or more THREATS are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify vulnerabilities and associated risks	The steering committee, together with the stakeholders, identifies relevant VULNERABILITIES and associated RISKS facing the organization. Zero or more VULNERABILITIES are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify most critical assets and associated risks	The steering committee, together with the stakeholders, identifies relevant CRITICAL ASSETS and associated RISKS facing the organization. Zero or more CRITICAL ASSETS are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify incidents and associated risks	The steering committee, together with the stakeholders, identifies relevant INCIDENTS and associated RISKS facing the organization. Zero or more INCIDENTS are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify laws & regulations and associated risks	The steering committee, together with the stakeholders, identifies relevant LAWS & REGULATIONS and associated RISKS facing the organization. Zero or more LAWS & REGULATIONS are stored in a LANDSCAPE description.	Steering committee, stakeholders
Perform a gap analysis	Define the as-is situation (via a framework)	The steering committee, together with the stakeholders, will define the AS-IS SITUATION by using a framework of choice as a reference.	Steering committee, stakeholders
	Define the to-be situation (via a framework)	The steering committee, together with the stakeholders, will define the TO-BE SITUATION by using a framework of choice as a reference.	Steering committee, stakeholders

Activity	Sub activity	Description	Role
	Define the amount at risk (via risk analysis)	The steering committee, together with the stakeholders, will define the AMOUNT AT RISK for every critical asset by using a risk analysis approach.	Steering committee, stakeholders
	Define the risk appetite (via risk analysis)	The steering committee, together with the stakeholders, will define the RISK APPETITE by considering the RISKS found in the previous step using a risk analysis approach.	Steering committee, stakeholders
	Evaluate the risks (via risk analysis)	The steering committee, together with the stakeholders, will evaluate the risks (RISK EVALUATION).	Steering committee, stakeholders
	Determine the gap	The steering committee, together with the stakeholders, determine the GAP between the AS-IS SITUATION and the TO-BE SITUATION or between the AMOUNT AT RISK and the RISK APPETITE, dependent on the chosen gap analysis approach.	Steering committee, stakeholders
Define multiple scenario's	Perform multiple sessions with stakeholders to come up with multiple measures	The management board and the steering committee, together with the stakeholders, will perform multiple sessions to come up with multiple MEASURES to close the GAP found in the previous step.	Management board, steering committee, stakeholders
	Define the business case for every measure	The steering committee defines the BUSINESS CASE for every MEASURE.	Steering committee
	Group measures into scenario	The steering committee groups every MEASURE into one or more SCENARIOS, based on, for example, implementation time and costs.	Steering committee
	Determine top three potentially best scenarios	The management board and the steering committee, together with the stakeholders, will work out a top three of potentially best SCENARIOS, which is based on the MEASURES and BUSINESS CASES found in the previous sub activity.	Steering committee
	Let the management board choose one or more scenarios to elaborate on	The management board will make a decision about one or more SCENARIOS to elaborate on (CHOSEN SCENARIO).	Management board
Elaborate on chosen scenario	Describe the scenario in detail	The steering committee elaborates on the chosen scenario in detail, resulting in a DETAILED SCENARIO.	Steering committee
	Describe the effect on the organization	The steering committee describes the EFFECT on the organization for implementing the CYBER SECURITY STRATEGY. The EFFECT, DETAILED SCENARIO, RISK GAP ANALYSIS RESULT or FRAMEWORK GAP ANALYSIS RESULT, LANDSCAPE, CSS PROJECT SETUP, STRATEGIC OBJECTIVES, CYBER SECURITY AMBITION and the NEED FOR CYBER SECURITY STRATEGY provide input for the CYBER SECURITY STRATEGY.	Steering committee
	Describe the roadmap	The steering committee describes the ROADMAP to implement the CYBER SECURITY STRATEGY in a certain timespan.	Steering committee

Sub activity	Sub sub activity	Description	Role
Consider a changing environment	Consider the cyber threat landscape	The management board may consider the CYBER THREAT LANDSCAPE as part of the ENVIRONMENT description.	Management board
	Consider the position of the organization in the marketplace	The management board may consider the POSITION OF THE ORGANIZATION in the marketplace as part of the ENVIRONMENT description.	Management board
	Consider the value of the information and risks involved	The management board may consider the VALUE OF THE INFORMATION and the RISKS INVOLVED as part of the ENVIRONMENT description.	Management board
	Consider developments and decreasing de-perimeterization	The management board may consider the CONSEQUENCE OF DEVELOPMENTS and the CONSEQUENCE OF DE-ERIMETERISATION as part of the ENVIRONMENT description.	Management board
Determine the ambition	Identify the organization's ambition	The steering committee identifies the ORGANIZATION'S AMBITION.	Steering committee
	Decide on and describe the cyber security ambition by connecting it to the organization's ambition	The steering committee decides on and describes the CYBER SECURITY AMBITION based on the ORGANIZATION'S AMBITION.	Steering committee
Define the as-is situation	Choose a framework	The steering committee chooses a cyber security FRAMEWORK to assess the AS-IS SITUATION.	Steering committee
	Assess the current status	The steering committee uses the cyber security FRAMEWORK to assess the STATUS of the AS-IS SITUATION.	Steering committee
	Benchmark assessment	The steering committee BENCHMARKS the STATUS against the status of likewise organizations.	Steering committee
	Describe the results	The steering committee describes the results of analysing the AS-IS SITUATION with a FRAMEWORK.	Steering committee
Define the amount at risk	Define the amount at risk for every critical asset	The steering committee defines the AMOUNT AT RISK PER CRITICAL ASSET. These are stored in a LIST OF RISKS.	Steering committee, stakeholders
	Consider risks found in the previous step	The steering committee considers the RISKS found in the previous step.	Steering committee
	Describe the total amount at risk	The steering committee describes the total amount at risk as the RISK AS-IS SITUATION.	Steering committee
Determine top three potentially best scenarios	Define implementation effort	The steering committee defines the IMPLEMENTATION EFFORT for every MEASURE.	Steering committee
	Define costs	The steering committee defines the COSTS for every MEASURE.	Steering committee
	Define resources needed	The steering committee defines the RESOURCES NEEDED for every MEASURE.	Steering committee
	Define residual risk	The steering committee defines the RESIDUAL RISK for every MEASURE.	Steering committee
	Decide on top three scenarios	The steering committee decides on the top three SCENARIOS based on the SCENARIOS created in the previous step.	Steering committee
Describe the effect on the organization	Describe effect on the staff	The steering committee describes the EFFECT on the STAFF when the CHOSEN SCENARIO is implemented.	Steering committee

Sub activity	Sub sub activity	Description	Role
	Describe effect on the skills	The steering committee describes the EFFECT on the SKILLS of the staff when the CHOSEN SCENARIO is implemented.	Steering committee
	Describe effect on the knowledge	The steering committee describes the EFFECT on the KNOWLEDGE of the staff when the CHOSEN SCENARIO is implemented.	Steering committee
	Describe effect on the processes	The steering committee describes the EFFECT on the PROCESSES when the CHOSEN SCENARIO is implemented.	Steering committee
	Describe effect on the technologies	The steering committee describes the EFFECT on the TECHNOLOGIES when the CHOSEN SCENARIO is implemented.	Steering committee
	Describe effect on the culture	The steering committee describes the EFFECT on the CULTURE when the CHOSEN SCENARIO is implemented.	Steering committee
	Describe effect on the roles and responsibilities	The steering committee describes the EFFECT on the ROLES & RESPONSIBLITIES when the CHOSEN SCENARIO is implemented.	Steering committee
Describe the roadmap	Define the milestones	To construct the ROADMAP, the steering committee defines the MILESTONES. Every MILESTONE is stored in a LIST OF MILESTONES.	Steering committee
	Define the time needed	To construct the ROADMAP, the steering committee defines the TIME NEEDED.	Steering committee
	Define the money needed	To construct the ROADMAP, the steering committee defines the MONEY NEEDED.	Steering committee
	Define the resources needed	To construct the ROADMAP, the steering committee defines the RESOURCES NEEDED.	Steering committee
	Define the collaboration needed	To construct the ROADMAP, the steering committee defines the COLLABORATION NEEDED.	Steering committee
	Define the quality	To construct the ROADMAP, the steering committee defines the necessary QUALITY to be achieved for the different projects.	Steering committee
	Define the measures for effectiveness	To construct the ROADMAP, the steering committee defines the necessary EFFECTIVENESS MEASURES to be achieved for the different projects. Every EFFECTIVENESS MEASURE is stored in a LIST OF EFFECTIVENESS MEASURES.	Steering committee

13.4.3 Concept tables

TABLE 22: CONCEPT TABLE CONCEPTUAL METHOD

Concept	Description
ENVIRONMENT	The internal and external surroundings of the organization of interest.
SOCIAL ENVIRONMENT	"The social environment encompass the immediate physical surroundings, social relationships, and cultural milieus within which defined groups of people function and interact"[7].
EXTERNAL ENVIRONMENT	The external environment consists of elements that exist outside the organization that are hard to control, but do influence the organization in different ways.
INTERNAL ENVIRONMENT	The internal environment deals with all elements that exist within the organization.
CURRENT SITUATION	The present status of how cyber security is arranged at the organization of interest.
LAWS & REGULATIONS	(a system of) Rules that must be followed, induced by an authority.

Concept	Description
NEED FOR A CYBER SECURITY STRATEGY	The rationale of having a cyber security strategy.
CYBER SECURITY AMBITION	A certain goal or aim: something an organization wants to do or achieve with cyber security.
STRATEGIC OBJECTIVE	"A broadly defined, measurable objective that an organization must achieve to make its strategy succeed" http://www.businessdictionary.com/definition/strategic-objective.html
LIST OF STRATEGIC OBJECTIVES	A list containing all strategic objectives.
STAKEHOLDER	"People or small groups with the power to respond to, negotiate with, and change the strategic future of the organization" (Eden & Ackermann, 1998, p. 117).
INTERNAL STAKEHOLDER	A stakeholder who resides within the organization of interest.
EXTERNAL STAKEHOLDER	A stakeholder who resides outside the organization of interest.
LIST OF STAKEHOLDERS	A list containing information about one or more stakeholders.
SCOPING REQUIREMENT	A requirement about the boundaries of the cyber security project.
DEFINITION	A formal statement of the explanation of a concept.
LIST OF CYBER SECURITY DEFINITIONS	A list containing one or more definitions related to the field of cyber security.
CSS PROJECT SETUP	A document containing information about the stakeholders, scope, and cyber security definitions.
THREAT (AND RISK)*	"Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service (NIST, 2012)".
VULNERABILITY (AND RISK)*	"A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events" (ISACA, 2014)
CRITICAL ASSET (AND RISK)*	"Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances, and reputation" (ISACA, 2014)
INCIDENT (AND RISK)*	"Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service" (ISACA, 2014).
LAWS & REGULATIONS (AND RISK)*	(a system of) Rules that must be followed, induced by an authority.
LANDSCAPE	The aspects of the cyberspace influencing the organization of interest.
RISK	"A function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" (NIST, 2012)
AS-IS SITUATION	The current situation at the organization of interest.
TO-BE SITUATION	The desired situation the organization of interest is striving to achieve.
FRAMEWORK GAP ANALYSIS RESULT	The results of the gap analysis where a framework is used as a tool to assess the as-is and to-be situation.
AMOUNT AT RISK	The degree to which the confidentiality, integrity, and availability of a critical asset is affected.
RISK APPETITE	"The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission" (ISACA, 2014).
RISK EVALUATION	"The process of comparing the estimated risk against given risk criteria to determine the significance of the risk" (ISACA, 2014).
RISK GAP ANALYSIS RESULT	The results of the gap analysis where a risk analysis is used as a tool to assess the as-is and to-be situation.
GAP DESCRIPTION	A description of a gap, where the actual performance does not meet the desired performance.
MEASURE	How something is solved.
BUSINESS CASE	A cost-benefit assessment, both implicit as explicit.
SCENARIO	A sequence of options.
CHOSEN SCENARIO	A scenario chosen by the management board.
DETAILED SCENARIO	A scenario which is detailed in terms of, amongst others, time and money.
EFFECT	A consequence of something.
CYBER SECURITY STRATEGY	"The direction and scope of an organization with cyber security over the long term, which achieves advantage in a changing environment through its

Concept	Description
	configuration of resources and competences with the aim of fulfilling stakeholder expectations" (Johnson et al., 2008)
ROADMAP	An implementation plan.

Concept	Description
CYBER THREAT LANDSCAPE	The threats via cyberspace an organization is facing.
POSITION OF THE ORGANIZATION	-
VALUE OF THE INFORMATION	The relative worth of information for the organization of interest.
RISK INVOLVED	-
CONSEQUENCE OF DEVELOPMENTS	The result of developments in the environment.
CONSEQUENCE OF DE-PERIMETERISATION	The result of the boundaryless cyberspace.
ORGANIZATION'S AMBITION	A certain goal or aim: something an organization wants to do or achieve with their organization.
FRAMEWORK	"The basic structure of something : a set of ideas or facts that provide support for something" http://www.merriam-webster.com/dictionary/framework
APPROACH	A methodology to handle things.
AMOUNT AT RISK PER CRITICAL ASSET	The degree to which the confidentiality, integrity, and availability of every critical asset is affected.
LIST OF RISKS	A list containing all relevant risks.
IMPLEMENTATION EFFORT	The work needed to implement the cyber security strategy.
COST	A certain amount of money needed to implement a specific measure.
RESOURCES NEEDED	The resources the organization needs for implementing the cyber security strategy.
RESIDUAL RISK	"The remaining risk after management has implemented a risk response" (ISACA, 2014).
STAFF EFFECT	The consequences the implementation of the cyber security strategy will have on the staff needed in the organization.
SKILLS EFFECT	The consequences the implementation of the cyber security strategy will have on the necessary skills needed by the staff in the organization.
KNOWLEDGE EFFECT	The consequences the implementation of the cyber security strategy will have on the necessary knowledge needed by the staff in the organization.
PROCESSES EFFECT	The consequences the implementation of the cyber security strategy will have on the business processes in the organization.
CULTURAL EFFECT	The consequences the implementation of the cyber security strategy will have on the culture in an organization.
TECHNOLOGICAL EFFECT	The consequences the implementation of the cyber security strategy will have on the use of new and emerging technologies.
ROLES & RESPONSIBILITIES EFFECT	A list defining tasks and the persons who should ensure that these tasks work out as planned.
MILESTONE	"A terminal element that marks the completion of a work package or phase " (ISACA, 2014).
LIST OF MILESTONES	A list defining all milestones.
TIME NEEDED	A list that defines how much time it will cost to implement a specific measure.
MONEY NEEDED	A list that defines how much money it will cost to implement a specific measure.
RESOURCES NEEDED	A list that defines which resources are needed in implementing the cyber security strategy.
COLLABORATION NEEDED	A list that defines which persons or organizations and tasks are necessary in implementing the cyber security strategy.
QUALITY	"A list that defines the degree of superiority of something". http://en.wikipedia.org/wiki/Quality_(business)
EFFECTIVENESS MEASURE	A measure to assess the accomplishment of desired goals.
LIST OF EFFECTIVENESS MEASURES	A list consisting of one or more effectiveness measures.

13.4.4 Plain text conceptual method

1. Identify the need for a cyber security strategy and determine the ambition

1.1. Consider a changing environment
  1.1.1. Consider the cyber threat landscape
  1.1.2. Consider the position of the organization in the marketplace
  1.1.3. Consider the value of the information and risks involved
  1.1.4. Consider developments and decreasing de-perimeterization
1.2. Consider what is already in place
1.3. Consider regulatory requirements
1.4. Determine the cyber security ambition
  1.4.1. Consider the organization's ambition
  1.4.2. Decide on and describe the cyber security ambition by connecting it to the organization's ambition
1.5. Define strategic objectives and prioritize them

2. Define the cyber security strategy project setup

2.1. Determine and invite stakeholders for requirements setting
2.2. Define the scope of the cyber security strategy
2.3. Set up definitions to use within strategy regarding cyber security

3. Analyze the landscape

3.1. Identify relevant threats and associated risks
3.2. Identify vulnerabilities and associated risks
3.3. Identify most critical assets and associated risks
3.4. Identify incidents and associated risks
3.5. Identify laws & regulation and associated risks

4. Perform a gap analysis (by using a framework or performing a risk analysis)

➔ Via a framework (A)
4.1. Define the as-is situation
  4.1.1. Choose a framework
  4.1.2. Assess the current status
  4.1.3. Benchmark assessment
  4.1.4. Describe the results
4.2. Define the to-be situation
4.3. Determine the gap
➔ Via a risk analysis (B)
4.1. Define the amount at risk (as-is)
  4.1.1. Define the amount at risk for every critical asset
  4.1.2. Consider risks found in step 3
  4.1.3. Describe total amount at risk
4.2. Define the risk appetite (to-be)
4.3. Evaluate the risks
4.4. Determine the gap

5. Define multiple scenarios

5.1. Perform a brainstorm session with stakeholders to come up with multiple measures
5.2. Define the business case for every measure
5.3. Group measures into scenario
5.4. Determine the top three potentially best scenarios
  5.4.1. Define implementation effort
  5.4.2. Define costs
  5.4.3. Define resources needed
  5.4.4. Define effects on residual risks
5.5. Let the board of directors choose one or more scenarios to elaborate on

6. Elaborate on chosen scenario

6.1. Describe the scenario in detail
6.2. Describe the effect on the organization
  6.2.1. Describe effect on the staff
  6.2.2. Describe effect on the skills
  6.2.3. Describe effect on the knowledge
  6.2.4. Describe effect on the processes
  6.2.5. Describe effect on the technologies
  6.2.6. Describe effect on the culture
  6.2.7. Describe effect on the roles and responsibilities
6.3. Describe the roadmap
  6.3.1. Define the milestones
  6.3.2. Define the time needed
  6.3.3. Define money needed
  6.3.4. Define resources needed
  6.3.5. Define quality
  6.3.6. Define the measures for effectiveness

13.5 Additional resources from the final method

13.5.1 Evidence

TABLE 23: EVIDENCE TABLE FINAL METHOD

Nr	Activity	Reference
1.	Identify the need for a cyber security strategy and determine the ambition	• Literature: 5.2, 5.4 • Interviews: all (14) • NCSS: 13.2.1, 13.2.4 (1. Strategic drivers & scope: drivers, 4. To-be situation: vision, ambition)
1.1	Consider a changing environment	• Literature: 1.1, 1.2, 4.1, 4.3, 5.1 • Interviews: 1, 7, 8, 9, 12 • NCSS: 13.2.2 (2. Analyze the cyber threat landscape: cyber trends, ICT trends)
1.1.1	Consider the emerging cyber threat landscape	• Literature: 4.2.6, 4.3 • Interviews: 1, 9, 10 • NCSS: -
1.1.2	Consider the position of the organization in the marketplace	• Literature: 6.1.1, 6.1.2, 6.1.3 • Interviews: - • NCSS: -
1.1.3	Consider the value of the information and risks involved	• Literature: • Interviews: 4, 5, 6, 7, 8 • NCSS: 13.2.2 (2. Analyze the cyber threat landscape: risks)
1.1.4	Consider developments and decreasing de-perimeterisation	• Literature: 4.1, 4.3 • Interviews: 1, 7, 8, 9, 12 • NCSS: -
1.2	Consider what strategy and controls are already in place	• Literature: - • Interviews: 3, 4, 7, 8, 9, 10, 11 • NCSS: 13.2.3 (3. As-is situation: analysis current situation)
1.3	Consider regulatory requirements	• Literature: - • Interviews: 2, 3, 4, 6, 7, 8, 9, 12 • NCSS: 13.2.1 (1. Strategic drivers & scope: compliance with laws)
1.4	Define the scope of the cyber security strategy	• Literature: - • Interviews: 11 • NCSS: 13.2.1 (1. Strategic drivers & scope: scope) • Validation: 13.3.1.2
1.5	Determine the cyber security ambition	• Literature: 2.1, 5.2 • Interviews: 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12 • NCSS: 13.2.4 (4. To-be situation: vision, ambition)

1.5.1	Consider the organization's ambition	• Literature: 5.5 • Interviews: 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12 • NCSS: 13.2.1 (1. Strategic driver & scope: relation with other strategic documents)
1.5.2	Decide on and describe the cyber security ambition by connecting it to and making it part of the organization's ambition	• Literature: 5.5 • Interviews: 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12 • NCSS: 13.2.1 (1. Strategic driver & scope: relation with other strategic documents) • Validation: 13.3.1.1
1.6	Optional: determine cyber security visions per domain the cyber security ambition applies to	• Literature: - • Interviews: - • NCSS: - • Validation: 13.3.2.1
1.7	Define guiding principles of the cyber security strategy	• Literature: - • Interviews: - • NCSS: 13.2.4 (4. To-be situation: guiding principles, strategy guidelines) • Validation: 13.3.2.7
1.8	Define desired outcomes of the cyber security strategy	• Literature: - • Interviews: - • NCSS: • Validation: 13.3.1.1, 13.3.1.2
2.	Define CSS operating setup	• Literature: - • Interviews: - • NCSS: 13.2.1 (1. Strategic drivers & scope) • Validation: 8.1, 8.3
2.1	Determine and invite stakeholders for requirements setting	• Literature: - • Interviews: All (14) • NCSS: 13.2.1 (1. Strategic drivers & scope: stakeholders)
2.2	Set up definitions to use within the cyber security strategy regarding cyber security	• Literature: - • Interviews: - • NCSS: 13.2.1 (1. Strategic drivers & scope: definition cyber security, glossary) • Validation: 8.1
2.3	Define the governance of the cyber security strategy	• Literature: - • Interviews: 5, 7, 10 • NCSS: - • Validation: 8.1, 13.3.1.1
2.4	Define strategy dependencies	• Literature: - • Interviews: 5 • NCSS: 13.2.1 (1. Strategic drivers & scope: relation with other strategic documents, relation with previous strategies) • Validation: 8.1, 13.3.1.1
2.5	Describe desired interaction with key stakeholders	• Literature: - • Interviews: 5 • NCSS: - • Validation: 8.1, 13.3.1.1
3.	Analyze the current situation	• Literature: 6.1, 6.2, 6.3 • Interviews: 9 • NCSS: 13.2.2 (2. Analyze cyber threat landscape) • Validation: 8.1, 13.3.1
3.1	Analyze the social, external and internal landscape	• Literature: 6.1 • Interviews: - • NCSS: 13.2.2 (2. Analyze cyber threat landscape) • Validation: 8.1
3.1.1	Identify relevant threats	• Literature: 4.2.6, 6.1.1.5 • Interviews: all (14) • NCSS: 13.2.2 (2. Analyze cyber threat landscape: threats)
3.1.2	Identify vulnerabilities and associated risks	• Literature: 4.2.4 • Interviews: 4, 10, 11, 12

		• NCSS: -
3.1.3	Identify most critical assets and associated risks	• Literature: 4.2.2 • Interviews: 4, 10, 11, 12 • NCSS: 13.2.3 (3. As-is situation)
3.1.4	Identify incidents and associated risks	• Literature: - • Interviews: 2, 3, 4, 5, 7, 8, 10, 12 • NCSS: -
3.1.5	Identify requirements	• Literature: 6.1.1.4, 6.1.3 • Interviews: 2, 3, 4, 6, 7, 8, 9, 12 • NCSS: 13.2.1 (1. Strategic drivers & scope: compliance with laws) • Validation: 8.1, 13.3.2.1
3.1.5.1	Identify external laws and regulations	• Literature: 6.1.1.4, 6.1.3 • Interviews: 2, 3, 4, 6, 7, 8, 9, 12 • NCSS: 13.2.1 (1. Strategic drivers & scope: compliance with laws) • Validation: 13.3.2.1
3.1.5.2	Identify internal laws and regulations	• Literature: 6.1.1.4, 6.1.3 • Interviews: 2, 3, 4, 6, 7, 8, 9, 12 • NCSS: 13.2.1 (1. Strategic drivers & scope: compliance with laws) • Validation: 13.3.2.1
3.1.6	Identify running activities related to cyber security	• Literature: - • Interviews: - • NCSS: - • Validation: 8.2, 13.3.2.4, 13.3.2.7
3.1.7	Identify the internal culture	• Literature: 6.1.1.2, 6.1.2, 6.1.3 • Interviews: 13, 14 • NCSS: - • Validation: 8.2, 13.3.2.6
3.2	Evaluate landscape analysis with stakeholders and adjust if necessary	• Literature: - • Interviews: - • NCSS: - • Validation: 8.2
3.3	Perform a gap analysis	• Literature: - • Interviews: 6, 7, 11, 12 • NCSS: 13.2.3 (3. To-be situation)
3.3.1A	Define the as-is situation	• Literature: - • Interviews: 3, 4, 7, 8, 9, 11 • NCSS: 13.2.3 (3. To-be situation: maturity analysis, SWOT analysis, analysis current situation)
3.3.1.1A	Choose a framework	• Literature: - • Interviews: 1, 2, 4, 5, 6, 7, 8, 9, 10, 11 • NCSS: -
3.1.1.2A	Assess the current status	• Literature: - • Interviews:1, 2, 4, 5, 6, 7, 8, 9, 10, 11 • NCSS: 13.2.3 (3. To-be situation: maturity analysis, SWOT analysis, analysis current situation)
3.1.1.3A	Optional: benchmark assessment	• Literature: - • Interviews: 14 • NCSS: 13.2.3 (3. As-is situation: comparison with other countries)
3.1.1.4A	Describe the results	• Literature: - • Interviews: - • NCSS: -
3.3.2A	Define the to-be situation	• Literature: • Interviews: • NCSS: 13.2.4 (4. To-be situation)
3.3.3A	Optional: determine cyber security visions per framework domain the cyber security ambition applies to	• Literature: - • Interviews: - • NCSS: - • Validation: 13.3.2.1

3.3.4B	Define the amount at risk (as-is)	• Literature: 4.2.5 • Interviews: 1, 2, 3, 4, 6, 7, 8, 10, 11, 12 • NCSS: -
3.3.4.1B	Define the amount at risk for every critical asset	• Literature: - • Interviews: 6 • NCSS:
3.3.4.2B	Describe total amount at risk	• Literature: - • Interviews: - • NCSS: -
3.3.5B	Define risk appetite (to-be)	• Literature: 4.2.5 • Interviews: 1, 2, 3, 4, 6, 7, 8 • NCSS: -
3.3.6B	Evaluate the risks	• Literature: 4.2.5? • Interviews: - • NCSS: -
3.4	Determine and prioritize the gaps	• Literature: • Interviews: 6, 7, 11, 12 • NCSS:
3.5	Evaluate gap analysis with stakeholders and adjust if necessary	• Literature: - • Interviews: - • NCSS: - • Validation: 8.1, 8.2
3.6	Define problem areas based on the landscape and gaps found	• Literature: • Interviews: • NCSS: • Validation: 8.1 (+ logic)
4.	Describe multiple strategic objectives and associated activities	• Literature: 5 • Interviews: - • NCSS: 13.2.4 (4. To-be situation: strategic objectives, strategic priorities) • Validation: 8.1, 13.3.1
4.1	Perform a brainstorm session with stakeholders to communicate problem areas and decide on multiple strategic objectives	• Literature: - • Interviews: 7 • NCSS: 13.2.5 (5. Countermeasures: action) • Validation: 8.1, 13.3.1
4.2	Evaluate results of brainstorm session and adjust if necessary	• Literature: - • Interviews: - • NCSS: - • Validation: 8.2
4.3	Determine high-level activities and associated options for every strategic objective	• Literature: - • Interviews: • NCSS: 13.2.5 (5. Countermeasures: action) • Validation: 8.1, 8.2
4.4	Define the business case for every activity	• Literature: - • Interviews: 1, 9, 14 • NCSS: - • Validation: 8.2, 13.3.2.6
4.5	Elaborate on the high-level activities	• Literature: • Interviews: 4, 6, 7, 9, 11, 12 • NCSS: 13.2.5 (5. Countermeasures: action plan) • Validation: 8.1
4.5.1	Define the milestones	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: important milestones and CSF)
4.5.2	Define time needed	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action timeframe)
4.5.3	Define money needed	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action plan)

4.5.4	Define resources needed	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action plan)
4.5.5	Define the collaboration needed	• Literature: - • Interviews: - • NCSS: 13.2.5 (6. Implementation: cooperation)
4.5.6	Describe effect on the responsibilities	• Literature: - • Interviews: - • NCSS: 13.2.5 (5. Countermeasures: action stakeholders, roles and responsibilities government, roles and responsibilities stakeholders)
4.5.7	Define the measures for effectiveness and intermediary goals	• Literature: - • Interviews: - • NCSS: 13.2.6 (6. Implementation: assessment of effectiveness, expected effects, effectiveness of actions, effectiveness measures)
4.6	Prioritize strategic objectives with stakeholders	• Literature: - • Interviews: - • NCSS: 13.2.4 (4. To-be situation: strategic priorities)
4.7	Let management board choose the ultimate course of action	• Literature: - • Interviews: - • NCSS: - (+ logic)
4.8	Describe the effect of the strategy on the organization	• Literature: - • Interviews: - • NCSS: 13.2.6 (6. Implementation: consequences, organization)
4.8.1	Describe the effect on the staff	• Literature: 6.1.1.2 • Interviews: - • NCSS: 13.2.6 (6. Implementation: consequences, organization)
4.8.2	Describe the effect on the skills	• Literature: 6.1.1.2 • Interviews: - • NCSS: 13.2.6 (6. Implementation: consequences, organization)
4.8.3	Describe the effect on the knowledge	• Literature: • Interviews: - • NCSS: 13.2.6 (6. Implementation: consequences, organization)
4.8.4	Describe the effect on the processes	• Literature: 6.1.1.2 • Interviews: 10, 14 • NCSS: -
4.8.5	Describe the effect on the technologies	• Literature: 6.1.1.4 • Interviews: 10, 14 • NCSS: -
4.8.6	Describe effect on the responsibilities	• Literature: 6.1.1.2, 6.1.2, 6.1.3 • Interviews: 13, 14 • NCSS: - • Validation: 8.2

13.5.2 Activity tables

TABLE 24: ACTIVITY TABLE FINAL METHOD

Activity	Sub activity	Description	Role
Identify the need for a cyber security strategy and determine the ambition	Consider a changing environment	The management board considers the ENVIRONMENT on a high-level, which might be part of the NEED FOR A CYBER SECURITY STRATEGY. The elements to be assessed in the ENVIRONMENT can be SOCIAL, EXTERNAL, and/or INTERNAL.	Management board
	Consider what strategy and	The management board considers the CURRENT SITUATION on a high-level,	Management board

Activity	Sub activity	Description	Role
	controls are already in place	which might be part of the NEED FOR A CYBER SECURITY STRATEGY.	
	Consider regulatory requirements	The management board considers the LAWS & REGULATIONS on a high-level, which might be part of the NEED FOR A CYBER SECURITY STRATEGY.	Management board
	Define the scope of the cyber security strategy	The steering committee will decide on the SCOPE for the CYBER SECURITY STRATEGY by determining SCOPING REQUIREMENTS.	Management board
	Determine the cyber security ambition	If there is a NEED FOR A CYBER SECURITY STRATEGY, the management board will need to determine a CYBER SECURITY AMBITION.	Management board
	Optional: determine cyber security visions per domain the cyber security ambition applies to	Based on the CYBER SECURITY AMBITION, the management board defines one or more SUB VISIONS dependent on whether there are different domains visible to which the CYBER SECURITY AMBITION applies. Every SUB VISION is stored in a LIST OF SUB VISIONS	Management board
	Define guiding principles of the cyber security strategy	The management board defines one or more GUIDING PRINCIPLES and stores this in a LIST OF GUIDING PRINCIPLES.	Management board
	Define desired outcomes of the cyber security strategy	The management defines DESIRED OUTCOMES of the cyber security strategy. These are stored in a LIST OF DESIRED OUTCOMES.	Management board
Determine the scope and stakeholders / Define CSS project setup	Determine and invite stakeholders for requirements setting	The steering committee will determine and invite every STAKEHOLDER, INTERNAL or EXTERNAL, for the upcoming activities. A STAKEHOLDER is stored in a LIST OF STAKEHOLDERS which can be used later on.	Steering committee
	Set up definitions to use within the cyber security strategy regarding cyber security	The steering committee will set up DEFINITIONS to use within the CYBER SECURITY STRATEGY. Every DEFINITION is stored in a LIST OF CYBER SECURITY DEFINITIONS.	Steering committee
	Define the governance of the cyber security strategy	The steering committee defines GOVERNANCE structures by identifying who is responsible for, accountable for, consulted, and informed by the strategy.	Steering committee
	Define strategy dependencies	STRATEGY DEPENDENCIES are defined by the steering committee and stored in a LIST OF STRATEGY DEPENDENCIES.	Steering committee
	Describe desired interaction with key stakeholders	The steering committee describes the DESIRED INTERACTION expected from and with key stakeholders.	Steering committee
Analyze the current situation	Analyze the social, external, and internal landscape	A LANDSCAPE overview is created by analyzing the social, external, and internal landscape by the steering committee by interviewing stakeholders.	Steering committee, stakeholders
	Evaluate landscape analysis with stakeholders and adjust if necessary	The results from the internal and social LANDSCAPE analysis are evaluated with stakeholders and adjusted if necessary. These LANDSCAPE EVALUATION RESULTS are stored in a LIST OF LANDSCAPE EVALUATION RESULTS.	Steering committee, stakeholders
	Perform a gap analysis	A gap analysis is performed by the steering committee, with help of stakeholders. This results in a GAP ANALYSIS.	Steering committee, stakeholders
	Determine and prioritize gaps	The steering committee uses the GAP ANALYSIS to determine one or more	Steering committee, stakeholders

Activity	Sub activity	Description	Role
		GAPS and stores these in a LIST OF GAPS. The LIST OF GAPS is used to prioritize the gaps together with the stakeholders.	
	Evaluate gap analysis with stakeholders and adjust if necessary	The GAP ANALYSIS together with the LIST OF GAPS are evaluated with stakeholders and adjusted if necessary. These GAP EVALUATION RESULTS are stored in a LIST OF GAP EVALUATION RESULTS.	Steering committee, stakeholders
	Define problem areas based on the landscape and gaps found	Based on the LANDSCAPE ANALYSIS RESULT and the GAP ANALYSIS RESULT, the steering committee defines one or more PROBLEM AREAS which are then stored in a LIST OF PROBLEM AREAS.	Steering committee
Describe multiple strategic objectives and associated activities	Perform a brainstorm session with stakeholders to communicate problem areas and decide on multiple strategic objectives	The steering committee performs one or more brainstorm sessions with stakeholders to communicate the LIST OF PROBLEM AREAS and decides on one or more STRATEGIC OBJECTIVES. Every STRATEGIC OBJECTIVE is stored in a LIST OF STRATEGIC OBJECTIVES.	Steering committee, stakeholders
	Evaluate results of brainstorm session(s) and adjust if necessary	The steering committee evaluates the LIST OF STRATEGIC OBJECTIVES with the stakeholders and adjusts these if necessary. The EVALUATION RESULTS are stored in a LIST OF EVALUATED STRATEGIC OBJECTIVES.	Steering committee, stakeholders
	Determine high-level activities and associated options for every strategic objective	Based on the LIST OF EVALUATED STRATEGIC OBJECTIVES, the steering committee determines one or more HIGH-LEVEL ACTIVITIES per STRATEGIC OBJECTIVE.	Steering committee
	Define the business case for every strategic objective	The steering committee defines the BUSINESS CASE for every STRATEGIC OBJECTIVE as found in the LIST OF EVALUATED STRATEGIC OBJECTIVES.	Steering committee
	Elaborate on the high-level activities	The steering committee elaborates on the HIGH-LEVEL ACTIVITIES and stores these DETAILED HIGH-LEVEL ACTIVITIES in a DETAILED LIST OF HIGH-LEVEL ACTIVITIES.	Steering committee
	Prioritize strategic objectives with stakeholders	The steering committee, together with stakeholders, prioritizes the STRATEGIC OBJECTIVES, as found in the EVALUATED LIST OF STRATEGIC OBJECTIVES, and with the use of the associated LIST OF BUSINESS CASES and DETAILED LIST OF HIGH-LEVEL ACTIVIES.	Steering committee, stakeholders
	Let the management board choose the ultimate course of action	The management board will make a decision about the ultimate course of action, being the to-follow STRATEGIC OBJECTIVES and associated HIGH-LEVEL ACTIVITIES. Based on the DECISION, DETAILED LIST OF HIGH-LEVEL ACTIVITIES, EVALUATED LIST OF STRATEGIC OBJECTIVES, CURRENT SITUATION ANALYSIS RESULT, CSS OPERATING SETUP, CYBER SECURITY AMBITION and the NEED FOR CYBER SECURITY	Management board

Activity	Sub activity	Description	Role
		STRATEGY provide input for the CYBER SECURITY STRATEGY.	
	Describe the effect on the organization	Based on the CYBER SECURITY STRATEGY, the steering committee describes the EFFECT on the organization.	Steering committee

Sub activity	Sub sub activity	Description	Role
Consider a changing environment	Consider the emerging cyber threat landscape	The management board may consider the CYBER THREAT LANDSCAPE as part of the ENVIRONMENT description.	Management board
	Consider the position of the organization in the marketplace	The management board may consider the POSITION OF THE ORGANIZATION in the marketplace as part of the ENVIRONMENT description.	Management board
	Consider the value of the information and risks involved	The management board may consider the VALUE OF THE INFORMATION and the RISKS INVOLVED as part of the ENVIRONMENT description.	Management board
	Consider developments and decreasing de-perimeterization	The management board may consider the CONSEQUENCE OF DEVELOPMENTS and the CONSEQUENCE OF DE-ERIMETERISATION as part of the ENVIRONMENT description.	Management board
Determine the ambition	Identify the organization's ambition	The steering committee identifies the ORGANIZATION'S AMBITION.	Steering committee
	Decide on and describe the cyber security ambition by connecting it to and making it part of the organization's strategy	The steering committee decides on and describes the CYBER SECURITY AMBITION based on the ORGANIZATION'S AMBITION.	Steering committee
Analyze the internal and social landscape	Identify relevant threats	The steering committee, together with the stakeholders, identifies relevant THREATS. Zero or more THREATS are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify vulnerabilities	The steering committee, together with the stakeholders, identifies relevant VULNERABILITIES. Zero or more VULNERABILITIES are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify most critical assets	The steering committee, together with the stakeholders, identifies relevant CRITICAL ASSETS. Zero or more CRITICAL ASSETS are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify incidents	The steering committee, together with the stakeholders, identifies relevant INCIDENTS. Zero or more INCIDENTS are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify requirements	The steering committee, together with the stakeholders, identifies relevant REQUIREMENTS, relating to internal and external laws & regulation. Zero or more REQUIREMENTS are stored in a LANDSCAPE description.	Steering committee, stakeholders
	Identify running activities related to cyber security	The steering committee, together with the stakeholders, identifies RUNNING PROJECTS related to cyber security. Zero or more RUNNING PROJECTS are stored in a LANDSCAPE description.	Steering committee, stakeholders

Sub activity	Sub sub activity	Description	Role
	Identify the internal culture	The steering committee, together with the stakeholders, identifies the INTERNAL culture. Zero or one INTERNAL CULTURE is stored in a LANDSCAPE description.	Steering committee, stakeholders
Perform a gap analysis	Define the as-is situation (via a framework)	The steering committee, together with the stakeholders, will define the AS-IS SITUATION by using a framework of choice as a reference.	Steering committee, stakeholders
	Choose a framework	The steering committee chooses a cyber security FRAMEWORK to assess the AS-IS SITUATION.	Steering committee
	Assess the current status	The steering committee uses the cyber security FRAMEWORK to assess the STATUS of the AS-IS SITUATION.	Steering committee
	Optional: benchmark assessment	The steering committee BENCHMARKS the STATUS against the status of likewise organizations.	Steering committee
	Describe the results	The steering committee describes the results of analyzing the AS-IS SITUATION with a FRAMEWORK.	Steering committee
	Define the to-be situation (via a framework)	The steering committee, together with the stakeholders, will define the TO-BE SITUATION by using a framework of choice as a reference.	Steering committee, stakeholders
	Optional: determine cyber security visions per framework domain the cyber security ambition applies to	Based on the FRAMEWORK, the steering committee defines one or more SUB VISIONS dependent on whether there are different domains visible to which the CYBER SECURITY AMBITION applies. Every SUB VISION is stored in a LIST OF SUB VISIONS	Steering committee
	Define the amount at risk (via risk analysis)	The steering committee, together with the stakeholders, will define the AMOUNT AT RISK for every critical asset by using a risk analysis approach.	Steering committee, stakeholders
	Define the amount at risk for every critical asset	The steering committee defines the AMOUNT AT RISK PER CRITICAL ASSET. These are stored in a LIST OF RISKS.	Steering committee
	Describe the total amount at risk	The steering committee describes the total amount at risk as the RISK AS-IS SITUATION.	Steering committee
	Define the risk appetite (via risk analysis)	The steering committee, together with the stakeholders, will define the RISK APPETITE by considering the RISKS found in the previous step using a risk analysis approach.	Steering committee, stakeholders
	Evaluate the risks (via risk analysis)	The steering committee, together with the stakeholders, will evaluate the risks (RISK EVALUATION).	Steering committee, stakeholders
Elaborate on the high-level activities	Define the milestones	The steering committee defines the MILESTONES for every HIGH-LEVEL ACTIVITY. Every MILESTONE is stored in a LIST OF MILESTONES.	Steering committee
	Define the time needed	The steering committee defines the TIME NEEDED for every HIGH-LEVEL ACTIVITY.	Steering committee
	Define the money needed	The steering committee defines the MONEY NEEDED for every HIGH-LEVEL ACTIVITY.	Steering committee
	Define the resources needed	The steering committee defines the RESOURCES NEEDED for every HIGH-LEVEL ACTIVITY. Every RESOURCE NEEDED is stored in a LIST OF RESOURCES NEEDED.	Steering committee

Sub activity	Sub sub activity	Description	Role
	Define the collaboration needed	The steering committee defines the COLLABORATION NEEDED for every HIGH-LEVEL ACTIVITY. Every COLLABORATION NEEDED is stored in a LIST OF COLLABORATIONS NEEDED.	Steering committee
	Define the measures for effectiveness and intermediary goals	The steering committee defines the necessary EFFECTIVENESS MEASURES to be achieved for the different projects for every HIGH-LEVEL ACTIVITY, as well as INTERMEDIARY GOALS. Every EFFECTIVENESS MEASURE is stored in a LIST OF EFFECTIVENESS MEASURES.	Steering committee
Describe the effect on the organization	Describe effect on the staff	The steering committee describes the EFFECT on the STAFF when the CYBER SECURITY STRATGY is implemented.	Steering committee
	Describe effect on the skills	The steering committee describes the EFFECT on the SKILLS of the staff when the CYBER SECURITY STRATEGY is implemented.	Steering committee
	Describe effect on the knowledge	The steering committee describes the EFFECT on the KNOWLEDGE of the staff when the CYBER SECURITY STRATEGY is implemented.	Steering committee
	Describe effect on the processes	The steering committee describes the EFFECT on the PROCESSES when the CYBER SECURITY STRATEGY is implemented.	Steering committee
	Describe effect on the technologies	The steering committee describes the EFFECT on the TECHNOLOGIES when the CYBER SECURITY STRATEGY is implemented.	Steering committee
	Describe effect on the culture	The steering committee describes the EFFECT on the CULTURE when the CYBER SECURITY STRATEGY is implemented.	Steering committee
	Describe effect on the responsibilities	The steering committee describes the CYBER SECURITY STRATEGY is implemented.	Steering committee

13.5.3 Concept tables

TABLE 25: CONCEPT TABLE FINAL METHOD

Concept	Description
ENVIRONMENT	The internal and external surroundings of the organization of interest.
CURRENT SITUATION	The present status of how cyber security is arranged at the organization of interest.
LAWS & REGULATIONS	(a system of) Rules that must be followed, induced by an authority.
NEED FOR A CYBER SECURITY STRATEGY	The rationale of having a cyber security strategy.
SCOPING REQUIREMENT	A requirement about the boundaries of the cyber security project.
LIST OF SCOPING REQUIREMENTS	A lists containing all scoping requirements.
CYBER SECURITY AMBITION	“A certain goal or aim: something an organization wants to do or achieve with cyber security”. http://www.merriam-webster.com/dictionary/ambition
SUB VISION	A vision, goal for the future, for a specific domain or category.
LIST OF SUB VISIONS	A list containing all sub visions.
GUIDING PRINCIPLE	Principles that need to be followed in order to achieve what is aimed for.
LIST OF GUIDING PRINCIPLES	A list containing all guiding principles.
DESIRED OUTCOME	A result that is wished for from someone or something.
LIST OF DESIRED OUTCOMES	A list containing all desired outcomes.

Concept	Description
STAKEHOLDER	“People or small groups with the power to respond to, negotiate with, and change the strategic future of the organization” (Eden & Ackermann, 1998, p. 117).
INTERNAL STAKEHOLDER	A stakeholder who resides within the organization of interest.
EXTERNAL STAKEHOLDER	A stakeholder who resides outside the organization of interest.
LIST OF STAKEHOLDERS	A list containing information about one or more stakeholders.
DEFINITION	A formal statement of the explanation of a concept.
LIST OF CYBER SECURITY DEFINITIONS	A list containing one or more definitions related to the field of cyber security.
GOVERNANCE	“All processes of governing, whether undertaken by a government, market, or network, whether over a family, tribe, formal or informal organization, or territory, and whether through laws, norms, power, or language” (Bevir, 2012).
STRATEGY DEPENDENCY	People, processes, or technologies dependent on the strategy.
LIST OF STRATEGY DEPENDENCIES	A list containing all strategy dependencies.
DESIRED INTERACTION	Interactions with stakeholders that are wished for to successfully achieve something.
LIST OF DESIRED INTERACTIONS	A list containing all desired interactions.
CSS PROJECT SETUP	A document containing information about the stakeholders, scope, and cyber security definitions.
LANDSCAPE	The aspects of the cyberspace influencing the organization of interest.
LANDSCAPE EVALUATION RESULTS	Result, and potential adjustment, of the evaluation session with stakeholders.
LIST OF LANDSCAPE EVALUATION RESULTS	A list containing all results of the landscape evaluation session with stakeholders.
LANDSCAPE ANALYSIS RESULT	An updated landscape overview based on the landscape analysis and the evaluation results.
GAP ANALYSIS	The results of the gap analysis.
GAP	A description of a gap, where the actual performance does not meet the desired performance.
LIST OF (PRIORITIZED) GAPS	A list containing all gaps and a prioritization for every gap.
GAP EVALUATION RESULT	A statement about the found gaps by a stakeholder.
LIST OF GAP EVALUATION RESULTS	A list that contains all results from the gap analysis evaluation.
GAP ANALYSIS RESULT	The results of the gap analysis.
PROBLEM AREA	“A place that is prone to a particular problem or danger” http://www.collinsdictionary.com/dictionary/english/problem-area
LIST OF PROBLEM AREAS	A list containing all problem areas.
STRATEGIC OBJECTIVE	“A broadly defined, measurable objective that an organization must achieve to make its strategy succeed” http://www.businessdictionary.com/definition/strategic-objective.html
LIST OF STRATEGIC OBJECTIVES	A list containing all strategic objectives.
EVALUATED LIST OF STRATEGIC OBJECTIVES	A list of strategic objectives that are validated by stakeholders.
BUSINESS CASE	A cost-benefit assessment, both implicit as explicit.
LIST OF BUSINESS CASES	A list containing all business cases per strategic objective.
HIGH-LEVEL ACTIVITY	A generic task.
LIST OF HIGH-LEVEL ACTIVITIES	A list that contains all high-level activities.
DETAILED HIGH-LEVEL ACTIVITY	An activity that is described in detail on specific subjects.
DETAILED LIST OF HIGH-LEVEL ACTIVITIES	A list containing a detailed activities.
PRIORITIZED LIST OF STRATEGIC OBJECTIVES	A list that contains all activities, and information about these activities, and are given a prioritization.
DECISION	A statement that either confirms or denies the information in the proposed cyber security strategy.
CYBER SECURITY STRATEGY	“The direction and scope of an organization with cyber security over the long term, which achieves advantage in a changing environment through its

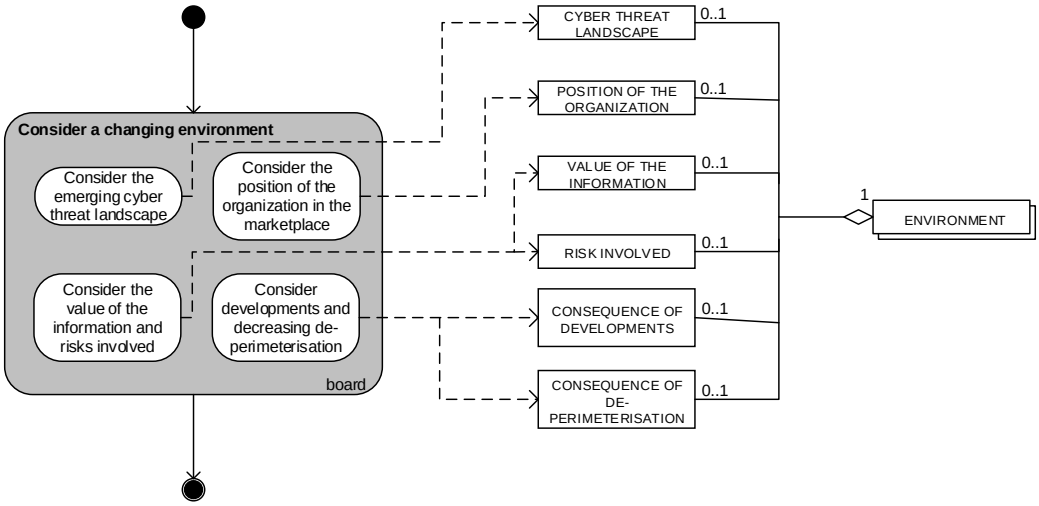
Concept	Description
	configuration of resources and competences with the aim of fulfilling stakeholder expectations" (Johnson et al., 2008)
EFFECT	A consequence of something.

Sub Concept	Description
CYBER THREAT LANDSCAPE	The threats via cyberspace an organization is facing.
POSITION OF THE ORGANIZATION	-
VALUE OF THE INFORMATION	The relative worth of information for the organization of interest.
RISK INVOLVED	-
CONSEQUENCE OF DEVELOPMENTS	The result of developments in the environment.
CONSEQUENCE OF DE-PERIMETERISATION	The result of the boundaryless cyberspace.
ORGANIZATION'S AMBITION	"A certain goal or aim: something an organization wants to do or achieve with their organization". http://www.merriam-webster.com/dictionary/ambition
THREAT	"Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service" (NIST, 2012).
CRITICAL ASSET	"Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances, and reputation" (ISACA, 2014)
VULNERABILITY	"A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events" (ISACA, 2014)
INCIDENT	"Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service" (ISACA, 2014).
INTERNAL CULTURE	
RUNNING ACTIVITY	A task or project that is currently performed with regard to cyber security.
REQUIREMENT	(a system of) Rules that must be followed, induced by an authority.
INTERNAL LAWS & REGULATION	(a system of) Rules that must be followed, induced by an internal authority.
EXTERNAL LAWS & REGULATIONS	(a system of) Rules that must be followed, induced by an external authority.
AS-IS SITUATION	The current situation at the organization of interest.
TO-BE SITUATION	The desired situation the organization of interest is striving to achieve.
FRAMEWORK GAP ANALYSIS RESULT	The results of the gap analysis where a framework is used as a tool to assess the as-is and to-be situation.
AMOUNT AT RISK	The degree to which the confidentiality, integrity, and availability of a critical asset is affected.
RISK APPETITE	"The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission" (ISACA, 2014).
RISK EVALUATION	"The process of comparing the estimated risk against given risk criteria to determine the significance of the risk" (ISACA, 2014).
RISK GAP ANALYSIS RESULT	The results of the gap analysis where a risk analysis is used as a tool to assess the as-is and to-be situation.
GAP DESCRIPTION	A description of a gap, where the actual performance does not meet the desired performance.
FRAMEWORK	"The basic structure of something : a set of ideas or facts that provide support for something" http://www.merriam-webster.com/dictionary/framework
RESULT	A methodology to handle things.
BENCHMARK	A comparison of the results against the results on the same subject from peers in the industry.
AMOUNT AT RISK PER CRITICAL ASSET	The degree to which the confidentiality, integrity, and availability of every critical asset is affected.
LIST OF RISKS	A list containing all relevant r
STAFF EFFECT	The consequences the implementation of the cyber security strategy will have on the staff needed in the organization.

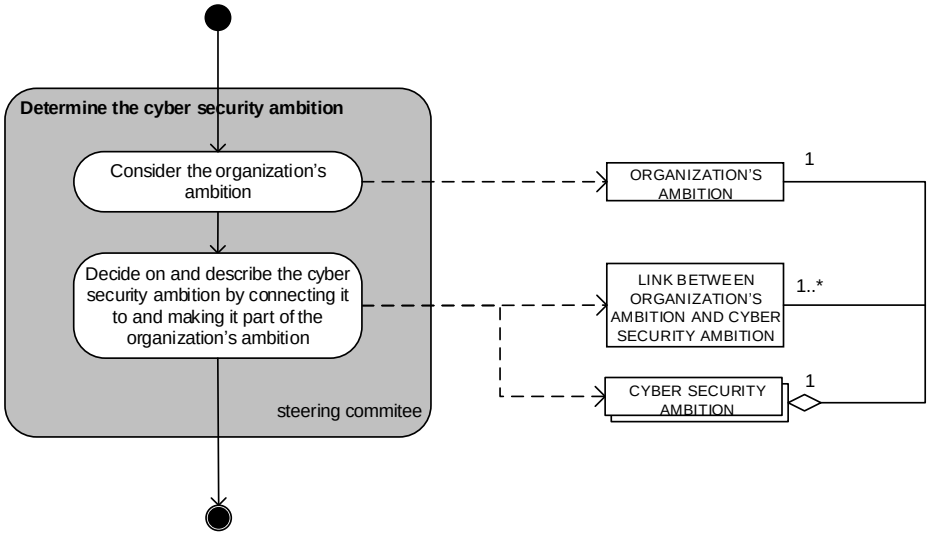
SKILLS EFFECT	The consequences the implementation of the cyber security strategy will have on the necessary skills needed by the staff in the organization.
KNOWLEDGE EFFECT	The consequences the implementation of the cyber security strategy will have on the necessary knowledge needed by the staff in the organization.
PROCESSES EFFECT	The consequences the implementation of the cyber security strategy will have on the business processes in the organization.
RESPONSIBILITIES EFFECT	A list defining tasks and the persons who should ensure that these tasks work out as planned.
TECHNOLOGICAL EFFECT	The consequences the implementation of the cyber security strategy will have on the use of new and emerging technologies.
MILESTONE	“A terminal element that marks the completion of a work package or phase “ (ISACA, 2014).
TIME NEEDED	A list that defines how much time it will cost to implement a specific measure.
MONEY NEEDED	A list that defines how much money it will cost to implement a specific measure.
RESOURCES NEEDED	A list that defines which resources are needed in implementing the cyber security strategy.
COLLABORATION NEEDED	A list that defines which persons or organizations and tasks are necessary in implementing the cyber security strategy.
RESPONSIBILITIY	“Something that you should do because it is morally right, legally required, etc.” http://www.merriam-webster.com/dictionary/responsibility
EFFECTIVENESS MEASURE	A measure to assess the accomplishment of desired goals.

13.5.4 Sub process deliverable diagrams final method

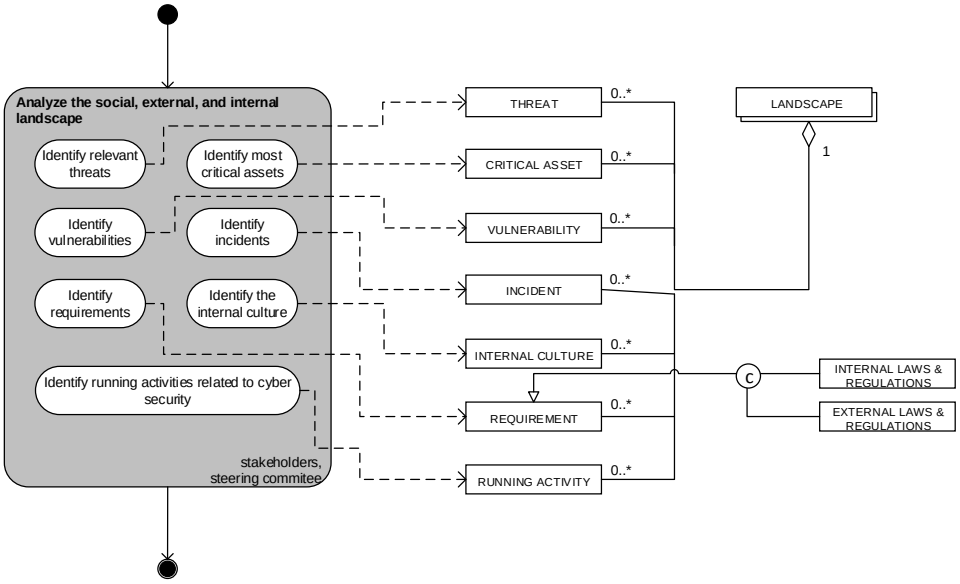
Consider a changing environment



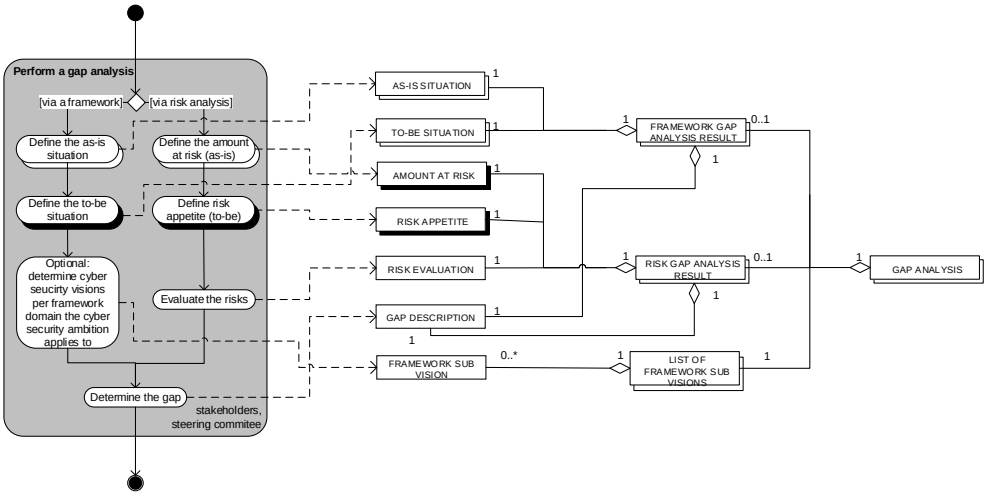
Determine the cyber security ambition



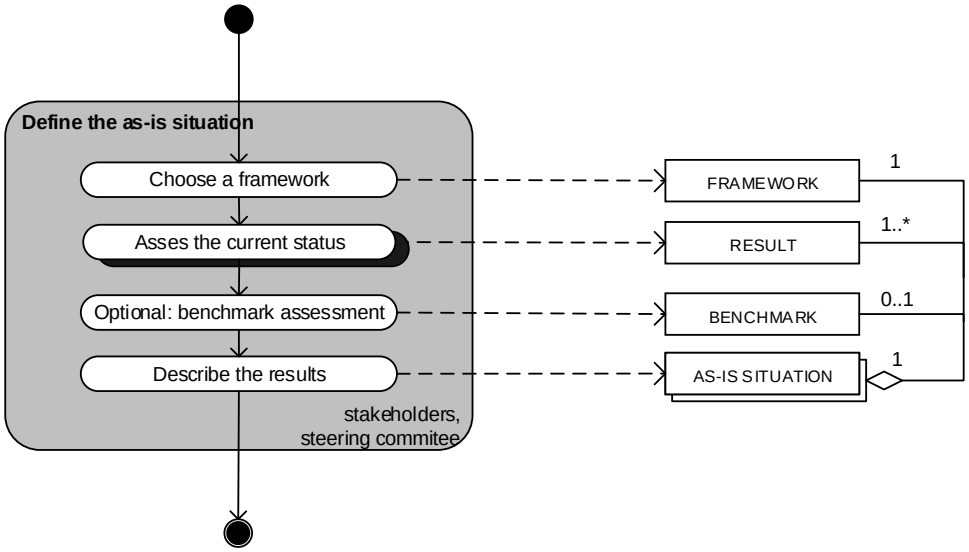
Analyze the social, external, and internal landscape



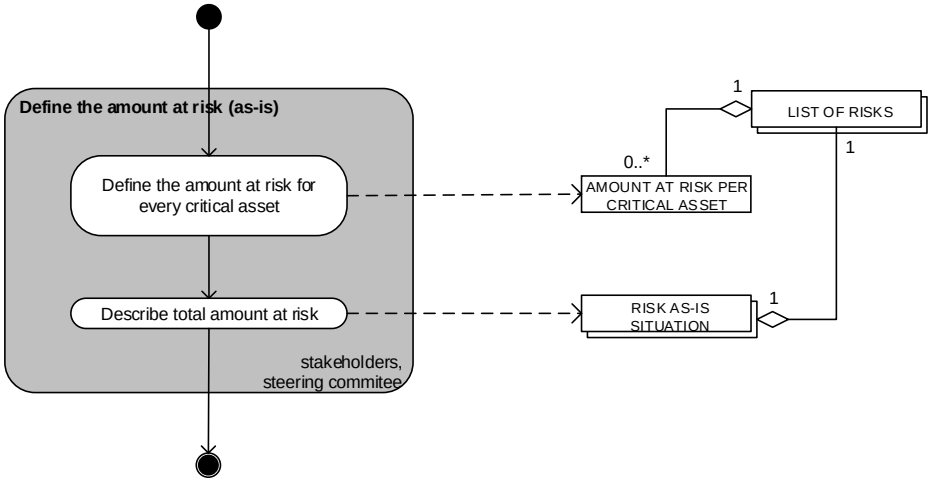
Perform a gap analysis



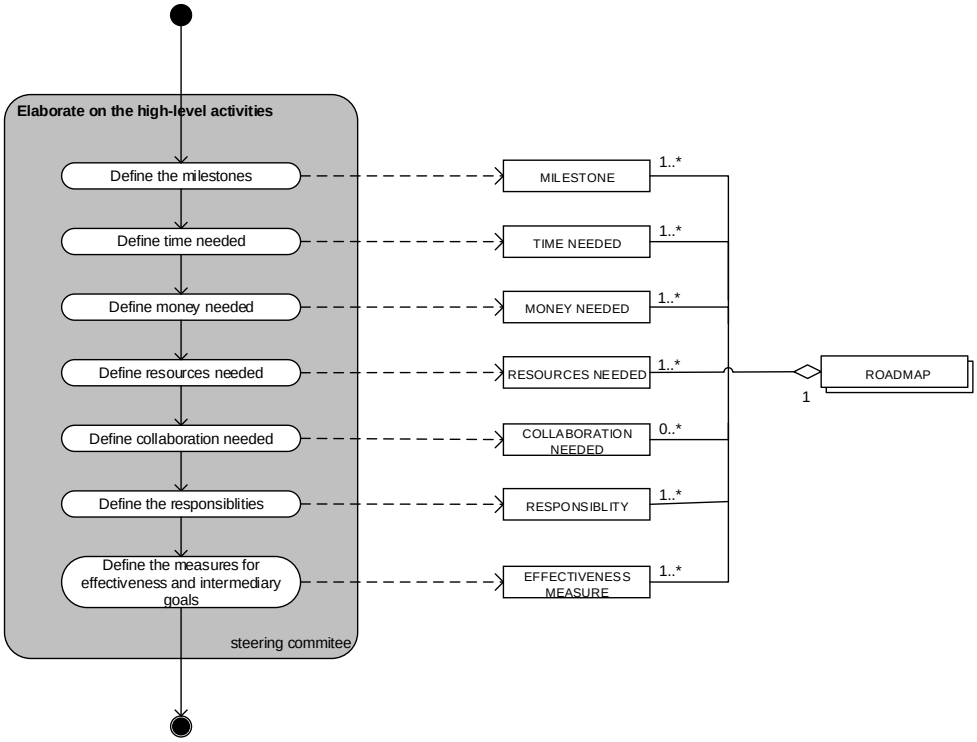
Define the as-is situation



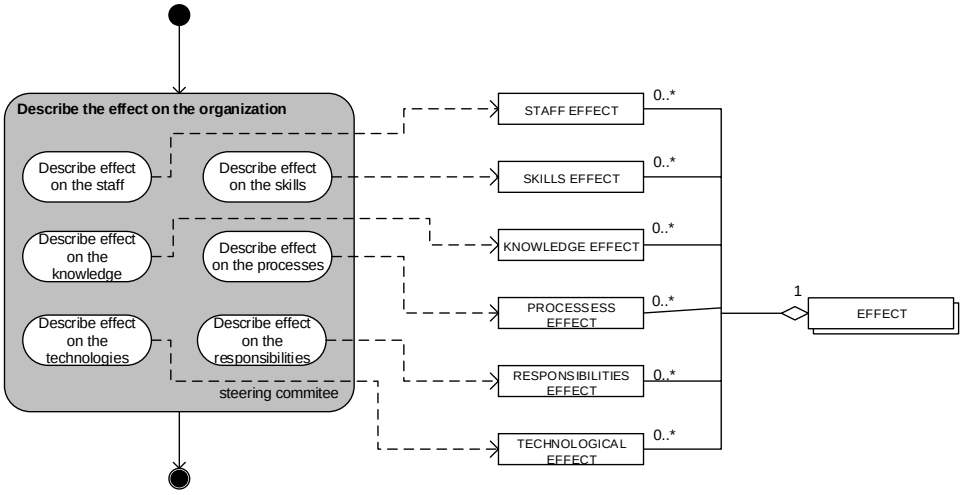
Define the amount at risk



Elaborate on high-level activities



Describe the effect of the strategy on the organization



13.5.5 Plain text final method

1. Identify the need for a cyber security strategy and determine the ambition

1.1. Consider a changing environment
  1.1.1. Consider the emerging cyber threat landscape
  1.1.2. Consider the position of the organization in the marketplace
  1.1.3. Consider the value of the information and risks involved
  1.1.4. Consider developments and decreasing de-perimeterization
1.2. Consider what strategy and control are already in place
1.3. Consider regulatory requirements
  If there is a need, continue. If not, stop.
1.4. Define the scope of the cyber security strategy
1.5. Determine the cyber security ambition
  1.5.1. Identify the organization's ambition

1.5.2. Decide on and describe the cyber security ambition by connecting it to and making it part of the organization's strategy
1.6. Optional: determine cyber security visions per domain the cyber security ambition applies to
1.7. Define guiding principles of the cyber security strategy
1.8. Define desired outcomes of the cyber security strategy

2. Define the cyber security strategy operating setup

2.1. Determine and invite stakeholders for requirements setting
2.2. Set up definitions to use within the cyber security strategy regarding cyber security
2.3. Define the governance of the cyber security strategy
2.4. Define strategy dependencies
2.5. Describe desired interaction with key stakeholders

3. Analyze the landscape

3.1. Analyze the social, external, and internal landscape
3.1.1. Identify relevant threats
3.1.2. Identify most critical assets
3.1.3. Identify vulnerabilities
3.1.4. Identify incidents
3.1.5. Identify requirements
3.1.5.1. Identify external laws and regulations
3.1.5.2. Identify internal laws and regulations
3.1.6. Identify running activities related to cyber security
3.1.7. Identify the internal culture
3.2. Evaluate landscape analysis with stakeholders and adjust if necessary
3.3. Perform a gap analysis (by using a framework or performing a risk analysis)
➔ Via a framework (A)
3.3.1. Define the as-is situation
3.3.1.1. Choose a framework
3.3.1.2. Assess the current status
3.3.1.3. Benchmark assessment (optional)
3.3.1.4. Describe the results
3.3.2. Define the to-be situation
3.3.3. Optional: determine cyber security visions per framework domain the cyber security ambition applies to
➔ Via a risk analysis (B)
3.3.4. Define the amount at risk (as-is)
3.3.4.1. Define the amount at risk for every critical asset
3.3.4.2. Describe total amount at risk
3.3.5. Define the risk appetite (to-be)
3.3.6. Evaluate the risks
3.4. Determine and prioritize the gap
3.5. Evaluate gap analysis with stakeholders and adjust if necessary
3.6. Define problem areas based on the landscape and gaps found

4. Describe multiple strategic objectives and associated activities

4.1. Perform a brainstorm session with stakeholders to communicate problem areas and decide on multiple strategic objectives (directions)
4.2. Evaluate results of brainstorm session and adjust if necessary
4.3. Define the business case for every strategic objective
4.4. Determine high-level activities and associated options for every strategic objective
4.5. Elaborate on the high-level activities
4.5.1. Define the milestones
4.5.2. Define the time needed
4.5.3. Define the money needed
4.5.4. Define the resources needed
4.5.5. Define the collaboration needed
4.5.6. Define the responsibilities

4.5.7. Define the measures for effectiveness (kpis) and intermediary goals
4.6. Prioritize strategic objectives with stakeholders
4.7. Let the management board choose ultimate course of action
4.8. Describe the effect of the strategy on the organization
4.8.1. Describe the effect on the staff
4.8.2. Describe the effect on the skills
4.8.3. Describe the effect on the knowledge
4.8.4. Describe the effect on the processes
4.8.5. Describe the effect on the technologies
4.8.6. Describe the effect on the responsibilities

14 Scientific papers

Towards strategy creation in the field of cyber security: the building blocks for a cyber security strategy for corporate organizations

ABSTRACT

While there are many approaches to create a business strategy, we know little about how strategy is created in the cyber security domain. Meanwhile data is one of the most valuable assets of an organization which needs protection against threats coming from cyberspace. We have evidence that, in order to adequately protect critical assets of an organization against attacks from cyberspace, it is of importance to have a structured, approach to handle cybersecurity, i.e. a strategy. In addition, we assume that this cyber security strategy, developed for corporate organization, should be in line with a cyber security ambition and support the organization's strategy. In order to explicate the steps necessary to come to a well-thought cyber security strategy, we reviewed existing literature in different domains (i.e. the business, military, and game theory domain), analyzed national cyber security strategy documents, and conducted interviews with experts in the field. The results from these three approaches resulted in a four-step approach to create a cyber security strategy. First, the management board should identify the need for a cyber security strategy and determine the cyber security ambition. Second, the steering committee should define the cyber security strategy operating setup. Third, the steering committee, together with help from the stakeholders, analyze the landscape. And finally, the steering committee, together with the stakeholders, describe multiple objectives and associated activities. The results from these four steps will be documented in a cyber security strategy document.

INTRODUCTION

In the past decades, innovative technologies in a rapidly changing environment together with larger and more complex IT landscapes have created a challenge for companies to keep their information security up to speed (Adomavicius et al., 2008; Deloitte, 2011). Internal vulnerabilities can cause cyber criminals to breach into the systems or workstations and infringe the confidentiality, integrity, and availability of data and information.

Data is currently one of the most valuable assets of organizations. Given certain types of organizations, the most important data possessed differs. For example, the banking and finance industry deals with customer, company and market specific data with regard to their finances, and the most significant detected incident is financial fraud (PwC, 2014). Another example is public agencies, where data about citizens is highly sensitive. Unauthorized access or use of data, systems, and networks counts for a quarter of all detected incidents in this industry. In 2014, "1.500 data breaches led to one billion data records comprised worldwide"; a 78% increase compared to 2013 (Gemalto, 2015) . Several reasons for the increased number of breaches are cloud computing, bring your own device, the lack of sufficient awareness amongst employees, and the increased interconnection of critical systems (Byres & Lowe, 2004; Deloitte, 2011, 2013; Verizon, 2014).

Given the importance of data and the severity of some incidents, organizations should aspire and maintain a high level of cyber security to address their most relevant threats that endanger their most valuable data. Damage to the reputation of a company by not being able to deliver a service (e.g. banks that face DDoS attacks) is a well-known consequence of data breaches. Other social costs to breaches (Grant Thornton, 2011) include amongst others: slow the pace of innovation, victimization costs, crime prevention, changes in human behavior, cost of over insurance, and job losses. In addition, financial costs to this problem also grew. The average loss per incident from the unauthorized access to information has become six times as large and the loss from the theft of proprietary information has doubled since 2004 (Dorantes, 2006). The average cost of the loss of a data record is $170, but is at least $100 more expensive when it concerns data from the healthcare or education industry (Ponemon, 2015). Taken into account that these industries mostly rely on customer data, i.e. privacy sensitive data, it is of importance to protect this data. Not only from the citizens' perspective, who does not want his/her personal data in the wrong hands, but also from a company perspective, who does not want any reputation or financial loss due to comprised data. Most data is accessible through cyberspace and therefore, this needs to be protected in a structured way that is in line with the organization's strategy.

However, organizations cannot be 100% safe from cyber-attacks. Although prevention is a step that must be undertaken, many more measures are necessary to prevent a cyber-attack (Deloitte, 2013). One should focus on either decreasing or eliminating the threat, the vulnerability, and/or the consequence to minimize the probability and impact of a cyber-attack. Threats can be eliminated by preventing threat actors to act, vulnerabilities can be prevented by hardening the targets, and consequences can be deterred or prevented by focusing on minimizing the impact of an attack (Chabinsky, 2010). To tackle this in a structured, and well-thought manner, a cyber security strategy is necessary. Currently, 72% of companies have 'outdated and overly restrictive approaches to information security', hindering performance (CEB, 2013).

In addition, there are indications that most organizations do not strategically invest in cyber security nor align this strategy with their business goals, or ambitions (PwC, 2014). Also, there is a 'continuing lack of understanding regarding the strategic importance of managing information security' (McFadzean et al., 2007). As such, a need for a formal, structured method exists (Adomavicius et al., 2008) to help organizations strategize their cyber security in order to adequately address and maintain current and future threats and corporate ambitions. But more importantly, the rationale of an organization's willingness to strategize cyber security and the actual strategy is a key factor in, ultimately, determining the effectiveness of the implementation of a cyber security strategy and carrying out the cyber security ambition. Doing this right can give an organization a competitive advantage (McFadzean et al., 2007). Therefore, this article tries to answer the following question:

How can a corporate organization develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition?

To answer our research question, (I) we gained insight in the relationship between a mission, vision, and strategy; (II) we searched literature for information about strategy creation in different domains; (III) we analyzed national cyber security strategy documents for common elements; (IV) we conducted interviews with experts; (V) the main findings were structured in a conceptual method which (VI) was validated by having a workshop session with experts and tested against a case study; (VII) the method was updated and we drew our conclusions.

LITERATURE

Information security and cyber security are often used interchangeably. However, they do not indicate the exact same thing. While cyber security is related to protecting information and non-information based assets which are processed, stored, and transported via the internet (ISACA, 2014), information security takes a broader perspective by focusing on "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability". The key differences between these terms is the perspective of information and non-information, and access through the internet or other sources. Although some might refer to information security as an umbrella term for ICT security and cyber security, information security expands on the concepts of ICT security. And cyber security, in addition, expands on the concepts of information security (von Solms & van Niekerk, 2013). Figure 5 shows the relationship between information, ICT, and cyber security.

Information security deals with both analogue and digital information (von Solms & van Niekerk, 2013). For example, leaving a paper report at a printer can pose a threat to the confidentiality of the information stored in the report. ICT security deals only with information based assets stored or transmitted using ICT, i.e. digital information. For example, passwords stolen by hackers can pose a threat to the integrity of the digital information. And lastly, cyber security deals with both information based assets stored or transmitted using ICT and non-information based assets that are vulnerable to threats via ICT (von Solms & van Niekerk, 2013). This means that also humans are an important factor in cyber security as they can be vulnerable for, for example, phishing mails. Cyber security is thus solely focused on threats from and happening in cyberspace. For example, the Stuxnet worm made use of the internet to attack Iran's nuclear centrifuges. Machines were not built with cyber security taken into mind. SCADA systems were therefore targeted via cyberspace by the Stuxnet worm.

Cyberspace is the "realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online" (Singer & Friedman, 2014). One of the key elements of cyberspace are humans, the people behind the computers and who connect to the internet. Cisco (2011) predicts that by 2020 there will be about 50 Billion of internet connected devices versus a population of 7.6 Billion people; the amount of devices connected to cyberspace is continuously growing and evolving. With the growth of cyberspace, organizations need protection against threats from cyberspace. Every organization has valuable assets that are worth protecting against threat agents who wishes to damage or abuse the asset. They will do that by exploiting vulnerabilities that exist in the asset or the environment. Security controls can be imposed to reduce the number of vulnerabilities and thereby reducing risk to an acceptable level.

Cyberspace provides several advantages above the 'real' physical world: it is timeless, borderless and anonymous. However, cyberspace was 'not designed with security in mind' according to the UK's National Audit Office (2013). Cyberspace was never designed for tracking and tracing user behavior, nor to resist highly untrustworthy users (Lipson, 2002). In addition, the current threat environment far exceeds cyberspace's design parameters and high-speed traffic hinders tracking (Lipson, 2002).

It is thus not surprising that cybercrimes followed rather quickly after the 'commercial' introduction of the internet. One of the first recognized cybercrimes, a worm, was the Morris worm in 1988 (Orman, 2003). Since then, the number of attacks has grown exponentially, especially in the 21st century. In addition, the skills needed to perform an attack has become significantly less (Lipson). For example, the ZeuS bot (Choo, 2011a) made it possible for less skilled hackers to distribute the malware and steal tons of personal identity information (PII) and financial identity information (FII).

In the past years, the threat landscape has changed by economic-, technological-, market-, and legal developments (KPMG, 2014) and has been characterized by phishing and malware. In 2009 and 2010, Australia's industry was dominated by malware attacks (Choo, 2011b). This meant a 71% increase in malware attacks compared to 2008. The period of 2004-2008 was also characterized by malware attacks, in most cases targeting the financial services industry (Choo, 2011a). Besides malware, phishing attacks was listed in the top five most expensive crime in 2009 and 2010 in Australia (Choo, 2011b). However, the

amount of fully automated attacks decreased (Potts, 2012). Also, in recent years, the motivation for committing a cybercrime shifted from curiosity and fame seeking to financial gain (Choo, 2011a). The UK's National Audit Office (2013) saw that 'serious organized crime using the internet to steal personal or financial data to commit fraud, steal corporate intellectual property, or launder money; political activists hacking and using the internet to steal information or damage computer systems to serve political agendas; and state supported espionage and attacks on critical national infrastructure' are existing and evolving threats to the internet. In addition, a research by Gragido (2011) stated that the current threat landscape is shaped by the growing availability and consumption of enterprise technologies and the increasing sophistication of cyberattacks. Besides that, web applications remain the main target of cyberattacks and legacy threats are in revival (Gragido, 2011).

And what about the future? The Internet of Things (IoT), smart devices, cloud computing, consumerization of IT (e.g. BYOD), and social media will soon shape the cyber threat landscape. (Choo, 2011a, 2011b; Contreras, Denardis, & Teplinsky, 2013; Gragido, 2011; Kellerman, 2010; Potts, 2012; Victoria & Florin, 2012; Zimski, 2011).

METHOD

Research setup

The normative research we conduct consists, first of all, of a literature review. The literature review is performed by using a snowballing technique where references within articles are further explored available on the internet or intranet. Also, current strategy processes or methods, from different domains, are researched.

In addition, expert interviews are held with security strategy experts to gain more insight in the strategy processes used in practice (in addition to what is found in the literature and current models). These experts are gathered through the network of Deloitte and others or via open channels. And finally, we look at real cyber security strategy documents to see if we can deduce a method for creating this document.

Combining this information results in the creation of an own conceptual method. This method is validated using a real case to compare our method with the one used in practice, and by having a workshop session with experts in the field of cyber security. Feedback from these validations is used to update the model.

This approach resembles the technology transfer model by Gorschek, Wohlin, Garre & Larsson (2006), where a problem is seen in an industry. The problem is then defined and studied on an academic level. The created candidate solution is both validated in academia and in practice. Finally, a practical solution is provided to the industry.

Data collection

Literature review

There are two ways to perform a literature review, structured and unstructured (or random). A structured literature review is a "form of secondary study that uses a well-defined methodology to identify, analyze, and interpret all available evidence related to a specific research question in a way that is unbiased and (to a degree) repeatable" (Kitchenham & Charters, 2007). A structured literature review offers the advantage of looking at useful literature in a structured way, so that most useless literature is quickly excluded. However, a quick scan through relevant literature revealed that not much literature is available and therefore a systematic literature review is not effective since more specific searches are needed than just one. Therefore, we perform an unstructured literature review, meaning that we search through literature by using different terms and by using the snowballing technique.

The search engine that is used to search for literature is Google Scholar. Subscriptions of Utrecht University is used to gain access to journals and other databases. Google Scholar is a hub that incorporates all scientific papers from scientific journals. It is therefore not necessary to look for another search engine, such as the ACM library.

The results from a search are first screened on the basis of the title and abstract. Only those articles that are considered relevant enough, and are available (i.e. meaning a PDF is available), are read in full-text. Notes and annotations are used in Mendeley (reference manager) to easily track articles and their subjects. The results from the unstructured literature review are presented throughout chapters 4, 5, and 0.

In addition, we use these articles to further search for relevant papers, i.e. the snowballing technique. Snowballing refers to the approach where one seeks for other relevant scientific literature in the references of already found interesting literature. In addition, casual searches (not systematic) are carried out when certain information is needed.

Analysis of national cyber security strategy documents

In addition, the second approach is to gain more insight into how strategies are created in the cyber security domain. Therefore, we ought to look at real cyber security strategies from corporate organization. However, no cyber security strategies from corporate organizations could be found online. These documents could give indirect insights in the method they used for creating that document. However, due to the transparent nature of public organizations, and their social

responsibility towards citizens, it is not surprising that in the public domain cyber security strategies are generally published. Besides, citizens are one of the most important stakeholders in governmental cyber security strategies. Therefore these published strategies are a good basis for the understanding of a cyber security strategy. This understanding can create a basis for discussion about cyber security strategy in corporate organizations. By analyzing the strategy documents on content, and identifying what is generally described (e.g. strategic objectives, cyber threat landscape for a specific country), we can externalize the critical factors taken into account when constructing a security strategy and what steps were followed.

A search was performed via Google, by using the search term 'cyber security strategy'. With this search, two hubs for national cyber security strategies were found, namely the website of ENISA[13] and the website of the NATO Cooperative Cyber Defense Centre of Excellence[14]. Scanning through these sites resulted in 31 adequate national cyber security strategies, meaning that they fulfilled the inclusion criteria. The national security strategies were included when (a) they would discuss the topic of either information security or cyber security; (b) the strategy is published in Dutch or English; (c) a PDF version is available; and (d) the strategy document is final.

The national cyber security strategies that were excluded from the analysis are listed in Table 1..

Table 1: Excluded national cyber security strategies

Country	Exclusion criteria
India	Only a draft version (notification) is available
Luxembourg	Only published in French
Malaysia	Only a summary is available
Romania	Only published in Romanian
Russia	Only available in plain HTML
Rwanda	Only a draft version is available
South Africa	Only a draft version is available

The goal of the analysis is to deduce the critical factors taken into account when constructing these national cyber security strategies. By analyzing what is discussed, one can translate this back to what is thought of when creating the strategy document. This was done by highlighting all important aspects that are discussed in the strategy documents. In this case, it did not matter what the exact directions are or content is of a certain section. Only the general content, like the fact that in section 1 strategic drivers were discussed, matters.

Expert interviews

And finally, expert interviews were necessary because of limited literature available about the creation of a cyber security strategy. Due to the explorative nature of the interviews, questions were asked in a semi-structured manner. At first, specific questions are posed to the interviewee, but later on, questions may vary between interviews. In addition, other questions will be asked to evoke additional information from the interviewee.

Due to limited time and resources, participants are chosen on the basis of purposive sampling. Purposive sampling is a non-probability based sampling method and is especially effective when experts are needed to be interviewed in a certain domain (Flick, 2009; Tongco, 2007). Participants are selected based on two criteria: their function and their knowledge about creating a (cyber) security strategy. Consultants in the field of cyber security and Chief Information Security Officer (CISO) were considered as suitable interviewees in order to gain answers and insights into the methods used to create a cyber security ambition and strategy. However, it was needed that these potential interviewees were familiar with creating a (cyber) security ambition or strategy.

Table 2 shows the selected participants for the qualitative research. Fifteen interviews were held with security officers and consultants. However, two of those interviews were held in the beginning of the process to gain background information about the subject and to assess the feasibility of the study.

[13] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world , consulted on 17-02-2015
[14] https://ccdcoe.org/strategies-policies.html , consulted on 17-02-2015

Table 2: Selected participants for the qualitative research

	Role	Sector or industries	Via list?
Expert 1	Information security officer	Public sector	Yes
Expert 2	Consultant	Insurance sector, public sector, computer industry	Yes
Expert 3	Security officer	Public sector	Yes
Expert 4	Consultant / ex-information security officer	Electronics industry, transport industry	Yes
Expert 5	Consultant / ex-CISO	Transport industry, defense industry, energy industry	Yes
Expert 6	CISO / ex-consultant	Financial industry	Yes
Expert 7	Security and policy advisor	Public sector	Yes
Expert 8	Risk officer	Financial industry	Yes
Expert 9	Consultant	Belastingdienst. Achmea	Yes
Expert 10	Consultant	Electronics	Yes
Expert 11	Consultant	Electronics	Yes
Expert 12	Consultant / ex-CISO	Public sector, financial industry	Yes
Expert 13	Security manager	Insurance sector	No
Expert 14	Consultant	Defense industry	No
Expert 15	Consultant	Electronics	No

Every interviewee was sent the questions up front. The interview existed of four questions about ambition and six questions about strategy. Before the formal questions were posed, interviewees were given a definition of cyber security ambition and strategy. During the interview the following definitions were used:

- An ambition is "a certain goal or aim: something an organization hopes to do or achieve";
- A strategy is "a plan, method, or series of maneuvers or stratagems for obtaining a specific goal or result".

The interviewees were asked whether they agreed with this definition. This was necessary so that every interviewee had the same understanding of these definitions and there was little chance of misunderstandings.

All interviews were recorded and transcribed afterwards. These transcriptions can be found in the Appendix. All data gained from the interviews is analyzed with NVivo. NVivo is a qualitative analysis tool used to code data. The data is coded in nodes resembling the questions asked. After this first set of nodes, every node is coded again to identify categories and concepts in the data per question. This is a useful way to structure and to analyze interviews.

Data validation

Based on the results from the research as described above, a conceptual method is created. This method is validated with experts from the cyber security field in the form of a workshop session and by using a case study for comparison. The findings of these validations will be used to adapt the conceptual method to a final method. The conceptual method is not presented here. More information about the conceptual method can be found in <scriptie>

The workshop session was held with 17 experts from the cyber and privacy advisory team of Deloitte. The experts were given a brief presentation of the conceptual method. In addition, plain text versions of the conceptual method were given. After the presentation, the experts were asked to form groups of 2 or 3 persons, resulting in 6 groups. This was done to stir up discussion about the presented method within the groups and afterwards between groups. Each group was given a form with two questions about the completeness, six questions about the correctness, and two questions about the acceptability of the conceptual method. Also, a question to discuss a certain topic was posed. The group of experts were asked to fill in the questions in a 30 minute time span. Due to this time limitation, every group was asked to start at a different set of questions. This is done because if time ran out, all questions were answered at least once. The full results of the workshop validation can be found in section 13.3.1.

In addition to a workshop session, one case study was performed. Case studies offer the advantages of (George & Bennett, 2004) potentially achieving high conceptual validity, having strong procedures for fostering new hypotheses, having value as a useful means to closely examine the hypothesized role of causal mechanisms in the context of individual cases, and having the capacity for addressing causal complexity.

During the case study, the created method was used to assess if the cyber security strategy of the case company followed a likewise method. The network of Deloitte was used to select a case company. The results from the case studies are used to update and finalize the method. Unfortunately, due to time constraints, only one case study can be performed. In addition, confidential information in the cyber security strategy of the case organization is disclosed, no information about the case company is given except that it is a large, corporate, Dutch organization.

THEORETICAL FRAMEWORK AND EXPERT INSIGHTS

Strategy creation from different perspectives

Strategies are often created if a goal is to be met. These goals can be various, and therefore strategy is created everywhere and by everyone. Whereas we are interested in the creation of a cyber security strategy, literature is almost non-existent. Therefore strategy creation from the organizational, military, and game theory perspective will be researched additionally.

Strategy elements from the organizational, military, and game theory perspective

The list of models, present in the organizational, military, and game theory domain, used is not exhaustive, but it does contain the best known strategic models. In addition, all models listed are translated to the domain of cyber security, making them applicable for further analysis. This section will elaborate on the strategy elements from the organizational, military, and game theory domain. First the BCG growth-share matrix, the 7-S model of McKinsey, Porter's five forces, PEST(EL) analysis, SWOT analysis, and the balanced scorecard will be discussed as organizational strategy models. Next, strategic theorists in the military field and the OODA loop will be discussed. And lastly, game theory in relation to strategy creation is presented.

Strategy elements from the organizational perspective

In 1977, The Boston Consulting Group created an approach for organizations to develop a strategy. This approach was based on an earlier research that indicated the requirements for strategic success by organizations. According to Hedley (1977), key to strategic success is considering both the organization's growth and the market share. The growth is inherently linked to gaining market share: by expanding capacity earlier than competitors, a larger market share can be obtained. In addition, growth also provides the opportunity to invest. When a company has a high market growth, investments are necessary to keep that position, also in terms of the market share. But, this also gives an advantage for the investors who will receive larger amounts of money later on. Although it is hard to position an organization in the business portfolio matrix based on its security, it is however, a useful tool. Especially the position of the wildcat is interesting; is there a way that a wildcat organization could not reach the star position when their cyber security is not adequate enough? And, could an organization reach a certain desired position quicker, or stay on this position longer, when security is adequate? The BCG growth-share matrix is primarily focused on the external environment. A model that focusses on the internal environment is the 7-S model of McKinsey.

Waterman, Peters, and Philips (1980) researched the relationship between structure, strategy, and organization. Their research resulted in the 7-S framework, presenting 7 concepts related to organizational thought, where changing an organization is not just changing its structure. According to Waterman et al. (1980), "effective change is the relationship between structure, strategy, systems, style, skills, staff, and something we call superordinate goals". Structure is the way an organization is composed. Strategy deals with what goals a business wants to pursue and how. A system deals with all procedures necessary to run a business, especially financial procedures. Style is the way in which a business is run. In addition, staff is defined by the people and their skills are decisive for the organization's competitive advantage. These components all refer to internal variables that are useful in reaching a strategic transformation. But the ultimate success will highly depend on the ability to derive strategy from shared values of the ones who implement it (Ward & Peppard, 2008). The 7-S framework is based upon the ideas that multiple factors influence an organization's ability to change, interconnection between the components is inevitable, failure to pay attention to the other S's may cause the failure of the strategy, and there is no starting point, meaning that an organization can randomly start with an S. As is clear from the description above, the 7-S framework is useful to analyze the internal environment of an organization. Such an internal analysis of an organization's cyber security capabilities is also important to do. We want to see how cyber security is positioned and structured within the organization. Who is responsible for what? In addition, a strategy in the field of cyber security should be imposed. Therefore, we also need the systems holding the cyber security resources together, namely the formal and informal procedures that are necessary for business continuity. Also, the style of the responsible persons for cyber security is an important influencing factor when changing the environment. Furthermore, the staff factor deals with the profiles and skills of the people responsible for cyber security. The skills factor considers what the organization excels at with regard to cyber security, e.g. what are their strengths? And lastly, the shared values is related to corporate culture regarding cyber security and the cyber security vision within the organization.

In 1979, Michael Porter described how competitive forces shape strategy. Porter identified five forces to review competition in the marketplace, necessary to adapt the corporate strategy to. The five competitive forces are threat of new entrants, bargaining power of buyers, bargaining power of suppliers, threat of substitute products or services, and rivalry amongst existing competitors. The impact of the five forces on an organization and its competitive market can lead to a strategy. Simply said, these five forces are 'external things' an organization should assess in terms of impact. This assessment can be done on every organization, industry, or service. And therefore, cyber security can be seen in relation to these industry competitive forces. The five forces can be used to assess different aspects of cyber security. For instance, the threat of new entrants can be assessed by looking at the threat landscape. What are the chances that an industry will be attacked and what kind of attack will be done? The bargaining power of buyers can be assessed by looking at threat agents. Assessing the threat of substitute products or services can be seen similar to assessing the impact or consequences of a cyber security breach. Suppliers can be seen as third party suppliers that offer software solutions to companies. They too have to secure their software used by other companies. And lastly, rivalry amongst other companies can be seen as how other companies in the same industry have organized their cyber security.

Another tool to analyze the external macro-environment is the PEST(EL) framework. PEST(EL) stands for political, economic, social, technological, environmental, and legal. Usually the environmental factor is discussed within the social factor, and legal is discussed within the political factor. According to Ward & Peppard (2008, p. 72), "carefully and continuously monitoring these factors can lead to significant business opportunities or identification of potential threats in time to take action to mitigate the effects". There have been several studies that show two kinds of approach of the PEST(EL) analysis. First, it can be used to analyze the external environment. And second, it can be used to analyze the viability of a certain solution in the external environment (Peng & Nunes, 2007). Ultimately, this analysis tool is used to show which factors are of influence on the organization and its operations. The PEST(EL) factors can also be used to map both the external and the internal environment that influence the cyber security of an organization. Political and legal factors refer to laws and regulation that apply to the cyber security domain. Economic factors refer to the budgets available to implement cyber security measures. In addition, social and environmental factors refer to, amongst other, awareness of people in the internal environment and social developments in the external environment. The technology factor refers to technological developments in the external environment that call for new, extra, or advanced security.

In addition, the SWOT analysis is also a method to analyze an organization's strategic position. SWOT stands for strengths, weaknesses, opportunities, and threats. According to Hill and Westbrook (1997), an organization must have a good fit between the external environment, in terms of opportunities and threats, and the internal environment, in terms of its own strengths and weaknesses. The four elements of the SWOT analysis can be directly used for the application in the cyber security domain. For instance, the national information security strategy of Uganda lists their strengths, weaknesses, opportunities, and threats. One of the strengths is the "presence of Government political will in the area of national information security" (Uganda, 2011, p. 24). An internal weakness is, for example, "lack of information security awareness and persistent poor information security culture" (Uganda, 2011, p. 25). An opportunity identified by the government of Uganda is "actively participate in international co-operations on information security" (Uganda, 2011, p. 26). And lastly, an identified threat is "cybercrime, cyber warfare, and cyber terrorism" (Uganda, 2011, p. 27). Every strength, weakness, opportunity, and threat gives direction to a strategy.

Strategy elements from the military perspective

From the previous section we have learned that the organizational models are quite general and mostly focused on assessing the internal or the external environment. In this section we will discuss strategy creation from the military domain. The military domain is well known for always strategically planning and structuring military missions. Their structured approach from deciding on a mission, to formulating the mission and the strategy, to actually deploying soldiers is useful input for the creation of other strategies.

In the military world, Helmuth Karl Bernhard von Moltke and John Boyd are, amongst others, well-known names with regard to strategy. Their approaches have proven its effectiveness and have been translated to the business domain. According to von Moltke, a German field marshal from 1819 until 1888, "strategy is not a lengthy action plan but rather the evolution of a central idea through continually changing circumstances" (Perky, 1991). Adjusting means to ends was one of the key ideas of von Moltke about strategy. In addition, von Moltke viewed strategy as a series of options. Von Moltke's work was influenced by Napoleon and Carl von Clausewitz, the last one being a Prussian general who wrote many military theories. One of them is related to strategy, where strategy was defined by him as "the use of engagements for the object of war" (Owens, 2007, p. 116). Von Clausewitz stressed that the unexpected developments in the environment call for direct action by leaders. Unexpected developments may appear under the 'fog of war', a term used to describe "the ability to process cognitive information and act quickly, effectively, and decisively on the battlefield, as well as the many external factors contributing to uncertainty and indecision" (Lieberman et al., 2005). Like in fog, things tend to seem different than in reality and therefore rapid action is needed to overcome the sudden change in reality.

Another strategic thinker was John Boyd, a United States Air Force fighter pilot. According to Boyd, in order to understand the environment we must interact with it in different ways. And ultimately, strategy will be "a game in which we must be able to diminish adversary's ability to communicate or interact with his environment while sustaining or improving ours" (Boyd, 1986, p. 34). In order to create strategy, Boyd developed the so-called OODA loop, which stands for Observe, Orient, Decide, and Act. It was used to help respond quicker and more appropriate to actions than the competitor. The best way to do so is by getting inside the OODA loop of the competitor, or simply put, to think ahead of what the competitor would do. The first step in the OODA loop is observation. Observations are based on outside information, unfolding circumstances, implicit guidance and control from the orientation stage, and feedback from the decision and action stage. These observations are input for the orientation stage. The orientation stage is the most important stage of the model, and, among other things, filters the information on relevance from the previous stage. Important variables in the orientation stage that shape mental images, views or impressions of the world are cultural traditions, previous experiences, new information, and genetic heritage (Boyd, 1987a). It is said that "without cultural traditions and genetic heritage, the influence of new information and previous experiences increases"15. The analysis and synthesis element in the orientation stage is not so much a factor as it is an approach to analyze and synthesize the other factors by decomposing and recomposing them in a way that unrelated factors suddenly can become related. By emphasizing rather quickly made implicit relationships instead of more time-consuming explicit relationships, one can take an advantage above adversaries in terms of time and friction (Boyd, 1987a). The information from the orientation stage is fed forward to the decision stage where decisions are made about the strategy. The decision is the input for the actions that are needed to be taken in the action stage. Feedback from both the

[15] http://www.iohai.com/iohai-resources/certain-to-win-richards_files/frame.htm , consulted on 8-6-2015

decision and action stage is fed back to the observations stage making the OODA loop continuous. These stages are directly translatable to the field of cyber security.

Strategy elements from the game theory perspective

In the previous section we discussed how strategy is created in the military domain. In this section we present how strategy is created in the game theory domain. When playing a game, one is continually defining goals one wishes to obtain. These can be, for instance, winning the game or obtaining the high score. In order to achieve this goal, a strategy is created by the player and steps are undertaken. It is a simple approach to strategy creation, however, valid. In this section we go into depth in this way of creating a strategy.

According to Johnson et al. (2008), game theory is about "the interrelationships between the competitive moves of a set of competitors". Game theory is based upon two key assumptions: the rationality of competitors and the interdependent relationship between competitors. These can be translated into two ways in the process of creating a strategy. First, the strategist should get in the mind of the competitors and ask himself questions like "what would my competitor do?" Second, "decide strategy on the basis of understanding the outcomes of possible strategic moves of competitors" (Johnson et al., 2008, p. 280). This is also stressed by Brandenburger and Nalebuff (1995) who emphasize that the importance of game theory is in the focus on others instead of the own position. In addition, they add that a player can only take away from a game what he has put into it. This means that a strategist should look at the most value created player, and see how much value the remaining players create if this most value created player was not present. In addition, taking into account the steps that the attackers (the competitors) are likely to take can help find appropriate measures and justify those. In this way, a strategy is a continuous game in which steps are deliberated in advance and value is created and captured.

Game theory shows us that strategy can be created by focusing on others instead of the own position. This resembles, to some degree, how strategy is created in the military domain and therefore in the cyber security domain according to us. In addition, we saw that it is important to look at the most value created player and what value the remaining players create if the most value created player was not present. Let's say that security is a high value creator. If cyber security was taken away, can the other business services of the cookie factory still create value to the organization? Well, yes they can in our opinion. Security is not a high value creator in itself because security costs money and thus not directly contribute to the revenue of the cookie factory. A high value creator of the cookie factory is the recipe and in the future, will be the online portal. They can only stay a high value creator if the cyber security measures are up to the highest standards. Because if this is not the case, someone can steal the recipe or shut down the portal. Either way, it will take away the high value of the recipe or the online portal.

In addition, we should try to understand how the other players, the attackers, play. The cookie factory will most likely need to monitor the changing threat landscape and could implement a honeypot system to observe if an attacker breaches the security. This way the cookie factory can analyze the sophistication of the attacker

Sub analysis

Analyzing the purpose of the models discussed above shows us different ways of looking at the area of creating a strategy. We took all elements from the models explained above. These elements are for instance market growth, strengths, weaknesses etcetera. We combined all these elements into three groups, namely: the social environment, the external environment, and the internal environment. These three groups are most applicable in the cyber security domain because, as we have explained in the introduction, attacks can be done by outsiders but also insiders. In addition, the humans (the social environment) are usually a weak link.

The social environment deals with, amongst others, humans, social relationships and culture within an organization. The external environment deals with elements that exist outside the organization that are hard to control, but do influence the organization in different ways. For instance, a sudden rise in targeted phishing attacks may cause to focus a strategy more around being resilient towards this threat. The internal environment deals with all elements that exist within the organization. For instance, the business wants to go more digital and this thus results in having to have more and better protection of these digital services. The elements from the internal environment are, in comparison with the social environment, better measurable (e.g. comparable to hard skills).

Table 3 shows how the strategy elements from organizational, military and game theory models fit within the three groups. As such, we see how each model with associated elements relates to the three groups we classified. In our opinion, the results of analyzing the internal, external, and social environment can stress the need for a cyber security strategy, and determines the drivers. In addition, we use these three groups when we analyze the current situation during strategy creation because all models are used for this purpose.

Table 3: Common elements found in the business, game theory, and military domain related to strategy creation

Model	Element	Social environment	External environment	Internal environment
BCG Growth-share matrix	Market growth		X	
	Market share		X	
7-S model of McKinsey	Strategy			X
	Structure			X
	Style			X
	Staff			X
	Skills			X
	Shared values	X		
	Systems			X
Porter's five forces	Threats of new entrants		X	
	Bargaining power of buyers		X	
	Bargaining powers of suppliers		X	
	Threat of substitute products or services		X	
	Rivalry amongst competitors		X	
PEST(EL)	Political		X	
	Economic		X	
	Social		X	
	Technological		X	
SWOT	Strengths			X
	Weaknesses			X
	Opportunities		X	
	Threats		X	
OODA Loop	Cultural traditions	X		
	Outside information		X	
	Series of options			X
	Genetic heritage	X		
	Unfolding circumstances			X
	Unfolding environmental interaction		X	
	New information		X	X
	Previous experiences		X	X
Game theory	Added values			X
	Opponents		X	
	Players	X	X	
	Rules (Laws & regulations)		X	
	Tactics		X	

Strategy elements from the cyber security perspective

The classification found in the previous section shows that a common element in strategy formation is assessing the social, external, and internal environment. These environments are quite general, and as such, we want to get more insights into the specific cyber security strategy elements. Since there is nothing published on the creation of a cyber security strategy, we will base our information on what we could extract from national cyber security strategy documents and interviews with experts in the field of cyber security.

Cyber security strategy elements from a cross-border analysis of national cyber security strategies

Thirty-one national cyber security strategies across the world have been analyzed (see section 3.2.2) and elements for the creation of these strategy documents have been extracted. The analysis included both EU and non-EU countries where a cyber security strategy document was available. During the analysis, elements were searched for in the national cyber security strategy documents. Since we found 48 unique elements, we classified the elements found in the national cyber security strategy documents in self-made groups as was done in the previous section, namely general elements and cyber specific elements. The following categories are distinguished:

- Strategic drivers and scope: (1) Drivers; (2) Economic impact; (3) Scope; (4) Definitions; (5) Relation with other strategic documents; (6) Relation with previous strategies; (7) Compliance with laws; (8) Stakeholders.
- The cyber threat landscape: (1) Threats; (2) Risks; (3) Challenges; (4) Opportunities; (5) Cyber trends; (6) ICT trends.
- AS-IS analysis: (1) Maturity analysis; (2) Comparison with other countries; (3) Analysis of critical infrastructures; (4) Current situation.

- TO-BE analysis: (1) Vision; (2) Mission; (3) Ambition; (4) Strategic objectives; (5) Strategy guidelines; (6) Key benefits.
- Countermeasures: (1) Action; (2) Action timeframe; (3) Action stakeholders; (4) Action plan; (5) Action measure; (6) Important milestones and CSF; (7) Roles and responsibilities government and stakeholders.
- Implementation plan: (1) Implementation plan; (2) Follow-up; (3) Assessment of effectiveness; (4) Expected effects; (5) Effectiveness of actions; (6) Effectiveness measures; (7) Consequences; (8) Organization; (9) Cooperation; (10) Financing.

We distinguish 2 overarching categories, namely general elements and cyber threat landscape elements. The general elements category is made up of all categories listed above, except for the cyber threat landscape category. These categories will become useful when we create our method.

Cyber security strategy elements from the experts perspective

In addition to gathering which cyber security strategy elements in the public domain, experts were interviewed about their view on the creation of cyber security strategy. During the interviews, it was first asked how the interviewee developed a (cyber) security strategy and what process they followed. However, it was noticeable during the interviews that experts had trouble explicating the process they followed to create a (cyber) security strategy. The five most important elements mentioned were to look at threats (6x), analyze the current situation (6x), use a framework (5x), look at developments (5x), and assess critical assets (4x). In addition, experts also mentioned that one should use a risk analysis approach (3x).

Although we think these elements are very high-level, some experts discuss, for example, different kinds of developments. For instance, one can look at internal developments, technical developments, and social developments. These results show that the top 5 most mentioned process steps are analyzing the threats, analyzing the current situation, using a framework, analyzing development, and performing a risk analysis. However, the list provided above lists both process steps and elements. Since we are only interested in the elements for this section, the process steps are excluded from the analysis. For instance 'using a framework', or 'performing a risk analysis' because they are not so much elements as they are detailed processes that can be followed. In addition, elements that are common to be found in a strategy document, like 'scope', are also excluded from the analysis.

Table 4Table 10 shows the results of the analysis where we divided the elements in two categories, namely: generic elements and cyber specific elements. These categories are the same as we used in the analysis of national cyber security strategy elements to support uniformity. The elements we found are used to create a cyber security strategy, which is explained later on.

Table 4: The classification of the cyber security elements expressed by cyber security experts

	General elements	Cyber specific elements
Threats		X
Current situation	X	
Developments	X	X
Assets	X	
Link between the business ambition and the cyber security ambition		X
Company landscape, both internal as external	X	
Incidents		X
Stakeholders	X	
Responsibilities	X	
Risks		X
Vision of the future	X	

Sub analysis

The elements presented in Table 9 and Table 10 show which cyber security specific elements are of importance in creating a strategy. We have seen that we could divide the elements found in the national cyber security strategies and interviews into two categories, general elements and cyber specific elements. We are most interested for this section in the cyber specific elements. If we look closely at both tables, we see that there is some overlap in elements. In both tables we see that threats and risks are important. In addition, trends and developments are also relevant elements. Because we think trends and developments are quite similar, we paired them together. Below we constructed a summary of the cyber security elements that are important to look at when creating a cyber security strategy:

- Link between the business ambition and cyber security ambition.
- Threats;
- Risks;
- Challenges;
- Opportunities;
- Trends & developments;

- Incidents;

Sub conclusion

In this chapter we saw that the military, game theory, and business strategy elements are applicable to the cyber security domain. This means that these models can be used for further analysis to create our own method. The complete analysis showed us that we must focus on the social, external and internal environment when determining the need for a cyber security, as well as assessing the current situation. During the assessment, both the cyber security defense capabilities and the cyber security threat landscape are topic of assessment. The entire assessment needs to focus on the following aspects to discover strengths and weaknesses (threats):

- The social environment:
  - Cyber security defense capabilities: e.g. awareness amongst personnel, a sensible level of trust, feeling responsible for the security of personal data, careful use of BYOD.
  - Cyber security threat landscape: e.g. more and more targeted towards employees, personal data and personal smart devices rather than attacks on the enterprise networks.
- The external environment:
  - Cyber security defense capabilities: e.g. information about possible adversaries, no lock-in to a single external company, regular knowledge gathering regarding cyber security from external experts, regular external audits performed at outsourcing partners.
  - Cyber security threat landscape: e.g. increase in zero-day exploits, more complicated attacks, better equipped and organized cyber security attackers.
- The internal environment:
  - Cyber security defense capabilities: e.g. good detection mechanisms, good response mechanisms, qualified security intelligence personnel, up-to-date with latest patches, regular vulnerability scans, regular penetration tests performed.
  - Cyber security threat landscape: e.g. internal IT complexity disguises potential weak spots, internet connectivity everywhere (wired and wireless).

As discussed before, the assessment of the social, external and internal environment can be used to establish the current situation of cyber security defense capabilities and the cyber security threat landscape and give input for the need for a cyber security strategy.

TOWARDS A STRUCTURED METHOD

The goal of the research is to create a well-thought method for formulating a cyber security strategy, to answer the main research question. This chapter will show a method, based on the previous chapters, to formulate a cyber security strategy. We used the categories deduced from the analysis of the national cyber security strategy as our basis and transformed these with the results from the literature review and the expert interviews. This resulted in a conceptual method which was then validated with 17 experts in the field and by using a case study (for more information, see thesis). Finally, a four-step method was found.

Introduction

The method consists of four consecutive steps. Every step has sub activities, and related deliverables. The six main steps that are found during this research are:

1. Identify the need for a cyber security strategy and determine the ambition;
2. Define the cyber security operating setup;
3. Analyze the current situation;
4. Describe multiple strategic objectives and associated activities.

Each step will be elaborated in the following sections. But before creating such a strategy, one should take note of the following constraints:

- Without buy-in from the management board, one should not create a strategy. Their support is important for the implementation phase of the strategy. Most 'projects' fail without proper support from the management board;
- The cyber security strategy should be part of, aligned with, and support the business strategy. No exceptions;
- The cyber security strategy should be evaluated yearly and renewed every three years;
- Stakeholders should be involved early in the process of creating a cyber security strategy. Besides the management board, stakeholders are the basis for getting information and afterwards, implementing and propagating the strategy;
- The outcomes of every step and the previous steps should be reviewed after the completion of this step;
- After completion of creating a cyber security strategy, the process of executing the roadmap should be formalized (e.g. in the form of indicating next steps).

In addition, to execute the activities for creating the actual cyber security strategy, we acknowledge the following three roles:

- The management board;

- The responsible person(s) for group wide security management (with regard to ease of use, this will be called the steering committee[16]);
- The stakeholders.

The method to create a well-thought cyber security strategy is depicted in Figure 40.

Step 1: Identify the need for a cyber security strategy and determine the ambition

The first step is to decide on the need for a cyber security strategy. Without a proper driver, succeeding at establishing and implementing a cyber security strategy will be harder. The management board should deliberately ask themselves why they want a cyber security strategy. This can be done by considering a changing environment, by looking high-level into the cyber threat landscape, the position of the organization in the marketplace, the value of information stored and the risks involved when this information gets exposed, or the developments in the field and the consequence of de-perimeterization. In addition, the management board should consider the current situation regarding cyber security strategy and controls are in place. Also, the board should look into laws and regulations that might oblige them to have a certain cyber security strategy. For instance, the 'Nederlandse Bank' insists that all Dutch banks and insurance companies comply with the CobiT standard. During our research we saw that often the cyber security strategy is initiated by external regulators to comply with laws and regulation. When the need for a cyber security strategy is identified, the management board should document all their decisions.

Once the need for a cyber security strategy is identified, the scope should be defined. Next, the management board should determine the cyber security ambition. This ambition should state their high-level aspirations with cyber security. To establish the cyber security ambition, the management board should identify the organization's ambition and link this to the cyber security ambition. Cyber security should inherently support the organization's operations and therefore the organization's ambitions. Once this is done, the management board should make the cyber security ambition more practical and conveyable to the public by making it coherent, powerful, and realistic or by incorporating an ambition level.

For instance, one could think of industry-standard, industry-leading, and overall leading. Industry standard means that the company wants to do is what is recognized as standard in the industry and what most competitors have implemented. Industry-leading means that the company wants to excel in their industry with regard to cyber security. The company wants to have the best cyber security compared to industry competitors. And lastly, overall leading means that the company want to have the best cyber security outside of their own industry. They want to be leading, innovative, and of cyber security.

An example of an ambition from the Dutch cyber security strategy 2.0 (the Netherlands, 2013, p. 8-9):

The Netherlands is a leader in cyber security:

- Dutch society knows how to make safe, optimal use of the advantages of digitization;
- Dutch businesses and the research community are pioneers in 'security by design' and 'privacy by design';
- Together with its international partners, the Netherlands is part of a progressive coalition that seeks to protect fundamental rights and values in the digital domain.

Organizations can also determine cyber security visions per domain the cyber security ambition applies to. And finally, guiding principles (i.e. with what goals should the strategy comply to) and the desired outcomes of the cyber security strategy (i.e. what goals should be met with this strategy).

If the management board cannot identify a need for a cyber security strategy, it is advised not to continue formulating a cyber security strategy until there is a legitimate driver.

[16] Not every organization will create a project with a steering committee to establish a cyber security strategy. Therefore a responsible person or multiple persons for group wide security management is a more generic term. This person can be a CISO, or a CRO, or even security managers.

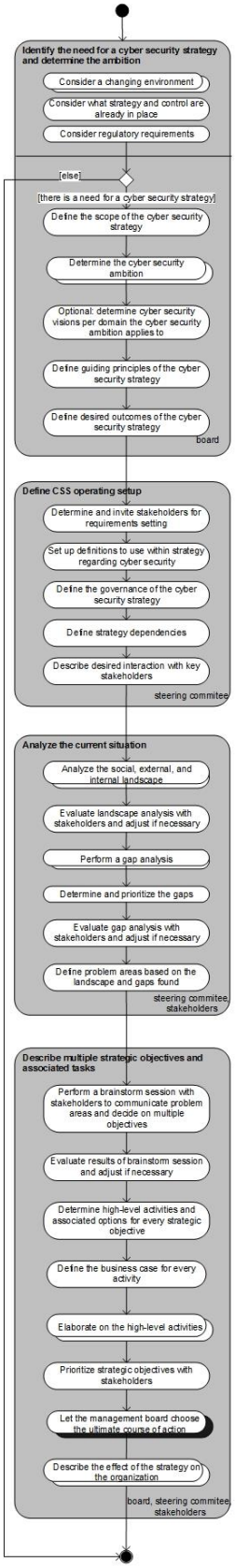


FIGURE 40: ACTIVITY DIAGRAM CYBER SECURITY STRATEGY CREATION METHOD

Step 2: Define the cyber security operating setup

Once there is a need for a cyber security strategy established and decided upon a cyber security ambition, the next step is to determine the scope and stakeholders. First, the steering committee should determine stakeholders and what their stake is in the cyber security strategy, and invite them for requirements setting. One could distinguish different stakeholders with certain priorities based on their stakes in the cyber security strategy. For instance:

- Business leaders (priority 1): to learn the needs from the business;
- IT (priority 2): to understand the current state of IT security;
- Privacy and Security (priority 3): to learn privacy and information security requirements;
- Risk Management (priority 4): to learn the current state of cyber security risk management practices.

In addition, the steering committee should set up definitions to use within the cyber security strategy. For instance by answering the questions: what does cyber security mean to us? When is a threat relevant? What is critical? In addition, governance structures should be defined by using, for example, a RACI matrix. Furthermore strategy dependencies should be defined to see what influence the strategy has on business units, people, and etcetera. And finally, by inviting stakeholders to help in the process of creating a cyber security strategy, it is important to describe the interaction one desires with these key stakeholders.

The steering committee should document all decisions regarding the stakeholders, scope, and definitions in a so-called project setup document.

Step 3: Analyze the current situation

Now that the operating setup has been determined, the steering committee, together with the stakeholders, can analyze the current situation in depth.

First, the internal landscape is analyzed by, for instance, examining relevant threats, most critical assets, vulnerabilities, incidents, internal and external requirements, running activities related to cyber security, and by identifying the internal culture. The results from this analysis should be evaluated with stakeholders and adjusted if necessary.

An example of considering threats to the critical assets of an organization:

Bank X has a number of customer accounts that store money. As such, one of their critical assets is the customer accounts, and another critical asset is money. A threat to these critical assets is that someone hacks into the system and steals customer data and/or money from the customers. If this happens, it will result in reputation and financial damage for the bank. The risk of this happening is medium, because the impact is high and the probability is medium.

Next, a gap analysis is performed by using a framework or performing a risk analysis. A framework is usually used as a baseline and consists of a basic set of measures. These measures are so generic that they can be used for every organization. A risk analysis is, however, performed specifically for the organization of interest. This approach should therefore only be used when the organization is mature enough. Performing a risk analysis is complex, labor-intensive, and requires a lot of knowledge on conducting it, while using a framework is, simply said, checking a list. In our method, the following activities are involved in determining the gap:

- Using a framework.

A common approach for determining a strategy is by using a framework. With a framework we mean standards (e.g. ISO2700x), frameworks (e.g. CobiT), and maturity models (e.g. NIST). These can be used as a checklist to see what is already in place, and to see what should be implemented to, for instance, comply with standards, or to gain a higher maturity. The first step is to define the as-is situation with a framework chosen by the steering committee and optionally, benchmark these results against results from peers in the industry. The second step is to use the framework to define the to-be situation. In addition, the steering committee can determine cyber security visions per framework domain the cyber security ambition applies to. The difference between these situations results in zero or more gaps.

An example of a commonly used framework is the NIST maturity model. It is developed by the Government of the United States of America, and specifically made for organization's that manage critical infrastructures. There is a clear link in the model between the business drivers and the cyber security activities that should be undertaken. In addition, a clear link is made with risks, and according to the government of the USA it provides "a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risks for those processes, information, and systems directly involved in the delivery of critical infrastructure services" (NIST,

2014, p. 3). According to several experts, the NIST model is primarily practical in use and easy to communicate to the board.

- Performing a risk analysis.
  A risk analysis is performed by, first, defining the as-is situation. This is done by defining the amount at risk for every critical asset and considering the risks found in the previous step. The amount at risk can be determined by assessing the degree to which the confidentiality, integrity, and availability of every critical asset is affected. A helpful tool for this are SPRINT forms. Second, the to-be situation is assessed in the form of a risk appetite. The risks appetite is the amount of risk the management board is willing to take. This too can be assessed by using a SPRINT form. Next, the risks are evaluated, meaning that the significance of a risk is determined. And finally, the gap between the risk appetite (the to-be situation) and the amount at risk (the as-is situation).

Within both approaches, the difference between the as-is situation and the to-be situation will result in zero or more gaps. These gaps are then prioritized. Next, the results of the gap analysis are evaluated with stakeholders and adjusted if necessary. Finally, problem areas are defined based on the landscape and gaps found.

Step 4: Describe multiple strategic objectives and associated tasks

The final step is to describe multiple strategic objectives and associated tasks. A brainstorm session is performed with stakeholders to communicate problem areas and decide on multiple strategic objectives. These strategic objectives should be SMART (specific, measurable, assignable, realistic, and time-oriented).

An example of strategic objectives are (the Netherlands, 2013):

- The Netherlands is resilient to cyber-attacks and protects its vital interests in the digital domain;
- The Netherlands tackles cybercrime;
- The Netherlands invests in secure ICT products and services that protect privacy;
- The Netherlands builds coalitions for freedom, security, and peace in the digital domain;
- The Netherlands has sufficient cyber security knowledge and skills and invests in ICT innovation to attain cyber security objectives.

These are linked to the cyber security ambition example presented earlier.

The results from the brainstorm session should be evaluated and adjusted if needed. In addition, high-level activities will be determined for every strategic objectives. A list of evaluated strategic objectives will be used to define a business case for every strategic objective. Next, the strategic objectives will need to be elaborated on by defining milestones, time needed, money needed, resources needed, collaboration needed, responsibilities, the measures for effectiveness, and intermediary goals.

Next, together with the stakeholders, one should prioritize the strategic objectives. This can be done, for example, by using the MoSCoW method. After the prioritization, the management board should choose the ultimate course of action.

Finally, the effect on the organization from implementing the chosen strategy is described. The steering committee should determine the effect on the staff, their skills and knowledge. In addition, the effect on the business processes should be considered, as well as on the technologies used, the culture of the organization and the consequences for the roles and responsibilities related to cyber security controls in place. This last one can be explicated by using a RACI matrix. RACI stands for Responsible, Accountable, Consulted, and Informed, and is used to map responsibilities to persons.

These decisions are documented and the roadmap is communicated to the stakeholders and the staff responsible for implementing the strategy. A cyber security strategy document can then be created based on the deliverables from every step.

CONCLUSION

Based on the research done which was described above, we can answer the main research question:

How can a corporate organization develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition?

A corporate organization can develop a cyber security strategy given a cyber security ambition that supports the organization's general ambition by following these high-level steps:

5. Identify the need for a cyber security strategy and determine the cyber security ambition;
6. Define the cyber security strategy operating setup;
7. Analyze the current situation;
8. Describe the strategic objectives and associated activities.

However, in order to successfully create and implement a cyber security strategy, several conditions apply. Buy-in from senior management is of utmost importance. Without their support, the strategy is likely to fail. In addition, the cyber security strategy should be part of, aligned with, and support the business strategy. Furthermore, the cyber security strategy should be evaluated yearly and renewed every three years. During the creation of the cyber security strategy, stakeholder should

be identified and involved early in the process. And finally, the outcomes of every step and previous steps need to be reviewed after completion of this step. Every step is an important building block for the next step and without proper consideration and evaluation, the chance will be higher that decision are made on incorrect information.

The found method extends the body of knowledge about strategy creation and specifically in the field of cyber security. By following this method to create a well-thought cyber security strategy, it also helps organizations to be more resilient to an emerging threat landscape. Furthermore, the validation showed that it is considered a useful tool to use in practice.

FUTURE RESEARCH

Based on what was found in this research, we identified several directions for future work. First of all, one could validate the method in practice by walking through all steps. This way, we could really validate the order and applicability of the steps in the field. In addition, one could research strategy creation from more perspectives, for instance from a marketing perspective. Furthermore, it would be interesting to look at more popular methods in the field, rather than scientific methods. For instance, the cyber security framework of NIST also shows steps to follow to improve cyber security programs at organization. One can also perform more research about every single step, to research what possible ambitions, project setups, strategic objectives, and strategies are in the field of cyber security. In addition, it is interesting to research which tools can be used to perform the found method steps. Moreover, one could research different methods to model traceability between the outcomes of different method steps (e.g. i*, tree diagrams). And finally, research into the successfulness of the method and the cyber security strategy would be very important and interesting. We would like to get answers to questions like when is a (cyber security) strategy considered successful? How do the steps used to come to a cyber security strategy relate to the successfulness of the strategy? How can you measure when a step in the method has been successfully executed? Our research raised all these questions and we are curious to the answers.

REFERENCES

Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2008). Making Sense of Technology Trends in the Information Technology Landscape: A Design Science Approach. MIS Quarterly, 32(4), 779–809.

Baetz, M. C., & Bart, C. K. (1996). Developing Mission Statements Which Work. Long Range Planning, 29(4), 526–533. doi:10.1016/0024-6301(96)00044-1

Boyd, J. (1987a). Organic Design for Command and Control.

Boyd, J. (1987b). The Strategic Game of ? and ?

Brandenburger, A. M., & Nalebuff, B. j. (1995). The Right Game: Use Game Theory to Shape Strategy. Long Range Planning, 28(5), 128. doi:10.1016/0024-6301(95)90326-7

Byres, E., & Lowe, J. (2004). The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. In Proceedings of the VDE Kongress (pp. 1–6).

CEB. (2013). Is Your Company Taking Risk Reduction Too Far? Retrieved from http://news.executiveboard.com/2013-04-15-Is-Your-Company-Taking-Risk-Reduction-Too-Far

Chabinsky, S. R. (2010). Cybersecurity Strategy : A Primer for Policy Makers and Those on the Front Line. Journal of National Security Law & Policy, 4(27), 27–39.

David, F. R. (1989). How companies define their mission. Long Range Planning, 22(1), 90–97. doi:10.1016/0024-6301(89)90055-1

Deloitte. (2011). Raising the Bar 2011 TMT Global Security Study – Key Findings.

Deloitte. (2013). Blurring the lines 2013 TMT Global Security Study.

Deming, W. E. (1982). Quality, productivity, and competitive competition. Massachusetss Institute of Technology Center for Advanced En.

Dorantes, C. (2006). The impact of information security breaches on financial performance of the breached firms: an empirical investigation. Journal of Information Technology Management, XVII(2), 13–22.

Eden, C., & Ackermann, F. (1998). Making Strategy: The Journey of Strategic Management. Londen: Sage Publications.

Gemalto. (2015). Breach Level Index Annual Report 2014.

Grant, R. M. (1991). The resource-based theory of competitive advantage Implications for strategy formulation. Strategic Management Journal, 17(S2), 109–122.

Grant Thornton. (2011). Cybercrime. doi:10.1007/SpringerReference_11517

Hedley, B. (1977). Strategy and the "business portfolio." Long Range Planning, 10(1), 9–15. doi:10.1016/0024-6301(77)90042-5

Hill, T., & Westbrook, R. (1997). SWOT analysis: It's time for a product recall. Long Range Planning, 30(1), 46–52. doi:10.1016/S0024-6301(96)00095-7

Ireland, R. D., & Hirc, M. a. (1992). Mission statements: Importance, challenge, and recommendations for development. Business Horizons, 35(June), 34–42. doi:10.1016/0007-6813(92)90067-J

Johnson, G., Scholes, K., & Whittington, R. (2008). Exploring Corporate Strategy. doi:10.1016/0142-694X(85)90029-8

Kaplan, R., & Norton, D. (1992). The Balanced Scorecard- Measures that drivePerformance. Harvard Business Review.

Lieberman, H. R., Bathalon, G. P., Falco, C. M., Morgan, C. a., Niro, P. J., & Tharion, W. J. (2005). The fog of war: Decrements in cognitive performance and mood associated with combat-like stress. Aviation Space and Environmental Medicine, 76(7 II), 7–14.

McFadzean, E., Ezingeard, J., & Birchall, D. (2007). Perception of risk and the strategic impact of existing IT on information security strategy at board level. Online Information Review, 31(5), 622–660. doi:10.1108/14684520710832333

Mintzberg, H. (1978). Patterns in Strategy Formation, 24(9), 934–948.

Mintzberg, H., Ahlstrand, B., & Lampel, J. (1998). Strategy safari: a guided tour through the wilds of strategic management. Free Press. New York, NY, USA: The Free Press. Retrieved from http://www.amazon.co.uk/dp/0273656368

the Netherlands. (2013). Nationale Cybersecurity Strategie 2.

NIST. (2014). Framework for Improving Critical Infrastructure Cybersecurity.

Owens, M. T. (2007). Strategy and The Strategic Way of Thinking. Naval War College Review, 60(4), 15.

Peng, G. C. A., & Nunes, M. B. (2007). Using PEST Analysis as a Tool for Refining and Focusing Contexts for Information Systems Research. In 6th European Conference on Research Methodology for Business and Management Studies (pp. 229–236). Lisbon, Portugal.

Perky, L. T. (1991). Strategic improvising: How to formulate and implement competitive strategies in concert. Organizational Dynamics, 19(4), 51–64. doi:10.1016/0090-2616(91)90053-C

Ponemon. (2015). Cost of data breach study: Global Analysis 2015.

PwC. (2014). US cybercrime : Rising Key findings from the 2014 US State of Cybercrime Survey.

Uganda. (2011). National Information Security Strategy Uganda.

Verizon. (2014). 2014 Data Breach Investigations Report.

Ward, D. (2005). An Overview of Strategy Development Models and the Ward-Rivani Model. Economic Working Papers, 1–24.

Ward, J., & Peppard, J. (2008). Strategic Planning for Information Systems. Chichester, West Sussex, England: John Wiley Sons, Ltd.

Whittington, R. (2001). What is strategy and does it matter? Cengage Learning EMEA.

Wilson, I. (1992). Realizing the power of strategic vision. Long Range Planning, 25(5), 18–28. doi:10.1016/0024-6301(92)90271-3

Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). Experimentation in Software Engineering. Heidelberg: Springer.

A cross-border analysis of national cyber security strategies

ABSTRACT

While there are many approaches to create a business strategy, we know little about how strategy is created in the cyber security domain. Meanwhile data is one of the most valuable assets of nation's and its inhabitant, which needs protection against threats coming from cyberspace. We have evidence that, in order to adequately protect critical assets and infrastructures of a nation against attacks from cyberspace, it is of importance to have a structured, approach to handle cybersecurity, i.e. a strategy. This research is particularly aimed at finding the key elements that exist within national cyber security strategies. In order to find this answer, 31 national cyber security strategy documents are analyzed on common elements and grouped. The following groups, each with different key elements, are found: (I) Strategic drivers & scope, (II) Cyber threat landscape, (III) AS-IS situation, (IV) TO-BE situation, (V) Countermeasures, and (VI) Implementation.

INTRODUCTION

In the past decades, innovative technologies in a rapidly changing environment together with larger and more complex IT landscapes have created a challenge for companies to keep their information security up to speed (Adomavicius et al., 2008; Deloitte, 2011). Internal vulnerabilities can cause cyber criminals to breach into the systems or workstations and infringe the confidentiality, integrity, and availability of data and information.

It is thus no surprise that protecting a nation's data, information, and critical infrastructures has also risen on the political agenda of countries. Data is currently one of the most valuable assets of organizations. Given certain types of organizations, the most important data possessed differs. For example, the banking and finance industry deals with customer, company and market specific data with regard to their finances, and the most significant detected incident is financial fraud (PwC, 2014). Another example is public agencies, where data about citizens is highly sensitive. Unauthorized access or use of data, systems, and networks counts for a quarter of all detected incidents in this industry. In 2014, "1.500 data breaches led to one billion data records comprised worldwide"; a 78% increase compared to 2013 (Gemalto, 2015). Several reasons for the increased number of breaches are cloud computing, bring your own device, the lack of sufficient awareness amongst employees, and the increased interconnection of critical systems (Byres & Lowe, 2004; Deloitte, 2011, 2013; Verizon, 2014).

Besides organizations who are developing cyber security strategies, there are many countries over the whole world who have developed a cyber security strategy. Countries feel the obligation to protect their data and assets the same way as an organization does. In addition, countries have a public responsibility to protect the national security and therefore, the need for a cyber security strategy is even more eminent.

Given the importance of data and the severity of some incidents, nations should aspire and maintain a high level of cyber security to address their most relevant threats that endanger their most valuable data. However, nations cannot be 100% safe from cyber-attacks occurring in and to their country. Although prevention is a step that must be undertaken, many more measures are necessary to prevent a cyber-attack (Deloitte, 2013). One should focus on either decreasing or eliminating the threat, the vulnerability, and/or the consequence to minimize the probability and impact of a cyber-attack. Threats can be eliminated by preventing threat actors to act, vulnerabilities can be prevented by hardening the targets, and consequences can be deterred or prevented by focusing on minimizing the impact of an attack (Chabinsky, 2010). To tackle this in a structured, and well-thought manner, a cyber security strategy is necessary. Therefore, this article tries to answer the following question:

What are the key elements of a national cyber security strategy?

To answer our research question, we analyzed national cyber security strategy documents for common elements.

This paper is structured as follows. First, a short literature review that depicts on the difference between information security and cyber security is given. Next, the research method is discussed. This research method led to the results, which are presented next. Finally, an answer to the main research question is given.

LITERATURE

Information security and cyber security are often used interchangeably. However, they do not indicate the exact same thing. While cyber security is related to protecting information and non-information based assets which are processed, stored, and transported via the internet (ISACA, 2014), information security takes a broader perspective by focusing on "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability". The key differences between these terms is the perspective of information and non-information, and access through the internet or other sources. Although some might refer to information security as an umbrella term for ICT security and cyber security, information security expands on the concepts

of ICT security. And cyber security, in addition, expands on the concepts of information security (von Solms & van Niekerk, 2013). Figure 5 shows the relationship between information, ICT, and cyber security.

Information security deals with both analogue and digital information (von Solms & van Niekerk, 2013). For example, leaving a paper report at a printer can pose a threat to the confidentiality of the information stored in the report. ICT security deals only with information based assets stored or transmitted using ICT, i.e. digital information. For example, passwords stolen by hackers can pose a threat to the integrity of the digital information. And lastly, cyber security deals with both information based assets stored or transmitted using ICT and non-information based assets that are vulnerable to threats via ICT (von Solms & van Niekerk, 2013). This means that also humans are an important factor in cyber security as they can be vulnerable for, for example, phishing mails. Cyber security is thus solely focused on threats from and happening in cyberspace. For example, the Stuxnet worm made use of the internet to attack Iran's nuclear centrifuges. Machines were not built with cyber security taken into mind. SCADA systems were therefore targeted via cyberspace by the Stuxnet worm.

Cyberspace is the "realm of computer networks (and the users behind them) in which information is stored, shared, and communicated online" (Singer & Friedman, 2014). One of the key elements of cyberspace are humans, the people behind the computers and who connect to the internet. Cisco (2011) predicts that by 2020 there will be about 50 Billion of internet connected devices versus a population of 7.6 Billion people; the amount of devices connected to cyberspace is continuously growing and evolving. With the growth of cyberspace, organizations need protection against threats from cyberspace. Every organization has valuable assets that are worth protecting against threat agents who wishes to damage or abuse the asset. They will do that by exploiting vulnerabilities that exist in the asset or the environment. Security controls can be imposed to reduce the number of vulnerabilities and thereby reducing risk to an acceptable level.

Cyberspace provides several advantages above the 'real' physical world: it is timeless, borderless and anonymous. However, cyberspace was 'not designed with security in mind' according to the UK's National Audit Office (2013). Cyberspace was never designed for tracking and tracing user behavior, nor to resist highly untrustworthy users (Lipson, 2002). In addition, the current threat environment far exceeds cyberspace's design parameters and high-speed traffic hinders tracking (Lipson, 2002).

It is thus not surprising that cybercrimes followed rather quickly after the 'commercial' introduction of the internet. One of the first recognized cybercrimes, a worm, was the Morris worm in 1988 (Orman, 2003). Since then, the number of attacks has grown exponentially, especially in the 21st century. In addition, the skills needed to perform an attack has become significantly less (Lipson, 2002). For example, the ZeuS bot (Choo, 2011a) made it possible for less skilled hackers to distribute the malware and steal tons of personal identity information (PII) and financial identity information (FII).

In the past years, the threat landscape has changed by economic-, technological-, market-, and legal developments (KPMG, 2014)and has been characterized by phishing and malware. In 2009 and 2010, Australia's industry was dominated by malware attacks (Choo, 2011b). This meant a 71% increase in malware attacks compared to 2008. The period of 2004-2008 was also characterized by malware attacks, in most cases targeting the financial services industry (Choo, 2011a). Besides malware, phishing attacks was listed in the top five most expensive crime in 2009 and 2010 in Australia (Choo, 2011b). However, the amount of fully automated attacks decreased (Potts, 2012). Also, in recent years, the motivation for committing a cybercrime shifted from curiosity and fame seeking to financial gain (Choo, 2011a). The UK's National Audit Office (2013) saw that 'serious organized crime using the internet to steal personal or financial data to commit fraud, steal corporate intellectual property, or launder money; political activists hacking and using the internet to steal information or damage computer systems to serve political agendas; and state supported espionage and attacks on critical national infrastructure' are existing and evolving threats to the internet. In addition, a research by (Gragido, 2011) stated that the current threat landscape is shaped by the growing availability and consumption of enterprise technologies and the increasing sophistication of cyberattacks. Besides that, web applications remain the main target of cyberattacks and legacy threats are in revival (Gragido, 2011).

And what about the future? The Internet of Things (IoT), smart devices, cloud computing, consumerization of IT (e.g. BYOD), and social media will soon shape the cyber threat landscape (Choo, 2011a, 2011b; Contreras et al., 2013; Gragido, 2011; Kellerman, 2010; Potts, 2012; Victoria & Florin, 2012; Zimski, 2011).

METHOD

Due to the transparent nature of public organizations, and their social responsibility towards citizens, it is not surprising that in the public domain cyber security strategies are generally published. Besides, citizens are one of the most important stakeholders in governmental cyber security strategies. Therefore these published strategies are a good basis for the understanding of a cyber security strategy. This understanding can create a basis for discussion about cyber security strategy in corporate organizations. By analyzing the strategy documents on content, and identifying what is generally described (e.g. strategic objectives, cyber threat landscape for a specific nation), one can externalize the critical factors taken into account when constructing a security strategy and what steps were followed.

A search was performed via Google, by using the search term 'cyber security strategy'. With this search, two hubs for national cyber security strategies were found, namely the website of ENISA[17] and the website of the NATO Cooperative Cyber Defense Centre of Excellence[18]. National security strategies were included when:

- they would discuss the topic of either information security or cyber security;
- the strategy is published in Dutch or English;
- a PDF version is available;
- the strategy document is final.

The national cyber security strategies that were excluded from the analysis are listed in Table 1.

Table 1: Excluded national cyber security strategies

Nation	Exclusion criteria
India	Only a draft version (notification) is available
Luxembourg	Only published in French
Malaysia	Only a summary is available
Romania	Only published in Romanian
Russia	Only available in plain HTML
Rwanda	Only a draft version is available
South Africa	Only a draft version is available

The goal of the analysis is to deduce the critical factors taken into account when constructing these national cyber security strategies. By analyzing what is discussed, one can translate this back to what is thought of when creating the strategy document. This was done by highlighting all important aspects that are discussed in the strategy documents. In this case, it did not matter what the exact directions are or content is of a certain section. During this research we focus on the elements of the national cyber security strategies. The correctness, completeness, and quality of the elements are out of scope for this research.

RESULTS

Based on the inclusion criteria shown in Table 1, 31 adequate national cyber security documents were found from countries within the European Union and outside the European Union. The analysis of these national cyber security strategies on common elements resulted in 48 unique concepts that were grouped into 6 general groups. During the grouping process, the concepts were organized based on their logical connection and on the order distilled from the strategy documents. The results of the grouping process can be found in Figure 1 Every group is discussed below.

Strategic drivers & scope

The strategic drivers & scope section resembles the introduction section of most national cyber security strategy documents. Here the drivers for having a strategy are discussed. For example, there could be more cyber-attacks in the last months or the economic impact resulting from a breach is very high for all stakeholders. In addition, the strategy is scoped according to what is held into account and what is not. This might include the definition of cyber security, to have everybody on the same page. For example, the following definitions for cyber security were used:

> "The term 'cyber security' stands for the security of infrastructures in cyber space, of the data exchanged in cyber space and above all of the people using cyber space" (Austria, 2013)
>
> "Cyber security means the desired end state in which the cyber domain is reliable and in which its functioning is ensured" (Finland, 2013)
>
> "Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace" (Hungary, 2013)

Although they are not similar to the one described by ENISA in the introduction, they do emphasize the cyber space as the environment where actions are performed and the environment which needs to be secured.

In addition, there is usually a link made to other strategic documents, like the national security strategy, and to previous cyber security strategies. For example, the Estonian Cyber Security Strategy (2014) already states in their introduction that "the Cyber Security Strategy 2014-2017 is the basic document for planning Estonia's cyber security and a part of Estonia's broader security strategy" and that "this strategy continues the implementation of many of the goals found in the Cyber Security Strategy 2008-2013; however, new threats and needs which were not covered by the previous strategy have also

[17] https://ccdcoe.org/strategies-policies.html , consulted on 17-02-2015
[18] https://ccdcoe.org/strategies-policies.html , consulted on 17-02-2015

been added". In addition, compliance with law and the identification of stakeholders are also discussed and related to the strategic drivers and scope of the strategy.

		EU Countries																Non-EU Countries												
		AUT	BEL	CZE	EST	FIN	FRA	ITA	DEU	HUN	LVA	LTU	NLD	POL	SVK	ESP	GBR	AUS	CAN	JPN	KEN	MNE	NZL	NOR	SGP	CHE	TUR	UGA	USA	GEO	KOR	TTO
1. Strategic drivers & scope	drivers	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
	economic impact							X			X						X	X	X					X		X						
	scope																	X									X					
	definition cyber security	X	X			X		X		X			X					X	X					X				X				X
	glossary	X	X			X		X	X		X	X		X							X	X	X	X			X					
	relation with other strategic documents	X		X	X	X				X	X	X	X	X	X	X	X	X			X	X		X		X		X				X
	relation with previous strategies				X		X						X							X					X							
	compliance with laws		X						X					X	X	X		X			X	X				X		X				
	stakeholders			X	X					X			X	X			X		X	X	X	X	X			X						
2. Cyber threat landscape	threats	X					X	X	X	X			X			X	X	X	X	X	X	X	X	X	X	X		X				X
	risks	X														X				X		X				X	X	X				
	challenges				X			X						X							X	X		X					X			
	opportunities	X																														
	cyber trends		X		X				X				X				X			X	X											
	ICT trends		X		X								X					X		X					X			X				X
3. AS-IS situation	maturity analysis																				X							X				
	comparison with other countries														X													X				
	cyber security perspective EU														X																	
	SWOT analysis																											X				
	analysis of critical infrastructures																									X		X				
	analysis current situation				X					X	X				X							X				X		X				
4. TO-BE situation	vision				X	X				X							X								X			X				X
	mission																								X			X				
	ambition	X			X	X	X				X	X	X					X	X	X	X			X	X	X	X		X	X	X	
	- guiding principles	X		X	X	X					X					X	X	X		X						X	X	X	X			X
	strategic objectives	X	X	X	X	X	X	X	X	X		X	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X	X	X	X
	- strategic priorities														X		X	X					X	X					X			
	- strategic measures			X																												
	key benefits																				X											
5. Countermeasures	action	X	X				X	X		X	X	X	X	X	X	X	X	X	X	X		X		X		X	X	X	X	X	X	X
	action timeframe											X	X		X			X		X		X					X	X		X		
	action stakeholders											X	X									X					X	X		X		
	action plan											X	X				X					X		X			X	X		X		X
	action measures	X										X																				
	operational goals																															X
	important milestones and CSF																											X				
	roles and responsibilities government					X	X	X					X		X		X	X		X			X	X			X					X
	roles and responsibilities stakeholders		X			X	X	X	X				X		X		X	X		X		X		X			X	X		X		X
6. Implementation	implementation	X							X			X		X		X								X		X						
	follow-up	X									X				X			X		X							X					
	assessment of effectiveness													X				X														
	- expected effects													X																		
	- effectiveness of actions													X																		
	- effectiveness measures													X	X											X						
	consequences													X			X															
	organisation													X		X		X				X						X				X
	cooperation							X						X					X			X			X	X						
	financing													X	X			X										X				

FIGURE 1: RESULTS OF ANALYZING NATIONAL CYBER SECURITY STRATEGIES

Cyber threat landscape

An important step within all national cyber security strategies is the assessment of the current and future cyber threat landscape, also as a way to illustrate the importance of having a cyber security strategy and to serve as a basis for the strategy. Here, threats, risks, attacks, challenges, opportunities, and trends are discussed in order to shape the threat environment the nation is dealing with. A good example is Austria, who made a matrix (Figure 2) by comparing different threats against the probability of occurring and the consequence.

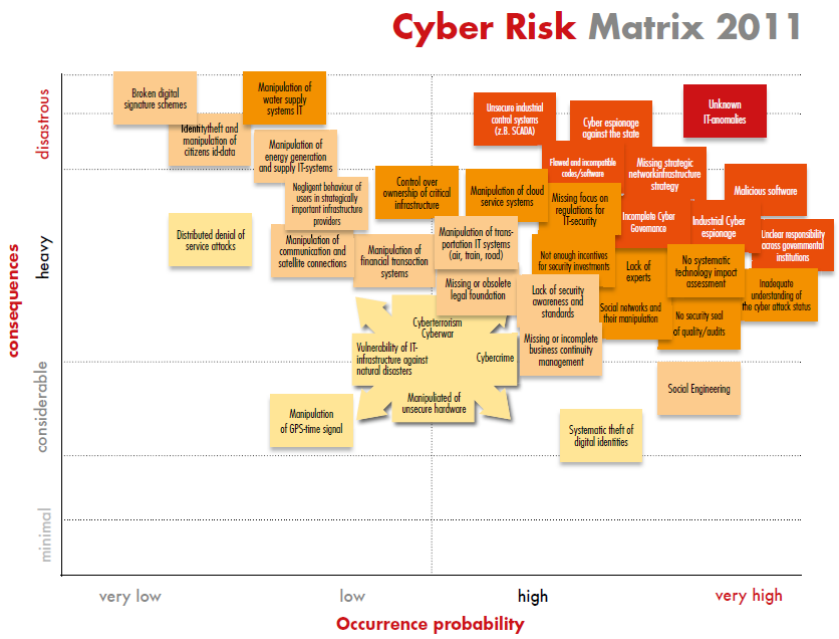


FIGURE 2: CYBER RISK MATRIX 2011 (AUSTRIA, 2013)

Another way of illustrating recent cyber-attacks is by showing a timeline, like Singapore (2013) did. In addition, some countries also identified challenges to cyber security. An example of a challenge to cyber security is the fact that the internet is more and more used for criminal activity and therefore gives the cyberspace a rather negative image (Montenegro, 2013).

AS-IS situation

Another important step is to analyze the internal situation, or at least to identify what is already in place. The national cyber security strategies have shown that this could be assessed in different ways. One way is by doing a maturity analysis. Although this is a rather extensively used method in organizations, it seems that public organizations are not using these to assess current situations and base their strategic objectives on the identified gap (i.e. only Kenya (2014) and Uganda (2011) use this method); or not disclosing them. Other initiatives are an analysis of the current situation, what is already in place concerning cyber security. Less used methods are a SWOT analysis, comparison with other countries, comparison with the EU perspective, analysis of IS soft controls, analysis of critical infrastructures, and the analysis of social growth. For example, the Slovakia states that "the tasks defined for the forthcoming period are based on the current state of play in information security in Slovakia compared to the situation in other EU Member States and other advanced countries of the world" (Slovakia, 2008). ENISA published a good practice guide to national cyber security strategies, and one of their main points is to identify critical information infrastructures. However, not many strategy documents, except for Switzerland and Uganda, describe what a nation's critical information infrastructures are.

TO-BE situation

The strategic drivers and the external and internal analysis of the nation's environment will lead to the whole of strategic goals. Within this step, we distinguish the components listed in Figure 3**Error! Reference source not found.**, from high evel to low level that constitute the strategy, based on their common occurrences in the national cyber security strategies.

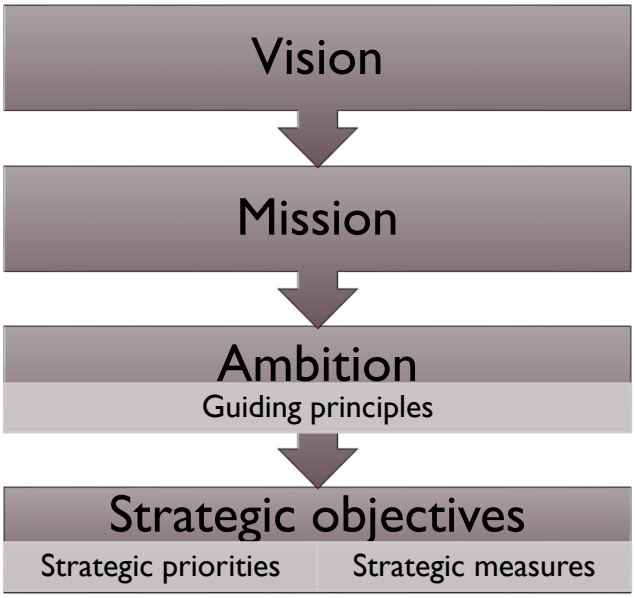


FIGURE 3: STRATEGY COMPONENTS DISTILLED FROM NATIONAL CYBER SECURITY STRATEGIES

An example of a vision is "Estonia is able to ensure national security and support the functioning of an open, inclusive and safe society" (Estonia, 2014). A mission is only mentioned twice, by Singapore (2013) and Uganda (2011), where Singapore states that "the NCSM2018's mission is to enhance Singapore's cyber security capabilities in four focal areas – Government, Critical Infocomm Infrastructure (CII), Businesses and Individuals".

In addition, an example of an ambition is "the Netherlands is leading in the field of cybersecurity" (the Netherlands, 2013, p. 8). This ambition is supported by guiding principles, like "the Dutch society successfully makes optimal and safe use of the benefits of digitization" (the Netherlands, 2013, p. 8). Examples of strategic objectives, priorities or measures can be, amongst others, found in the strategy of the Czech Republic (2015), New Zealand (2011), and Slovakia (2008). New Zealand's first priority is to create an increasing awareness and online security. The key initiative to this objective is "to partner with industry and non-government organizations, to centralize cyber security information and resources for ease of access, and deliver a coordinated cyber safety awareness-raising programme" (New Zealand, 2011).

Besides the above described strategy components, some countries also describe strategy guidelines (e.g. to which measures the strategy should satisfy) and key benefits of the strategy.

Countermeasures

Building forward from the previous step, strategic goals, action plans and specific actions are discussed that need to be taken to implement the strategy. These usually consist of clear-cut actions that need to be undertaken by specific stakeholders, within a certain time, within a certain budget. The strategy of Lithuania does this elaborately in an action plan, illustrated in Figure 4.

No. Nr.	*Objective*	*Task*	Assessment criterion	Indicator in 2011	Indicator in 2015	Indicator in 2019	Institution responsible for implementation of the criterion
1.	*1. To ensure the security of national information resources*		Level of compliance of national information resources with security requirements, (%)	–	95	98	All the institutions specified in items 3 to 29 of this Annex, according to their competences
2.		1.1. to improve the coordination and monitoring of electronic information security (cyber security);	Level of resources (%), security of which is monitored by an institution designated by the law on the basic requirements related to ensuring electronic information security (cyber security)	–	70	100	All the institutions specified in items 3 to 10 of this Annex, according to their competences
3.			Percentage of entities in defining and implementing national policy in the area of electronic information security (cyber security) that belong to the national system of coordination of electronic information security (cyber security), (%) Permanent collegial consultative council of electronic information security (cyber security) established	– –	80 yes	100 yes	Ministry of the Interior, Ministry of National Defence, Ministry of Transport and Communications, State Data Protection Inspectorate
4.			Number of evaluation studies of existing capabilities in the area of electronic information security (cyber security) and their potential	–	1	2	Ministry of the Interior

FIGURE 4: SCREENSHOT OF ACTION PLAN OF THE CYBER SECURITY STRATEGY OF LITHUANIA FOR 2011-2019 (LITHUANIA, 2012)

The strategy of Uganda also discusses important milestones that need to be achieved and critical success factors for the implementation of the strategy. Uganda is the only nation that elaborates on these two topics. However, what is more commonly discussed is the roles and responsibilities of the government and stakeholders. There are special tasks for the government itself, which it should carry out. In addition, stakeholders involved in some way in the strategy. The government can also be the stakeholder, as the strategy could affect them as well. Therefore the distinction is made between roles and responsibilities of the government (the sender) and of stakeholders (the receiver).

Implementation

After directed actions are discussed, some countries also roughly discuss how they are going to implement the strategy; the follow-up. For example, a follow-up could how the nation will assess the effectiveness of the strategy every year after the implementation. To give meaning to the 'effectiveness of the strategy', some countries propose a measure, and elaborate on the expected effects. In addition, the effectiveness of specific actions was also discussed by Poland. Poland is one of the only nation that discusses the topic of effectiveness elaborately, and dedicate a separate chapter to this topic. For example, an effectiveness measure is "the number of closed incidents in relation to the total number of categorized incidents" (Poland, 2013). In addition, they expect, amongst others that the strategy will result in a higher level of security and resistance against attacks (Poland, 2013). Also, they dedicate a section to the consequences of not achieving the desired effects.

Other more often used concepts regarding implementation are the governmental organization needed, collaboration with other both public and private institutions, and the financial resources necessary to implement the cyber security strategy.

DISCUSSION AND CONCLUSION

We searched for existing national cyber security strategies, due to a lack of literature on this specific topic to answer the research question, Therefore it makes it difficult to compare our results to previous or existing results. Many (31) national cyber security strategies were found. This number of strategy documents allows us to present our research results with more scientific confidence. However, it may be possible that these strategy documents are not always complete. As such, it is not to be ruled out that the outcome of this research is not complete either. Nevertheless, every document showed common high-level similarities which do give a direction which allows us find key elements.

This research aimed to find an answer to the following question: "*What are the key elements of a national cyber security strategy?*" The following key elements were found:

- Strategic drivers and scope: (1) Drivers; (2) Economic impact; (3) Scope; (4) Definitions; (5) Relation with other strategic documents; (6) Relation with previous strategies; (7) Compliance with laws; (8) Stakeholders.
- The cyber threat landscape: (1) Threats; (2) Risks; (3) Challenges; (4) Opportunities; (5) Cyber trends; (6) ICT trends.
- AS-IS analysis: (1) Maturity analysis; (2) Comparison with other countries; (3) Analysis of critical infrastructures; (4) Current situation.
- TO-BE analysis: (1) Vision; (2) Mission; (3) Ambition; (4) Strategic objectives; (5) Strategy guidelines; (6) Key benefits.
- Countermeasures: (1) Action; (2) Action timeframe; (3) Action stakeholders; (4) Action plan; (5) Action measure; (6) Important milestones and CSF; (7) Roles and responsibilities government and stakeholders.

- Implementation plan: (1) Implementation plan; (2) Follow-up; (3) Assessment of effectiveness; (4) Expected effects; (5) Effectiveness of actions; (6) Effectiveness measures; (7) Consequences; (8) Organization; (9) Cooperation; (10) Financing.

REFERENCES

Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2008). Making Sense of Technology Trends in the Information Technology Landscape: A Design Science Approach. MIS Quarterly, 32(4), 779–809.

Austria. (2013). Austrian Cyber Security Strategy.

Byres, E., & Lowe, J. (2004). The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. In Proceedings of the VDE Kongress (pp. 1–6).

Chabinsky, S. R. (2010). Cybersecurity Strategy : A Primer for Policy Makers and Those on the Front Line. Journal of National Security Law & Policy, 4(27), 27–39.

Choo, K.-K. R. (2011a). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719–731. doi:10.1016/j.cose.2011.08.004

Choo, K.-K. R. (2011b). Trends & issues financial and insurance industry. Trends and Issues in Crime and Criminal Justice, 408(1), 1–6.

Cisco. (2011). The Internet of Things How the Next Evolution of the Internet The Internet of Things How the Next Evolution of the Internet Is Changing Everything.

Contreras, J. L., Denardis, L., & Teplinsky, M. (2013). Mapping Today ' s Cybersecurity Landscape Mapping Today ' s Cybersecurity Landscape, 62(5), 1113–1130.

Czech Republic. (2015). Cyber Security Strategy of the Czech Republic.

Deloitte. (2011). Raising the Bar 2011 TMT Global Security Study – Key Findings.

Deloitte. (2013). Blurring the lines 2013 TMT Global Security Study.

Estonia. (2014). Cyber Security Strategy Estionia.

Finland. (2013). Finland´s Cyber security Strategy.

Gemalto. (2015). Breach Level Index Annual Report 2014.

Gragido, W. (2011). Beyond zero: analysing threat trends. Network Security, 2011(7), 7–9. doi:10.1016/S1353-4858(11)70074-5

Hungary. (2013). National Cyber Security Strategy.

ISACA. (2014). Glossary. Retrieved from http://www.isaca.org/Pages/Glossary.aspx?tid=2077&char=C

Kellerman, T. (2010). Cyber-Threat Proliferation. Security & Privacy, IEEE, 8(3), 70–73.

Kenya. (2014). National Cybersecurity Strategy.

KPMG. (2014). Cyber Security : from threat to opportunity.

Lipson, H. F. (2002). Tracking and Tracing Cyber-Attacks Technical Challenges and Global Policy Issues.pdf.

Lithuania. (2012). The programme for the Development of Electronic Information Security (Cyber-Security) for 2011-201.

Montenegro. (2013). National Cyber Security Strategy for Montenegro.

National Audit Office. (2013). The UK cyber security strategy : Landscape review.

the Netherlands. (2013). Nationale Cybersecurity Strategie 2.

New Zealand. (2011). New Zealand's Cyber Security Strategy.

Orman, H. (2003). The Morris Worm: A Fifteen-Year Perspective. IEEE Security & Privacy, 1(5), 35–43.

Poland. (2013). Cyperspace Protection Policy of the Republic of Poland.

Potts, M. (2012). The state of information security. Network Security, 2012(7), 9–11. doi:10.1016/S1353-4858(12)70064-8

PwC. (2014). US cybercrime : Rising Key findings from the 2014 US State of Cybercrime Survey.

Singapore. (2013). National Cyber Security Masterplan.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford, UK: Oxford University Press.

Slovakia. (2008). National Strategy for Information Security in the Slovak Republic.

Uganda. (2011). National Information Security Strategy Uganda.

Verizon. (2014). 2014 Data Breach Investigations Report.

Victoria, S., & Florin, B. (2012). Emerging IT Technologies - Advantages and Risks, 2012(5), 181–188.

Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. doi:10.1016/j.cose.2013.04.004

Zimski, P. (2011). Navigating the new threat landscape. Computer Fraud & Security, 2011(5), 5–8. doi:10.1016/S1361-3723(11)70049-5